Políticas del Programa para Desarrolladores

(en vigor a partir del 3 de octubre del 2022, a menos que se indique otra cosa)

Creemos la tienda de aplicaciones y juegos más fiable del mundo

Tu innovación es lo que impulsa nuestro éxito compartido, pero esto conlleva responsabilidades. Estas Políticas del Programa para Desarrolladores y el Acuerdo de Distribución para Desarrolladores aseguran que juntos sigamos proporcionando las aplicaciones más innovadoras y fiables del mundo a más de mil millones de usuarios a través de Google Play. Te invitamos a consultar nuestras políticas, que se incluyen a continuación.

Contenido restringido

Cada día, usuarios de todo el mundo utilizan Google Play para acceder a aplicaciones y juegos. Antes de publicar una aplicación, debes preguntarte si es adecuada para Google Play y si cumple la legislación local.

Protección infantil

Las aplicaciones que no prohíban a los usuarios crear, subir o distribuir contenido que facilite la explotación o el abuso de menores de edad estarán sujetas a la retirada inmediata de Google Play. Esto incluye toda clase de material de abuso sexual infantil. Para denunciar contenido de un producto de Google que pueda considerarse explotación de menores de edad, haz clic en **Denunciar abuso** . Si encuentras contenido de este tipo en otros sitios de Internet, ponte en contacto directamente con el organismo competente en tu país .

Está prohibido usar aplicaciones que pongan en peligro a menores de edad. Esto incluye, entre otras cosas, el uso de aplicaciones para promover comportamientos abusivos hacia menores de edad, como los siguientes:

- Interacciones inadecuadas (como tocamientos o caricias) dirigidas a menores de edad.
- Acoso a menores de edad (por ejemplo, entablar amistad con un menor de edad a través de servicios online para propiciar, ya sea mediante Internet o en persona, contactos sexuales o intercambio de imágenes sexuales con dicho menor de edad).
- Sexualización de menores de edad (por ejemplo, imágenes que representen, fomenten o promuevan el abuso sexual infantil, o que muestren a menores de edad de una forma que pueda dar lugar a la explotación sexual infantil).
- Extorsión sexual (por ejemplo, amenazar o chantajear a un menor de edad sobre la base de un acceso real o supuesto a imágenes íntimas suyas).
- Trata de menores de edad (por ejemplo, anuncios o solicitudes de menores de edad para su explotación sexual con fines comerciales).

Si detectamos contenido que incluya material de abuso sexual infantil, tomaremos las medidas oportunas, que pueden incluir denunciar los hechos ante el centro nacional para menores desaparecidos y explotados de Estados Unidos (National Center for Missing & Exploited Children). Si sospechas que un menor de edad está en peligro o ha sido objeto de abuso, explotación o trata, ponte en contacto con los cuerpos de policía locales y con una de las organizaciones de protección de menores de edad que figuran aquí .

Además, no están permitidas las aplicaciones que estén dirigidas a menores de edad, pero contengan temas para adultos, incluidas, entre otras:

- Aplicaciones con violencia excesiva, sangre o contenido macabro.

- Aplicaciones que muestren o fomenten actividades dañinas o peligrosas.

Tampoco permitimos aplicaciones que promuevan una imagen negativa del cuerpo o de uno mismo, ni aplicaciones que, por entretenimiento, muestren intervenciones de cirugía plástica, pérdida de peso u otros ajustes estéticos en la apariencia física de una persona.

Contenido inadecuado

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

Contenido sexual y palabras malsonantes

No admitimos aplicaciones que incluyan o promocionen contenido sexual o palabras malsonantes, incluyendo la pornografía, o cualquier contenido o servicio cuya finalidad sea provocar placer sexual. No admitimos aplicaciones ni contenido de aplicaciones que parezcan promocionar un acto sexual a cambio de una gratificación. Es posible que se permitan contenidos que incluyan desnudos justificados si el objetivo principal es educativo, informativo, científico o artístico.

Si una aplicación incluye contenido que infringe esta política, pero ese contenido se considera adecuado en una región en concreto, es posible que la aplicación esté disponible para los usuarios de esa región, pero seguirá sin estarlo para los usuarios de otras regiones.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Representaciones de desnudos de carácter sexual o de posturas sexualmente sugerentes en las que el sujeto aparezca desnudo, con zonas íntimas desenfocadas o con poca ropa, o con ropa que no se considere aceptable en un contexto público correcto.
- Representaciones, animaciones o ilustraciones de actividades sexuales, posturas sexualmente sugerentes, o la representación sexual de partes del cuerpo.
- Contenido que muestre o que cumpla la función de estímulo sexual, guía sobre sexo o juguete sexual, o que incluya fetiches o temas sexuales ilegales.
- Contenido lascivo o soez (por ejemplo, contenido que incluya palabras malsonantes, insultos, texto con contenido explícito o la inclusión de palabras clave sexuales o para adultos en la ficha de Play Store o en la aplicación).
- Contenido que represente, describa o fomente la zoofilia.
- Aplicaciones que promocionen ocio relacionado con el sexo, servicios de compañía u otros servicios que se puedan interpretar como favores sexuales a cambio de algún tipo de gratificación, entre los que se incluyen las citas remuneradas o los acuerdos sexuales en los que se espera o se supone que un participante ofrece dinero, regalos o ayuda financiera a otro participante ("sugar dating").
- Aplicaciones que degraden o cosifiquen a las personas, como aplicaciones que afirmen quitar la ropa o ver a través de la vestimenta de las personas, incluso si están etiquetadas como aplicaciones de broma o de entretenimiento.

Incitación al odio

No admitimos aplicaciones que fomenten la violencia o inciten al odio hacia personas o grupos por motivos de raza u origen étnico, religión, discapacidad, edad, nacionalidad, condición de veterano militar, orientación sexual, sexo, identidad de género, casta, estado de inmigración u otras características asociadas a la discriminación o la marginación sistémicas.

Las aplicaciones en las que haya contenido que tenga fines educativos, documentales, científicos o artísticos y guarde relación con el nazismo pueden ser bloqueadas en determinados países, de conformidad con lo estipulado en la legislación local.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Contenido o razonamientos destinados a deshumanizar a un grupo protegido o a presentarlo como inferior o merecedor de odio.
- Aplicaciones que contengan insultos, estereotipos o teorías sobre supuestas características negativas de un grupo protegido (por ejemplo, decir que son maliciosos, corruptos o perversos) o que afirmen de forma explícita o implícita que el grupo supone una amenaza.
- Contenido o discursos que inciten al odio o la discriminación de otras personas por formar parte de un grupo protegido
- Contenido que promocione símbolos de odio, como banderas, símbolos, insignias, artículos o comportamientos asociados a grupos de odio.

Violencia

No admitimos aplicaciones que representen o muestren escenas de violencia gratuita u otras actividades peligrosas. Por lo general, se permiten aplicaciones que representen violencia ficticia en el contexto de un juego, como dibujos animados, caza o pesca.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Representaciones gráficas o descripciones de violencia real, así como amenazas violentas dirigidas a cualquier persona o animal
- Aplicaciones que fomenten lesiones personales, suicidio, desórdenes alimenticios, juegos de asfixia u otras acciones que podrían causar daños graves o la muerte

Terrorismo

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

No admitimos aplicaciones que incluyan contenido relacionado con el terrorismo como, por ejemplo, aquel que fomente actos terroristas, incite a la violencia o celebre este tipo de ataques. Si publicas contenido relacionado con el terrorismo en un contexto educativo, documental, científico o artístico, debes proporcionar un contexto con fines educativos, documentales, científicos o artísticos (EDSA) pertinente.

Organizaciones y movimientos peligrosos

No permitimos que ningún movimiento ni ninguna organización que hayan preparado o participado en actos violentos contra civiles, o que hayan reivindicado su autoría, publiquen aplicaciones en Google Play con ningún fin, incluido el reclutamiento.

No permitimos que se publiquen aplicaciones con contenido relacionado con la planificación, preparación o la exaltación de la violencia contra civiles. Si tu aplicación incluye contenido de ese tipo con fines educativos, documentales, científicos o artísticos (EDSA), dicho contenido debe proporcionarse junto con el contexto EDSA pertinente.

Acontecimientos sensibles

No permitimos aplicaciones que saquen provecho o muestren una falta de sensibilidad con respecto a un acontecimiento sensible que tenga un impacto significativo en el ámbito social, cultural o político, como emergencias civiles, desastres naturales, emergencias de salud pública, conflictos, fallecimientos u otros sucesos trágicos. Por lo general, se permiten aplicaciones con contenido relacionado con un acontecimiento sensible si dicho contenido tiene fines educativos, documentales,

científicos o artísticos (EDSA), o pretende advertir o concienciar a los usuarios sobre el acontecimiento sensible del que trata.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Mostrar una falta de sensibilidad hacia la muerte de una o varias personas reales debida a una sobredosis, suicidio, causas naturales, etc.
- Negar que haya ocurrido un suceso trágico importante que esté bien documentado.
- Obtener beneficio económico de un acontecimiento sensible y que este beneficio no sea para las víctimas.
- Aplicaciones que infrinjan los requisitos de las aplicaciones relacionadas con la enfermedad por coronavirus del 2019 (COVID-19) .

Acoso

No admitimos aplicaciones que contengan o faciliten amenazas o acoso.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Contenido en el que se acose a víctimas de conflictos religiosos o internacionales.
- Contenido que incite a la explotación de otras personas, incluyendo la extorsión, el chantaje, etc.
- Contenido publicado con el objetivo de humillar a alguien públicamente.
- Contenido en el que se acose a víctimas de sucesos trágicos o a sus familiares o amigos.

Productos peligrosos

No admitimos aplicaciones que faciliten la venta de explosivos, armas de fuego, munición o determinados accesorios para armas de fuego.

- Entre los accesorios restringidos se incluyen aquellos que permitan simular disparos automáticos o convertir un arma de fuego para disparar automáticamente (por ejemplo, mecanismos de simulación de disparo automático, gatillos de repetición, accesorios de disparo automático o kits de conversión), así como tambores o cinturones con más de 30 disparos.

No admitimos aplicaciones con instrucciones para fabricar explosivos, armas de fuego, munición, accesorios restringidos para armas de fuego u otras armas. Esto incluye instrucciones que expliquen cómo convertir un arma de fuego en un arma automática o automática simulada.

Marihuana

No admitimos aplicaciones que faciliten la venta de marihuana o productos relacionados, independientemente de si son legales o no.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Permitir que los usuarios pidan marihuana a través de una función de compra en la aplicación.
- Ayudar a los usuarios a pedir o recoger marihuana.
- Facilitar la venta de productos que contengan THC (tetrahidrocannabinol), como aceites de CBD que contengan THC.

Tabaco y alcohol

No admitimos aplicaciones que faciliten la venta de tabaco (incluidos los cigarrillos electrónicos y los vapeadores) ni que inciten al consumo ilegal o inadecuado de alcohol o tabaco.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Representar o fomentar el consumo o la venta de alcohol o tabaco a menores.
- Afirmar que el consumo de tabaco puede mejorar las habilidades sociales, la potencia sexual, el rendimiento profesional, la capacidad intelectual o la condición física.
- Mostrar imágenes de consumo irresponsable de bebidas alcohólicas, incluida la representación favorable de un consumo excesivo, compulsivo o con carácter competitivo.

Servicios financieros

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

A efectos de esta política, consideramos que los productos y servicios financieros son aquellos que están relacionados con la gestión o la inversión de dinero y criptomonedas, incluido el asesoramiento personalizado.

Si tu aplicación contiene o promociona productos y servicios financieros, debes cumplir la normativa local y nacional de cualquier región o país en el que esté disponible tu aplicación. Por ejemplo, debes incluir los avisos concretos que exijan las leyes locales.

Opciones binarias

No admitimos aplicaciones que permitan a los usuarios comercializar opciones binarias.

Criptomonedas

No admitimos aplicaciones que minen criptomonedas a través de los dispositivos. Sí se permiten las aplicaciones que gestionen el minado de forma remota.

Préstamos personales

Definimos los préstamos personales como aquellos que hace una persona, una organización o una entidad a un consumidor de forma no recurrente y sin la finalidad de financiar la compra de un activo fijo o el pago de formación educativa. Los consumidores de préstamos personales necesitan información sobre la calidad, las funciones, las comisiones, los plazos de devolución, los riesgos y las ventajas de los préstamos para poder tomar una decisión fundamentada sobre la aceptación del préstamo.

- Ejemplos: préstamos personales, anticipos de nómina, préstamos entre particulares y préstamos sobre títulos de propiedad
- Ejemplos de lo que no está incluido: hipotecas, préstamos para coches y líneas de crédito rotativas (como tarjetas de crédito o líneas personales de crédito)

Las aplicaciones que ofrecen préstamos personales, incluidas las que ofrecen préstamos de forma directa, las que generan oportunidades de venta y las que ponen en contacto a consumidores con prestamistas externos, deben estar en la categoría "Finanzas" en Google Play Console y proporcionar la siguiente información en sus metadatos:

- El periodo mínimo y máximo para devolver el préstamo.
- La tasa anual efectiva (TAE) máxima, que suele incluir el tipo de interés, las comisiones y otros costes anuales u otra tarifa similar calculada de acuerdo con la legislación local.

- Un ejemplo representativo del coste total del préstamo, incluidas las comisiones principales y todas aquellas aplicables.
- Una política de privacidad que informe de forma exhaustiva sobre cómo se accede a los datos personales y sensibles de los usuarios, además de cómo se recogen, se usan y se comparten.

No admitimos aplicaciones que promocionen préstamos personales que se deban devolver en un plazo de 60 días o menos desde la fecha de emisión del préstamo (los consideramos préstamos personales a corto plazo).

Préstamos personales con un TAE alto

En Estados Unidos, no admitimos aplicaciones de préstamos personales cuyo TAE sea del 36 % o superior. En Estados Unidos, las aplicaciones de préstamos personales deben mostrar el TAE máximo, calculado de acuerdo con la ley estadounidense de veracidad en los préstamos (Truth in Lending Act, TILA).

Esta política se aplica a las aplicaciones que ofrecen préstamos de forma directa, generan oportunidades de venta o ponen en contacto a los consumidores con prestamistas externos.

Requisitos adicionales para aplicaciones de préstamos personales en Filipinas, India e Indonesia

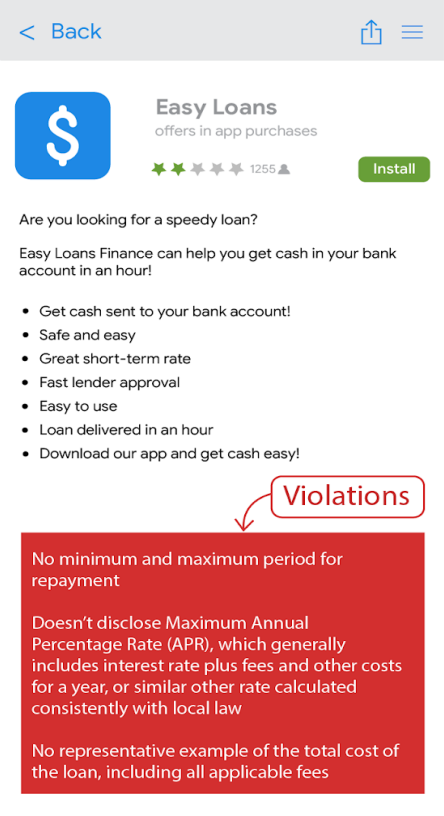
Las aplicaciones de préstamos personales en Filipinas, India e Indonesia deben aportar una prueba adicional de que cumplen los requisitos descritos a continuación.

1. **La India**
   - Rellena la Declaración de Aplicación de Préstamos Personales de la India y proporciona la documentación necesaria para respaldar tu declaración. Por ejemplo:
     - Si el Reserve Bank of India (RBI) te ha concedido licencia para ofrecer préstamos personales, debes enviar una copia de tu licencia para que la revisemos.
     - Si no proporcionas directamente servicios de préstamo de dinero, sino que simplemente ofreces una plataforma para que bancos o empresas financieras no bancarias (NBFC) puedan facilitar el préstamo de dinero a los usuarios, debes indicarlo de forma precisa en la declaración.
       - También debes hacer constar de forma destacada en la descripción de tu aplicación los nombres de todos esos bancos y empresas financieras no bancarias.
   - Asegúrate de que el nombre de la cuenta de desarrollador coincida con el nombre de empresa que se haya registrado, asociado e incluido en la declaración.
2. **Indonesia**
   - Rellena la Declaración de Aplicación de Préstamos Personales de Indonesia y proporciona la documentación necesaria para respaldar tu declaración. Por ejemplo:
     - Si tu aplicación se dedica a los servicios de préstamo de dinero basados en tecnologías de la información de conformidad con el reglamento OJK n.º 77/POJK.01/2016 (que podría experimentar cambios ocasionales), debes enviar una copia válida de tu licencia para que la revisemos.
   - Asegúrate de que el nombre de la cuenta de desarrollador coincida con el nombre de empresa que se haya registrado, asociado e incluido en la declaración.
3. **Filipinas**
   - Rellena la Declaración de Aplicación de Préstamos Personales de Filipinas y proporciona la documentación necesaria para respaldar tu declaración.
     - Todas las empresas financieras y crediticias que ofrezcan préstamos mediante plataformas de préstamo online (OLP) deben obtener un número de registro SEC y el número de certificado de autorización de la Comisión del Mercado de Valores de Filipinas (PSEC).
       - Además, debes revelar en la descripción de tu aplicación el nombre oficial de tu empresa, su nombre comercial, el número de registro del PSEC y el certificado de autorización para

operar una empresa financiera o crediticia.

- Las aplicaciones dedicadas a actividades de micromecenazgo mediante préstamos, como los préstamos de punto a punto (P2P), o según la definición de las normativas y regulaciones que rigen el micromecenazgo, deben procesar transacciones a través de intermediarios registrados con el PSEC.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.



Juegos de apuestas

Permitimos aplicaciones de juegos de apuestas con dinero real, anuncios relacionados con juegos de apuestas con dinero real, programas de fidelización con resultados gamificados y aplicaciones de fantasy sport diario que cumplan ciertos requisitos.

Aplicaciones de juegos de azar y apuestas

De acuerdo con las restricciones vigentes y de conformidad con todas las políticas de Google Play, admitimos las aplicaciones que permitan o faciliten los juegos de azar y apuestas online en determinados países, siempre y cuando el Desarrollador complete el proceso de solicitud para aplicaciones de juegos de azar y apuestas que se distribuyen en Google Play. Además, debe ser un operador gubernamental autorizado o debe estar registrado como operador con licencia proporcionada por la autoridad gubernamental con potestad sobre los juegos de azar y apuestas en el país especificado, y debe proporcionar una licencia de operación válida en el país especificado para el tipo de producto de juegos de azar y apuestas online que quiera ofrecer.

Solo permitimos aplicaciones de juegos de azar y apuestas con licencia o autorizadas que incluyan los siguientes tipos de productos relacionados con los juegos de azar y apuestas online:

- Juegos de casino online
- Apuestas deportivas

- Carreras de caballos (si las regulaciones y licencias son independientes de las que se aplican a las apuestas deportivas en el país o la región pertinente)
- Loterías
- Fantasy sport diarios

Las aplicaciones deben cumplir los siguientes requisitos:

- El desarrollador debe completar el proceso de solicitud correctamente para distribuir la aplicación en Google Play;
- La aplicación debe cumplir todas las leyes aplicables y los estándares del sector de cada país en el que se distribuya;
- El desarrollador debe contar con una licencia de juegos de apuestas en cada uno de los países, estados o territorios en los que se distribuya la aplicación;
- El desarrollador no debe ofrecer ningún tipo de producto de juegos de apuestas que sobrepase el alcance de su licencia de juegos de apuestas;
- La aplicación debe evitar que la utilicen usuarios menores de edad;
- La aplicación debe impedir su acceso y uso en países, estados, territorios o zonas geográficas no incluidos en la licencia de juegos de apuestas proporcionada por el desarrollador;
- La aplicación NO debe estar disponible como aplicación de pago en Google Play ni utilizar la Facturación en Google Play por Compras en Aplicaciones;
- La aplicación se debe poder descargar e instalar de forma gratuita desde Google Play Store;
- La aplicación debe estar clasificada como solo para adultos o un equivalente de la Coalición Internacional de Clasificación por Edad (IARC);
- La aplicación y su ficha deben mostrar información clara sobre cómo participar en juegos de azar y apuestas de forma responsable.

Otras aplicaciones de juegos, concursos y torneos con dinero real

En el caso de las demás aplicaciones que no cumplan los requisitos indicados más arriba para las aplicaciones de juegos de apuestas y que no estén incluidas en "Otras pruebas piloto de juegos con dinero real" más abajo, no admitimos contenido o servicios que permitan o faciliten que los usuarios hagan apuestas o participen con dinero real (incluidos artículos de compra en aplicaciones comprados con dinero) para obtener un premio de valor monetario real. Esto incluye, entre otros, los casinos online, las apuestas deportivas, las loterías y los juegos que acepten dinero y ofrezcan premios en metálico o de otro valor material real (excepto los programas permitidos que cumplan los requisitos para programas de fidelización gamificados descritos más abajo).

Ejemplos de infracciones

- Juegos que acepten dinero a cambio de la posibilidad de ganar un premio material o económico.
- Aplicaciones que cuenten con elementos o funciones de navegación (como opciones de menú, pestañas, botones, vistas web, etc.) que proporcionen una "llamada a la acción" para apostar o participar en juegos, concursos o torneos usando dinero real; por ejemplo, aplicaciones que inviten a los usuarios con mensajes como "¡APUESTA!", "¡REGÍSTRATE!" o "¡COMPITE!" en un torneo a cambio de la posibilidad de ganar un premio en efectivo.
- Aplicaciones que acepten o gestionen apuestas, dinero de la aplicación, ganancias o depósitos para obtener o apostar por un premio material o económico.

Otras pruebas piloto de juegos con dinero real

Para descubrir posibles actualizaciones de la política "Otras aplicaciones de juegos, concursos y torneos con dinero real", Google Play está llevando a cabo pruebas durante tiempo limitado para los siguientes tipos de juegos en las regiones que se indican a continuación, sujeto a términos y condiciones adicionales:

Tipo de juego	Región	Periodo de prueba piloto	Cómo participar

Tipo de juego	Región	Periodo de prueba piloto	Cómo participar
Juegos de gancho online	Solo en Japón	Del 11 de julio del 2022 al 11 de julio del 2023	Haz clic aquí para hacer una solicitud
Fantasy sport diario/rummy	Solo en la India	Del 28 de septiembre del 2022 al 28 de septiembre del 2023	Haz clic aquí para hacer una solicitud

Programas de fidelización gamificados

En los casos en los que la ley lo permita y no estén sujetos a requisitos adicionales de licencias de juegos de apuestas o de otros juegos, admitimos programas de fidelización que recompensen a los usuarios con premios materiales reales o con un importe monetario equivalente, de acuerdo con los siguientes requisitos de Play Store que se deben cumplir:

Para todas las aplicaciones (las que son juegos y las que no son juegos):

- Los beneficios, ventajas o recompensas del programa de fidelización deben ser claramente suplementarios y estar claramente subordinados a cualquier transacción monetaria apta realizada en la aplicación (la transacción monetaria apta debe ser una transacción independiente genuina para ofrecer bienes o servicios de forma independiente al programa de fidelización). Además, no pueden estar sujetos a compras ni estar vinculados a ningún otro tipo de intercambio, ya que esto supondría una infracción de las restricciones de la política sobre Juegos de Apuestas, Juegos y Concursos con Dinero Real.
  - Por ejemplo, ninguna parte de la transacción monetaria apta puede constituir una comisión o una apuesta para participar en el programa de fidelización y la transacción monetaria apta no debe dar lugar a la compra de bienes o servicios a precios superiores a los habituales.

Para aplicaciones que son juegos :

- Los puntos de fidelidad o las recompensas con beneficios, ventajas o recompensas asociados a transacciones monetarias aptas solo se pueden otorgar y canjear con una proporción fija, que debe indicarse claramente en la aplicación y también dentro de las reglas oficiales del programa disponibles públicamente. Asimismo, los beneficios o ventajas que se puedan canjear **no** deben ser objeto de apuesta, ofrecerse como premio ni basarse en el rendimiento del usuario en el juego ni en el azar.

Para aplicaciones que no son juegos:

- Los puntos de fidelidad o las recompensas pueden estar vinculados a un concurso o al azar si se cumplen los requisitos que se indican a continuación. Los programas de fidelización con beneficios, ventajas o recompensas asociados a una transacción monetaria apta deben:
  - Publicar las reglas oficiales del programa en la aplicación.
  - En el caso de los programas con sistemas de recompensa variables, basados en el azar o aleatorizados: informar en sus términos oficiales 1) de las probabilidades de determinar recompensas que tienen los programas de fidelización que utilizan probabilidades fijas y 2) del método de selección (por ejemplo, las variables utilizadas para determinar la recompensa) de todos los demás programas de este tipo.
  - Especificar un número fijo de ganadores, el plazo límite de participación y la fecha de entrega del premio para cada promoción en los términos oficiales de cada programa que ofrezca sorteos, rifas u otras promociones similares.
  - Indicar cualquier proporción fija de acumulación y canje de puntos o recompensas de fidelidad de forma visible tanto en la aplicación como en los términos oficiales del programa.

Tipo de aplicación con programa de fidelización	Fidelización gamificada y recompensas variables	Recompensas de fidelización basadas en una proporción fija o una programación	Se requieren los Términos y Condiciones del programa de fidelización	Los Términos y Condiciones deben indicar las probabilidades o el método de selección en cualquier programa de fidelización basado en el azar
Aplicaciones que son juegos	No permitido	Permitido	Obligatorio	No procede (los programas de fidelización de las aplicaciones que son juegos no pueden incluir elementos basados en el azar)
Aplicaciones que no son juegos	Permitido	Permitido	Obligatorio	Obligatorio

Anuncios de juegos de apuestas o de juegos, concursos y torneos con dinero real insertados en las aplicaciones distribuidas por Play

Admitimos aplicaciones con anuncios de juegos de apuestas y juegos, concursos o torneos con dinero real siempre que cumplan los siguientes requisitos:

- La aplicación y el anuncio (así como los anunciantes) deben cumplir todas las leyes aplicables y los estándares del sector en todas las ubicaciones en las que se muestre el anuncio.
- El anuncio debe cumplir todos los requisitos aplicables de licencias de anuncios locales de todos los productos y servicios relacionados con juegos de apuestas que se promocionen.
- La aplicación no debe mostrar anuncios de juegos de apuestas a usuarios menores de 18 años.
- La aplicación no debe estar registrada en el programa Diseñado para Familias.
- La aplicación no debe estar orientada a usuarios menores de 18 años.
- Si se anuncia una aplicación de juegos de apuestas (tal y como se define más arriba), el anuncio debe mostrar claramente información sobre el juego responsable, ya sea en la página de destino, en la ficha de la aplicación que se anuncia o dentro de la propia aplicación.
- La aplicación no debe ofrecer contenido de juegos de apuestas simulados (por ejemplo, aplicaciones de casino sociales o aplicaciones con máquinas tragaperras virtuales).
- La aplicación no debe ofrecer funciones complementarias ni de asistencia para juegos de apuestas ni para juegos, loterías o torneos con dinero real (por ejemplo, funciones que ayuden con las apuestas, los pagos, el seguimiento de probabilidades, rendimiento o resultados deportivos, o con la gestión de fondos para jugar).
- El contenido de la aplicación no debe promocionar servicios de juegos de apuestas ni servicios de juegos, loterías o torneos con dinero real, ni dirigir a los usuarios a dichos servicios.

Solo las aplicaciones que cumplan todos estos requisitos indicados más arriba en esta sección pueden incluir anuncios de juegos de apuestas o de juegos, loterías o torneos con dinero real. Las aplicaciones de juegos de apuestas aceptadas (tal y como se definen arriba) o las aplicaciones de fantasy sport diarios (tal y como se definen más abajo) que cumplan los requisitos del 1 al 6 indicados arriba pueden incluir anuncios de juegos de apuestas o de juegos, loterías o torneos con dinero real.

Ejemplos de infracciones

- Una aplicación diseñada para usuarios menores de edad que muestre un anuncio donde se promocionen servicios de juegos de apuestas.
- Un juego de casino simulado que promocione casinos con dinero real o dirija a los usuarios a dichos casinos.
- Una aplicación de seguimiento de probabilidades deportivas que contenga anuncios de juegos de apuestas integrados donde se incluyan enlaces a un sitio web de apuestas deportivas.

- Aplicaciones con anuncios de juegos de apuestas que infrinjan nuestra política sobre publicidad engañosa, como anuncios que parezcan botones, iconos u otros elementos interactivos en la aplicación.

Aplicaciones de fantasy sport diarios

Solo permitimos aplicaciones de fantasy sport diarios, según la definición de la legislación local aplicable, si cumplen los siguientes requisitos:

- La aplicación debe distribuirse solo en Estados Unidos o debe cumplir los requisitos de las aplicaciones de juegos de apuestas y los procesos de solicitud mencionados anteriormente para el resto de países.
- El desarrollador debe completar correctamente el proceso de solicitud de fantasy sports diarios y dicha solicitud debe ser aceptada para distribuir la aplicación en Play.
- La aplicación debe cumplir todas las leyes aplicables y los estándares del sector de los países en los que se distribuya.
- La aplicación debe impedir que los usuarios menores de edad puedan apostar o realizar transacciones monetarias en la aplicación.
- La aplicación no debe estar disponible como aplicación de pago en Google Play ni utilizar la Facturación en Google Play por Compras en Aplicaciones.
- Debe ser gratis descargar e instalar la aplicación de Play Store.
- La aplicación debe estar clasificada como solo para adultos o un equivalente de la Coalición Internacional de Clasificación por Edad (IARC).
- La aplicación y su ficha deben mostrar información clara sobre cómo participar en juegos de apuestas de forma responsable.
- La aplicación debe cumplir todas las leyes aplicables y los estándares del sector de cualquier territorio o estado de EE. UU. en el que se distribuya.
- El desarrollador debe contar con una licencia válida en cada territorio o estado de EE. UU. en el que sea necesaria para distribuir aplicaciones de fantasy sport diarios.
- La aplicación debe impedir su uso en los territorios o estados de EE. UU. en los que el desarrollador no tenga la licencia obligatoria para distribuir aplicaciones de fantasy sport diarios.
- La aplicación debe impedir su uso en los territorios o estados de EE. UU. en los que las aplicaciones de fantasy sport diarios no sean legales.

Actividades ilegales

No se permiten las aplicaciones que faciliten o promocionen actividades ilegales.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Facilitar la venta o la compra de drogas ilegales.
- Representar o fomentar el consumo o la venta de drogas, alcohol o tabaco en menores de edad.
- Instrucciones para cultivar o elaborar drogas ilegales.

En vigor desde el 11 de octubre del 2022

Contenido generado por usuarios

El contenido generado por usuarios (CGU) es aquel que aportan los usuarios a una aplicación y que al menos un subconjunto de los usuarios puede ver o acceder a él.

Las aplicaciones que contienen o incluyen CGU, como las aplicaciones que sirven de navegador o cliente especializados para dirigir a los usuarios a una plataforma de CGU, deben implementar medidas firmes, eficaces y continuas de moderación de contenido con los siguientes requisitos:

- Requerir que los usuarios acepten los términos de uso o la política de usuarios de la aplicación antes de crear o subir CGU.
- Definir el contenido y los comportamientos inadecuados (de acuerdo con las Políticas del Programa para Desarrolladores de Google Play), así como prohibirlos en los términos de uso o en las políticas de usuarios de la aplicación.
- Llevar a cabo una moderación de CGU de forma razonable y continua, y de acuerdo con el tipo de CGU alojado por la aplicación.
  - En el caso de las aplicaciones de realidad aumentada (RA), la moderación de CGU (incluido el sistema de generación de informes de la aplicación) debe tener en cuenta tanto el CGU de RA que pueda ser inadecuado (por ejemplo, imágenes de RA sexualmente explícitas) como la ubicación anclada del contenido de RA sensible (por ejemplo, contenido de RA anclado a una zona restringida, como una base militar, o a una propiedad privada donde el anclaje de RA pueda causar problemas a su propietario).
- Ofrecer un sistema en la aplicación para denunciar CGU y usuarios inadecuados, y adoptar medidas contra el CGU o el usuario (si corresponde).
- Proporcionar un sistema en la aplicación para el bloqueo de CGU y usuarios.
- Implementar medidas para evitar que se obtengan ingresos derivados de fomentar el comportamiento inadecuado de los usuarios.

Contenido sexual fortuito

El contenido sexual se considera "fortuito" si aparece en una aplicación de CGU que (1) proporciona acceso a contenido principalmente no sexual y (2) no promueve ni recomienda activamente el contenido sexual. No se considera "fortuito" (y, por tanto, no se permite) ningún contenido sexual tipificado como ilegal en virtud de la ley aplicable ni tampoco ningún contenido que resulte peligroso para niños .

Las aplicaciones de CGU pueden incluir contenido sexual fortuito si se cumplen todos los requisitos que se enumeran a continuación:

- El contenido se oculta de forma predeterminada mediante filtros que requieren al menos dos acciones del usuario para inhabilitarlos por completo (por ejemplo, con un intersticial de ofuscación u ocultos de la vista de forma predeterminada, a menos que se inhabilite la "búsqueda segura").
- A los niños, según la definición de la Política de Familias , se les prohíbe explícitamente acceder a tu aplicación mediante filtros de edad, como una pantalla de edad neutral u otro sistema adecuado, según la definición de la ley aplicable.
- Tu aplicación proporciona respuestas precisas al cuestionario de clasificación del contenido sobre CGU, tal y como requiere la Política de Clasificaciones del Contenido .

Las aplicaciones cuyo fin principal sea incluir CGU inadecuado se retirarán de Google Play. Del mismo modo, se retirarán de Google Play las aplicaciones que se usen principalmente para alojar CGU inadecuado o que se hagan conocidas por alojar ese tipo de contenido.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Promocionar contenido de carácter sexual explícito generado por usuarios, lo que incluye la implementación de funciones de pago (o la autorización para usar estas funciones) que inciten principalmente a compartir contenido inadecuado.
- Aplicaciones con contenido generado por usuarios (CGU) que no dispongan de la suficiente protección frente a amenazas, hostigamiento o acoso, especialmente cuando las víctimas sean menores de edad.

- Publicaciones, comentarios o fotos dentro de una aplicación, cuyo objetivo principal sea acosar, atacar, ridiculizar a otra persona o abusar de ella.
- Aplicaciones que no resuelven las reclamaciones de los usuarios sobre contenido inaceptable.

Contenido y servicios relacionados con la salud

No permitimos aplicaciones que expongan a los usuarios a contenido y servicios relacionados con la salud que sean dañinos.

Si tu aplicación contiene o promociona contenido y servicios relacionados con la salud, debes asegurarte de que cumpla la legislación aplicable.

Medicamentos con receta

No admitimos aplicaciones que faciliten la venta ni la compra sin receta de medicamentos que necesiten prescripción médica.

Sustancias no aprobadas

Google Play no admite aplicaciones que promocionen o vendan sustancias no aprobadas, independientemente de que se afirme que son legales.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Todos los artículos de esta lista no exhaustiva de fármacos y suplementos prohibidos .
- Productos que contengan efedra.
- Productos que contengan gonadotropina coriónica humana (hCG) para perder o controlar el peso, o que se promocionen conjuntamente con esteroides anabolizantes.
- Suplementos alimenticios o elaborados con hierbas que contengan componentes activos farmacéuticos o peligrosos.
- Productos con declaraciones de propiedades saludables falsas o engañosas, incluyendo los que insinúan ser tan eficaces como un medicamento con receta o como las sustancias controladas.
- Productos que carecen de autorización gubernamental y cuya forma de comercialización indica que se pueden utilizar de forma segura o efectiva para prevenir, curar o tratar una determinada enfermedad o dolencia.
- Productos que hayan sido objeto de una acción o advertencia gubernamental o regulatoria.
- Productos cuya denominación resulte engañosa por su similitud con un fármaco o suplemento no aprobado o una sustancia controlada.

Para obtener más información sobre los fármacos y suplementos no aprobados o engañosos que monitorizamos, visita la página www.legitscript.com .

Desinformación sobre salud

No permitimos aplicaciones que contengan afirmaciones engañosas relacionadas con la salud y que contradigan el consenso médico existente o puedan causar daños a los usuarios.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Afirmaciones engañosas sobre las vacunas (por ejemplo, afirmar que las vacunas pueden alterar el ADN de las personas).
- Defensa de tratamientos dañinos y no aprobados.

- Defensa de otras prácticas relacionadas con la salud que sean dañinas, como las terapias de conversión de homosexuales.

Restricciones relacionadas con el COVID-19

Las aplicaciones deben cumplir los requisitos de las aplicaciones relacionadas con la enfermedad por coronavirus del 2019 (COVID-19) .

Funciones médicas

No admitimos aplicaciones que incluyan funciones médicas o relacionadas con la salud que sean engañosas o potencialmente dañinas. Por ejemplo, no admitimos las aplicaciones que afirman disponer de una función de oximetría que únicamente se basa en la aplicación. Las aplicaciones de oxímetro deben ser compatibles con hardware externo, wearables o sensores integrados en smartphones diseñados para admitir la función de oximetría. Estas aplicaciones compatibles también deben incluir dentro de los metadatos renuncias de responsabilidad que señalen que no se han diseñado para un uso médico, que se han creado exclusivamente para usarse como herramienta de fitness y bienestar, y que no son dispositivos médicos. También deben indicar adecuadamente el modelo de dispositivo o hardware compatible.

Pagos - Servicios clínicos

Las transacciones relacionadas con servicios clínicos regulados no deben usar el sistema de facturación de Google Play. Para obtener más información, consulta el artículo Entender la política de pagos de Google Play .

Datos de Salud conectada

Los datos a los que se accede a través de los Permisos de Salud conectada se consideran datos de usuario personales y sensibles, y están sujetos a la política de Datos de Usuario y a requisitos adicionales .

Propiedad intelectual

No admitimos aplicaciones ni cuentas de desarrolladores que vulneren los derechos de propiedad intelectual de terceros, incluidos secretos comerciales, patentes, marcas, derechos de autor y otros derechos de propiedad. Tampoco admitimos aplicaciones que animen o induzcan a infringir derechos de propiedad intelectual.

Responderemos a las notificaciones claras de infracción de los derechos de autor. Para obtener más información al respecto o presentar una solicitud basada en la DMCA, consulta los procedimientos relativos a los derechos de autor .

Para presentar una reclamación por la venta o promoción de productos falsificados en una aplicación, envía un aviso de falsificación .

Si eres el propietario de una marca comercial y crees que una aplicación de Google Play infringe tus derechos, te animamos a que te pongas en contacto directamente con el desarrollador para resolver el asunto. Si no llegáis a un acuerdo, envíanos una reclamación por uso de marca a través de este formulario .

Si tienes información por escrito que demuestre que puedes utilizar la propiedad intelectual de un tercero en tu aplicación o ficha de Play Store (por ejemplo, nombres de marcas, logotipos o recursos gráficos), ponte en contacto con el equipo de Google Play antes de enviar el contenido para asegurarte de que tu aplicación no resulte rechazada por infringir la propiedad intelectual.

Uso no autorizado de contenido protegido por derechos de autor

No admitimos aplicaciones que infrinjan derechos de autor. La modificación de contenido protegido por derechos de autor también constituye una infracción. Es posible que los desarrolladores deban

aportar una prueba de que disponen de los derechos necesarios para utilizar el contenido protegido.

Ten cuidado a la hora de usar contenido protegido por derechos de autor para mostrar las funciones de tu aplicación. En general, lo más seguro es crear contenido original.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

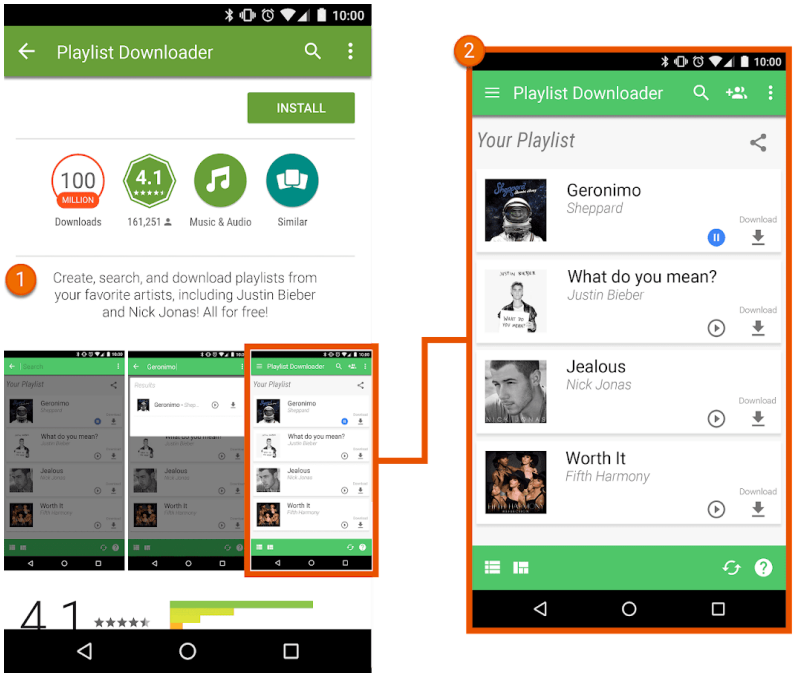
- Portadas de álbumes de música, videojuegos y libros
- Imágenes de marketing de películas, programas de TV y videojuegos
- Carátulas o imágenes de cómics, dibujos animados, películas, vídeos musicales o programas de TV
- Logotipos de equipos deportivos profesionales y universitarios
- Fotos publicadas en las cuentas de redes sociales de personajes públicos
- Imágenes profesionales de personajes públicos
- Reproducciones artísticas hechas por aficionados que resulten indistinguibles del contenido protegido por derechos de autor
- Aplicaciones que reproducen fragmentos de audio extraídos de contenido protegido por derechos de autor
- Traducciones o reproducciones completas de libros que no son de dominio público

Fomentar la infracción de derechos de autor

No admitimos aplicaciones que induzcan o animen a infringir derechos de autor. Antes de publicar tu aplicación, comprueba si contiene elementos que sí lo hagan y busca asesoramiento legal si es necesario.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones de streaming que permiten a los usuarios descargar una copia local de contenido protegido por derechos de autor sin autorización.
- Aplicaciones que animan a los usuarios a descargar o reproducir en streaming contenido protegido por derechos de autor, como música o vídeos, infringiendo así la ley aplicable sobre derechos de autor:



① La descripción incluida en la ficha de esta aplicación anima a los usuarios a descargar sin autorización contenido protegido por derechos de autor.
② La captura de pantalla incluida en la ficha de esta aplicación anima a los usuarios a descargar sin autorización contenido protegido por derechos de autor.

Infracción de derechos de marcas comerciales

No admitimos aplicaciones que infrinjan marcas comerciales 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 adquirida, el propietario obtiene derechos exclusivos sobre el uso de la marca comercial respecto a los productos o servicios en cuestión.

La infracción de marcas comerciales supone un uso inadecuado o no autorizado de una marca comercial idéntica o similar de tal forma que sea probable que provoque confusión respecto al origen de ese producto. Tu aplicación podrá suspenderse si utiliza marcas comerciales de un tercero de tal forma que sea probable que provoquen confusión.

Falsificación

No admitimos aplicaciones que vendan o promocionen productos falsificados. Un producto falsificado es aquel que contiene una marca o un logotipo iguales o muy difíciles de diferenciar de los de otra marca. Imitan las características de marca de un producto auténtico para hacerse pasar por él.

Privacidad, elementos engañosos y abuso de dispositivos

Nos comprometemos a proteger la privacidad de los usuarios y a ofrecerles un entorno seguro. Las aplicaciones engañosas, maliciosas o cuyo objetivo sea usar de forma abusiva o inadecuada las redes, los dispositivos o los datos personales están terminantemente prohibidas.

Datos de usuario

Debes ser transparente en lo relativo a cómo tratas los datos de los usuarios (por ejemplo, la información que proporcionan o que se recoge sobre ellos, incluyendo la información de los dispositivos). Por eso, debes incluir un aviso en el que se comunique si tu aplicación va a acceder, recoger, usar o compartir sus datos, así como limitar el uso de dichos datos a los fines especificados en dicho aviso. Además, si tu aplicación procesa datos personales y sensibles, debes cumplir los requisitos adicionales que se incluyen en la sección "Datos de usuario personales y sensibles". Estos requisitos de Google Play se suman a los requisitos prescritos en la legislación de protección de datos y privacidad aplicable. Si incluyes código de terceros (por ejemplo, SDKs) en tu aplicación, debes asegurarte de que el código de terceros que uses en tu aplicación cumpla las Políticas del Programa para Desarrolladores de Google Play.

En vigor desde el 11 de octubre del 2022

Datos de usuario personales y sensibles

Se consideran datos de usuario sensibles y personales, entre otros, la información personal identificable, los datos de pago y financieros, la información de autenticación, la agenda de contactos, los contactos, la ubicación del dispositivo , los datos relacionados con los SMS y las llamadas, los datos de Health Connect, el inventario del resto de las aplicaciones del dispositivo, el micrófono, la cámara y otros datos sensibles de uso o de los dispositivos. Si tu aplicación trata datos personales y sensibles de los usuarios, debes hacer lo siguiente:

- Recoger, usar, compartir y acceder a los datos de usuario personales y sensibles que se adquieran a través de la aplicación únicamente con los fines necesarios para proporcionar y mejorar las funciones de la aplicación (por ejemplo, funciones anunciadas a los usuarios que se mencionen y se

promocionen en la descripción de la aplicación en Google Play). Entre las formas de compartir datos de usuario personales y sensibles, se incluye el uso de SDKs o de otros servicios de terceros que hagan que los datos se transfieran a un tercero. Las aplicaciones que amplíen el uso de los datos de usuario personales y sensibles para publicar anuncios deben cumplir nuestra Política de Anuncios.

- Tratar todos los datos de usuario personales y sensibles de forma segura, y transmitirlos usando un sistema moderno de cifrado, como el protocolo HTTPS.
- Usar una solicitud de permiso de ejecución siempre que sea posible antes de acceder a los datos que tienes disponibles mediante los permisos de Android .
- No vender datos de usuario personales ni sensibles.

Requisitos de visibilidad de los avisos de divulgación y consentimiento

En los casos en los que los usuarios no puedan deducir de forma razonable que sus datos de usuario personales y sensibles vayan a ser necesarios para ofrecer o mejorar funciones o características de tu aplicación que cumplan las políticas necesarias (por ejemplo, si tu aplicación recoge datos en segundo plano), debes cumplir los siguientes requisitos:

Incluir un aviso en la aplicación en el que se indique cómo recoges, usas, compartes y accedes a los datos. El aviso de la aplicación:

- Debe incluirse dentro de la aplicación y no solo en la descripción o en un sitio web.
- Debe mostrarse durante el uso normal de la aplicación y no debe requerir que los usuarios accedan a un menú o a los ajustes.
- Debe describir los datos a los que accedes y que recoges.
- Debe explicar cómo se usarán y se compartirán los datos.
- No se puede incluir únicamente en una política de privacidad o en los términos del servicio.
- No se puede incluir con otros avisos que no estén relacionados con la recogida de datos personales y sensibles de los usuarios.

El aviso de la aplicación debe acompañar y preceder inmediatamente a una solicitud para obtener el consentimiento de los usuarios y, siempre que sea posible, a un permiso de ejecución asociado. No puedes recoger datos personales ni sensibles, ni tampoco acceder a ellos, hasta que el usuario dé su consentimiento. La solicitud de consentimiento de la aplicación:

- Debe presentar la ventana de consentimiento de forma clara e inequívoca.
- Debe solicitar una acción de confirmación del usuario (por ejemplo, tocar la opción de aceptar o marcar una casilla).
- No debe interpretar las acciones para salir del aviso (por ejemplo, tocar otra parte de la pantalla o pulsar el botón para volver o el botón de inicio) como un consentimiento.
- No debe usar mensajes que se cierren automáticamente o que caduquen para obtener el consentimiento del usuario.

Para cumplir los requisitos de la política, se recomienda tomar como modelo el siguiente formato de ejemplo de aviso destacado (cuando sea necesario):

- "[Esta aplicación] recoge/transmite/sincroniza/almacena [tipo de datos] para habilitar ['función'] [en qué circunstancias]".
- *Ejemplo: "Fitness Funds recoge datos de ubicación para habilitar la función de monitorización de tu actividad física, aunque la aplicación esté cerrada o no se esté usando. Los datos también se usan para mostrar anuncios".*
- *Ejemplo: "CallBuddy recoge datos de registros de llamadas para habilitar la función de organización de los contactos, aunque la aplicación no se esté usando".*

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Una aplicación que recoja la ubicación del dispositivo, pero que no incluya un aviso destacado para explicar qué función usa estos datos y/o informe sobre el uso de la aplicación en segundo plano.
- Una aplicación que incluya un permiso de ejecución para solicitar acceso a los datos **antes** de mostrar el aviso destacado donde se especifica para qué se usan los datos.
- Una aplicación que acceda al inventario de aplicaciones instaladas de un usuario y no trate estos datos como información personal o sensible sujeta a los requisitos de la Política de Privacidad, tratamiento de datos y visibilidad de los avisos de divulgación y consentimiento que se mencionan más arriba.
- Una aplicación que acceda a los datos del teléfono o la agenda de contactos de un usuario y no los trate como información sensible o personal sujeta a los requisitos de la Política de Privacidad, tratamiento de datos y visibilidad de los avisos de divulgación y consentimiento que se mencionan más arriba.
- Una aplicación que grabe la pantalla del usuario y no trate esta información como datos personales o sensibles sujetos a esta política.
- Una aplicación que recoja la ubicación del dispositivo y no explique de forma exhaustiva su uso y obtenga el consentimiento de acuerdo con los requisitos anteriores.
- Una aplicación que recoja permisos restringidos en segundo plano, incluyendo si los fines son de seguimiento, investigación o marketing, y no explique de forma exhaustiva su uso y obtenga el consentimiento de acuerdo con los requisitos anteriores.

Restricciones de acceso a datos personales y sensibles

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

Actividad	Requisito
Tu aplicación gestiona datos de pago, información financiera o números de identificación emitidos por el gobierno de un país.	Tu aplicación no debe revelar públicamente datos de usuario personales ni sensibles que contengan información financiera, datos de pago o números de documentos de identificación oficial.
Tu aplicación gestiona agendas telefónicas o información de contacto que no son públicos.	No se permite la divulgación o la publicación de información de los contactos privados de los usuarios sin autorización.
Tu aplicación incluye funciones de seguridad, como funciones antivirus o de eliminación de software malicioso.	Tu aplicación debe publicar una política de privacidad y avisos en la aplicación para explicar qué datos de usuario recoge y transmite, cómo se utilizan y con quién se comparten.
Tu aplicación va dirigida a niños.	Tu aplicación no debe incluir ningún SDK que no esté aprobado para su uso en servicios dirigidos a niños. Consulta el texto completo de la política y los requisitos en el artículo Crear aplicaciones para niños y familias .
Tu aplicación recoge o vincula identificadores de dispositivos persistentes (por ejemplo, IMEI, IMSI, número de serie de SIM, etc.).	Los identificadores de dispositivos persistentes no deben vincularse a otros datos de usuario personales ni sensibles o identificadores de dispositivo que se puedan cambiar, salvo en los siguientes casos: • Telefonía asociada a una SIM (por ejemplo, llamadas por Wi-Fi vinculadas a una cuenta de operador). • Aplicaciones de gestión de dispositivos empresariales que usen el modo de propietario del dispositivo. Estos usos deben indicarse a los usuarios de forma destacada tal como se especifica en la Política de Datos de Usuario . Consulta este artículo para obtener más información sobre los identificadores únicos alternativos. Lee la Política de Anuncios para consultar más directrices sobre el ID de publicidad de Android.

Sección Seguridad de los datos

Todos los desarrolladores deben incluir en todas las aplicaciones una sección "Seguridad de los datos" clara y precisa, donde se explique cómo se recogen, se usan y se comparten los datos de usuario. El desarrollador es responsable de la precisión de la etiqueta y de que esta información esté actualizada. Si procede, esta sección debe estar en consonancia con los avisos incluidos en la política de privacidad de la aplicación.

Consulta este artículo para ver más información sobre cómo completar la sección Seguridad de los datos.

Política de privacidad

Todas las aplicaciones deben publicar un enlace a su política de privacidad en el campo correspondiente de Play Console, así como un enlace a la política de privacidad o el texto en sí dentro de la propia aplicación. La política de privacidad y los avisos que aparezcan en la aplicación deben explicar de forma exhaustiva el modo en el que tu aplicación accede a los datos de usuario y los recoge, utiliza y comparte, sin limitarse a los datos incluidos en el aviso de la etiqueta de privacidad. Esta información debe incluir lo siguiente:

- Información del desarrollador y un punto de contacto para informarse sobre temas de privacidad o un mecanismo para enviar consultas.
- Los tipos de datos de usuario personales y sensibles a los que tu aplicación accede, recoge, utiliza y comparte, y los terceros con los que se comparten datos de usuario personales o sensibles.
- Los procedimientos seguros que se utilizan para tratar los datos de usuario personales y sensibles.
- La política de conservación y eliminación de datos que aplica el desarrollador.
- Un nombre que indique claramente que se trata de una política de privacidad (por ejemplo, utilizando la expresión "política de privacidad" en el título).

La entidad (por ejemplo, el desarrollador o la empresa) especificada en la ficha de Google Play Store de la aplicación debe figurar en la política de privacidad, o la política de privacidad debe nombrar la aplicación. Las aplicaciones que no accedan a datos de usuario personales ni sensibles también deben enviar una política de privacidad.

Tu política de privacidad debe estar disponible en una URL activa, accesible públicamente y sin geoperimetraje (no se admite el formato PDF), y no debe ser modificable.

Uso del ID definido en las aplicaciones

Android introducirá un nuevo ID para cubrir casos de uso esenciales, como analíticas y prevención de fraudes. A continuación se indican los términos de uso de este ID.

- **Uso:** el ID definido en las aplicaciones no se debe usar para personalizar ni medir anuncios.
- **Asociación a información personal identificable u otros identificadores:** el ID definido en las aplicaciones no debe estar conectado a ningún identificador de Android (por ejemplo, AAID), ni a otros datos personales y sensibles, con fines publicitarios.
- **Transparencia y consentimiento:** los usuarios deben estar informados sobre la recogida del identificador definido en las aplicaciones y su uso, así como sobre el cumplimiento de estos términos, a través de un aviso de privacidad adecuado de carácter legal que incluya tu política de privacidad. Debes obtener un consentimiento con validez legal de los usuarios cuando sea necesario. Para obtener más información sobre nuestros estándares de privacidad, consulta nuestra Política de Datos de Usuario .

EU-U.S. Privacy Shield (Escudo de la privacidad UE-EE. UU.) y Swiss-U.S. Privacy Shield (Escudo de la privacidad Suiza-EE. UU.)

Si utilizas o procesas información personal facilitada por Google, o accedes a ella, y esta información identifica de forma directa o indirecta a un individuo y tiene su origen en la Unión Europea o Suiza (en adelante, "Información Personal de la UE"), deberás:

- Cumplir todas las normativas, leyes, directivas y reglas aplicables sobre privacidad, seguridad y protección de datos.
- Utilizar, procesar o acceder a la Información Personal de la UE únicamente con los fines que se incluyen en el consentimiento otorgado por el usuario en cuestión.
- Implementar las medidas técnicas y de organización adecuadas para evitar la pérdida, el uso inadecuado, la divulgación, la alteración o la destrucción de la Información Personal de la UE, así como el acceso ilegítimo o no autorizado a dicha información.
- Proporcionar el mismo nivel de protección que se exige en los principios del marco Privacy Shield (Escudo de la privacidad).

Debes comprobar periódicamente que se cumplen estas condiciones. Si en algún momento no puedes cumplirlas (o si existe un riesgo significativo de que no puedas hacerlo en el futuro), debes avisarnos inmediatamente enviando un correo a la dirección data-protection-office@google.com . Además, debes dejar de procesar la Información Personal de la UE o tomar las medidas apropiadas y razonables para recuperar un nivel de protección adecuado de inmediato.

Desde el 16 de julio del 2020, Google ya no se basa en el marco EU-U.S. Privacy Shield (Escudo de la privacidad UE-EE. UU.) para transferir datos personales procedentes del Espacio Económico Europeo o del Reino Unido a Estados Unidos. Consulta más información. Puedes obtener más información en la sección 9 de la atribución basada en datos.

Permisos y APIs que acceden a información sensible

Las solicitudes de permisos y las APIs que acceden a información sensible deben resultar comprensibles para los usuarios. Solo puedes solicitar los permisos y las APIs que acceden a información sensible que sean necesarios para implementar en tu aplicación las funciones o los servicios que promociones en tu ficha de Google Play Store. No puedes usar permisos y APIs que accedan a información sensible y proporcionen acceso a datos de usuario o de dispositivos en relación con fines o funciones que no hayas especificado, no hayas implementado o no estén permitidos. No puedes vender en ningún caso los datos sensibles o personales a los que tengas acceso mediante permisos o APIs que acceden a información sensible.

Solicita permisos y APIs que accedan a información sensible para acceder a datos en contexto (mediante solicitudes incrementales), de manera que los usuarios comprendan el motivo por el que tu aplicación requiere esos permisos. Usa los datos únicamente con los fines para los cuales los usuarios hayan dado su consentimiento. Si más adelante quieres usar los datos con otros fines, debes pedir a los usuarios que den su consentimiento y accedan a estos nuevos usos.

Permisos restringidos

Además de lo expuesto más arriba, los permisos restringidos son permisos clasificados con los tipos Peligroso , Especial , De firma , o los que se indican a continuación. Estos permisos están sujetos a los siguientes requisitos y restricciones adicionales:

- Los datos sensibles de usuario o del dispositivo a los que se accede a través de Permisos Restringidos solo se pueden compartir con terceros si es necesario para proporcionar o mejorar funciones o servicios actuales de la aplicación de la que se hayan recogido los datos. También puedes compartir los datos necesarios para cumplir las leyes aplicables o como parte de una fusión, adquisición o venta de activos siempre que hayas informado a los usuarios de forma legalmente pertinente. No se permite compartir o vender los datos de usuario de cualquier otra forma.
- Respeta las decisiones de los usuarios si rechazan una solicitud de permisos restringidos. Además, no se puede manipular o forzar a los usuarios para que den su consentimiento a cualquier permiso que no sea esencial. Debes adaptarte en la medida de lo posible a los usuarios que no otorguen acceso a los permisos sensibles (por ejemplo, permitiendo a un usuario que introduzca un número de teléfono de forma manual si se ha restringido el acceso a los registros de llamadas).

- Se prohíbe expresamente el uso de permisos de forma que entren en conflicto con las prácticas recomendadas de permisos de aplicaciones para desarrolladores de Android o que infrinjan las políticas actuales (incluido el Abuso de Privilegios Avanzados).

Es posible que algunos permisos restringidos estén sujetos a requisitos adicionales detallados más adelante. El objetivo de estas restricciones es proteger la privacidad de los usuarios. Es posible que hagamos excepciones en casos limitados en los que las aplicaciones proporcionen una función esencial o de gran interés y no haya ningún método alternativo para ofrecer esa función. Evaluamos las excepciones propuestas teniendo en cuenta el impacto potencial en 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 de usuario sensibles y personales sujetos a la política Información personal y sensible y a los siguientes requisitos:

Permiso restringido	Requisito
Grupo de permisos de registro de llamadas (p. ej., READ_CALL_LOG, WRITE_CALL_LOG o PROCESS_OUTGOING_CALLS)	Tu aplicación debe estar registrada de forma activa como controlador predeterminado del teléfono o asistencia en el dispositivo.
Grupo de permisos de SMS (p. ej., READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH o RECEIVE_MMS)	Tu aplicación debe estar registrada de forma activa como controlador predeterminado de SMS o asistencia en el dispositivo.

Las aplicaciones que no tengan la función de controlador predeterminado de SMS, teléfono o asistencia no podrán declarar el uso de estos permisos en su archivo de manifiesto. Esto incluye texto de marcador de posición en el manifiesto. Además, estas aplicaciones deben estar registradas como controladores predeterminados de SMS, teléfono o asistencia para solicitar a los usuarios que acepten cualquiera de estos permisos. Asimismo, deben dejar de usar los permisos inmediatamente si dejan de actuar como controladores predeterminados. Puedes consultar los usos permitidos y las excepciones en esta página del Centro de Ayuda .

Las aplicaciones solo pueden utilizar un permiso (y los datos derivados de él) para ofrecer funciones principales aprobadas. La función principal de una aplicación es su objetivo principal. Puede incluir un conjunto de funciones principales, que deben estar claramente documentadas y promocionadas en la descripción de la aplicación. Sin estas funciones, la aplicación no funcionará. Solo se deben transferir, compartir o usar con licencia estos datos para ofrecer funciones o servicios principales de la aplicación, y no se deben usar con otros fines (p. ej., mejorar otros servicios o aplicaciones, mostrar publicidad o marketing). No se pueden usar métodos alternativos (como otros permisos, APIs o fuentes de terceros) para obtener datos atribuidos a los permisos relacionados con los SMS o el registro de llamadas.

Permisos de ubicación

La ubicación del dispositivo se considera un dato de usuario personal y sensible sujeto a las políticas Información Personal y Sensible y Ubicación en Segundo Plano, así como a los siguientes requisitos:

- Las aplicaciones no pueden acceder a los datos protegidos por los permisos de ubicación (por ejemplo, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION o ACCESS_BACKGROUND_LOCATION) una vez que dejan de ser necesarios para proporcionar las funciones o servicios de tu aplicación.
- Nunca debes solicitar permisos de ubicación de los usuarios con el único objetivo de realizar tareas de publicidad o análisis. Las aplicaciones que extiendan el uso permitido de estos datos para publicar anuncios deben cumplir nuestra Política de Anuncios .

- Las aplicaciones deben solicitar el nivel mínimo necesario de acceso a la ubicación (es decir, aproximado en lugar de exacto y en primer plano en lugar de en segundo plano) para proporcionar la función o el servicio que solicita la ubicación, y los usuarios deben esperar de forma razonable que la función o el servicio necesite el nivel de ubicación solicitado. Por ejemplo, podemos rechazar las aplicaciones que solicitan o acceden a la ubicación en segundo plano sin una justificación de peso.
- La ubicación en segundo plano solo se puede utilizar para proporcionar funciones beneficiosas para el usuario que sean pertinentes para la función principal de la aplicación.

Se permite que las aplicaciones accedan a la ubicación mediante el permiso de servicios en primer plano (cuando la aplicación solo tiene acceso en primer plano; por ejemplo, "mientras esté en uso") si el uso:

- Se inició como consecuencia de una acción iniciada por el usuario en la aplicación.
- Se cancela inmediatamente después de que la aplicación complete el caso de uso previsto de la acción que ha iniciado el usuario.

Las aplicaciones diseñadas específicamente para niños deben cumplir la política del programa Diseñado para Familias .

Para obtener más información sobre los requisitos de la política, consulta este artículo de ayuda .

Permiso de acceso a todos los archivos

Los archivos y los atributos de directorio del dispositivo de un usuario se consideran datos personales y sensibles sujetos a la política Información Personal y Sensible y a los siguientes requisitos:

- Las aplicaciones solo pueden solicitar acceso al almacenamiento del dispositivo si es fundamental para que funcionen. No pueden solicitar acceso al almacenamiento del dispositivo en nombre de ningún tercero por ningún motivo que no esté relacionado con las funciones esenciales de la aplicación de cara al usuario.
- Los dispositivos Android que ejecuten R o una versión posterior necesitarán el permiso MANAGE_EXTERNAL_STORAGE para gestionar el acceso en el almacenamiento compartido. Todas las aplicaciones orientadas a R y que soliciten un acceso amplio al almacenamiento compartido ("Acceso a todos los archivos") deben superar una revisión de acceso adecuada antes de su publicación. Las aplicaciones que puedan usar este permiso deben indicar claramente a los usuarios que habiliten la opción "Acceso a todos los archivos" de la sección "Acceso especial de aplicaciones". Para obtener más información sobre los requisitos de R, consulta este artículo de ayuda .

Permiso de visibilidad de paquetes (aplicaciones)

El inventario de aplicaciones instaladas que se consulta desde un dispositivo se considera como datos de usuario personales y sensibles sujetos a la política de Información Personal y Sensible y a los siguientes requisitos:

Las aplicaciones cuya finalidad principal sea iniciar y buscar otras aplicaciones del dispositivo, o interactuar con ellas, pueden obtener una visibilidad de otras aplicaciones instaladas en el dispositivo acorde con su alcance, como se indica a continuación:

- **Visibilidad general de las aplicaciones:** la visibilidad general es la capacidad de obtener una visibilidad amplia (o "general") de las aplicaciones instaladas ("paquetes") en el dispositivo.
  - En el caso de las aplicaciones orientadas al nivel de API 30 o posterior , la visibilidad general de las aplicaciones instaladas mediante el permiso QUERY_ALL_PACKAGES queda restringida a casos prácticos específicos en los que el conocimiento de alguna o de todas las aplicaciones del dispositivo o la interoperabilidad con ellas sea necesaria para que la aplicación funcione.
    - No puedes usar QUERY_ALL_PACKAGES si tu aplicación puede funcionar con una declaración de visibilidad de paquetes más específica y acorde con su alcance (por ejemplo, mediante

consultas e interacciones con paquetes específicos en lugar de solicitar visibilidad general).
  - El uso de métodos alternativos para aproximarse al nivel de visibilidad general asociado al permiso QUERY_ALL_PACKAGES también se restringe a la función principal de la aplicación dirigida al usuario y a su interoperabilidad con las aplicaciones detectadas mediante este método.
  - Puedes consultar este artículo del Centro de Ayuda para ver casos prácticos de uso permitido del permiso QUERY_ALL_PACKAGES.
- **Visibilidad limitada de las aplicaciones:** la visibilidad limitada consiste en que la aplicación minimiza el acceso a los datos efectuando consultas a aplicaciones específicas usando métodos más limitados (en lugar de "generales"), como hacer consultas a aplicaciones específicas que cumplan la declaración del archivo de manifiesto de la aplicación. Puedes utilizar este método para hacer consultas a aplicaciones en los casos en los que la interoperabilidad o la gestión de esas aplicaciones por parte de tu aplicación cumpla nuestras políticas.
- La visibilidad del inventario de aplicaciones instaladas en un dispositivo debe estar directamente relacionada con el propósito principal o con la función principal a los que los usuarios acceden en tu aplicación.

Los datos de inventario de aplicaciones consultados desde aplicaciones distribuidas por Play no se pueden vender ni compartir para analíticas ni para la obtención de ingresos por publicidad.

API Accessibility

La API Accessibility no se puede usar para:

- Cambiar la configuración del usuario sin su permiso o evitar que los usuarios inhabiliten o desinstalen cualquier aplicación o servicio, a menos que lo autorice el padre, la madre o un tutor a través de una aplicación de controles parentales, o bien los administradores autorizados a través de un software de gestión para empresas.
- Eludir los controles y las notificaciones de privacidad integrados de Android.
- Modificar o aprovechar la interfaz de usuario de forma que resulte engañosa o infrinja las Políticas para Desarrolladores de Google Play de cualquier otra forma.

La API Accessibility no se ha diseñado para grabar el audio de llamadas remotas y no se puede solicitar con dicho fin.

El uso de la API Accessibility debe documentarse en la ficha de Google Play.

Directrices para IsAccessibilityTool

Las aplicaciones cuya función principal sea ayudar directamente a personas con discapacidades pueden optar a usar **IsAccessibilityTool** para que se puedan clasificar públicamente como aplicaciones de accesibilidad.

Las aplicaciones que no puedan usar **IsAccessibilityTool** tampoco podrán utilizar el distintivo de aplicación de accesibilidad. Además, deberán cumplir los requisitos de aviso y consentimiento destacados (incluidos en la Política de Datos de Usuario), ya que las funciones relacionadas con la accesibilidad no serán evidentes para los usuarios. Para obtener más información, consulta el artículo sobre la API AccessibilityService en el Centro de Ayuda.

Las aplicaciones deben usar APIs y permisos más restrictivos en lugar de la API Accessibility cuando sea posible para lograr la funcionalidad deseada.

Permiso Solicitar instalación de paquetes

El permiso REQUEST_INSTALL_PACKAGES permite que la aplicación solicite la instalación de paquetes de aplicaciones. Para usar este permiso, la función principal de tu aplicación debe permitir:

- Enviar o recibir paquetes de aplicaciones.
- Habilitar la instalación iniciada por el usuario de paquetes de aplicaciones.

Entre las funcionalidades permitidas se incluyen las siguientes:

- Navegación o búsqueda web.
- Servicios de comunicación que admiten archivos adjuntos.
- Compartir, transferir o gestionar archivos.
- Gestión de dispositivos empresariales.
- Copia de seguridad y restauración.
- Migración entre dispositivos o cambio de teléfono.

La función principal es el objetivo fundamental de la aplicación, y tanto la función principal como cualquier característica esencial que esta última incluya deben documentarse y promocionarse de forma destacada en la descripción de la aplicación.

El permiso REQUEST_INSTALL_PACKAGES no debería usarse para hacer actualizaciones automáticas ni modificaciones, ni tampoco para crear paquetes de otros APKs en el archivo de recursos, salvo que sea con fines de gestión de dispositivos. Todas las actualizaciones o instalaciones de paquetes deben cumplir la política Abuso de dispositivos y redes de Google Play, y las debe iniciar y controlar el usuario.

Permisos de Health Connect by Android

Los datos a los que se accede a través de los Permisos de Health Connect se consideran datos de usuario personales y sensibles, y están sujetos a la política de Datos de Usuario y a los siguientes requisitos:

Acceso y uso adecuados de Health Connect

Las solicitudes de acceso a los datos a través de Health Connect deben ser claras y comprensibles. Health Connect solo puede usarse de acuerdo con las políticas, los términos y condiciones aplicables, y para los usos aprobados, tal como se establece en esta política. Esto quiere decir que solo podrás solicitar acceso a los permisos cuando tu aplicación o servicio cumpla uno de los usos aprobados.

Los usos aprobados para acceder a los Permisos de Health Connect son los siguientes:

- Aplicaciones o servicios con una o más funciones que benefician la salud y el estado físico de los usuarios a través de una interfaz de usuario que les permite **registrar, informar, supervisar o analizar** directamente su actividad física, el sueño, el bienestar mental, la nutrición, las medidas de salud, las descripciones físicas u otras descripciones y medidas relacionadas con la salud o el estado físico.
- Aplicaciones o servicios con una o más funciones que benefician la salud y el estado físico de los usuarios a través de una interfaz de usuario que les permite **almacenar** su actividad física, el sueño, el bienestar mental, la nutrición, las medidas de salud, las descripciones físicas u otras descripciones y medidas relacionadas con la salud o el estado físico en su teléfono o wearable, así como compartir sus datos con otras aplicaciones en el dispositivo que cumplan estos casos.

Health Connect es una plataforma de uso general para almacenar y compartir datos que permite a los usuarios añadir datos de salud y estado físico desde diferentes fuentes de su dispositivo Android y compartirlos con terceros a su elección. Estos datos pueden proceder de diversas fuentes, según establezcan los usuarios. Los desarrolladores deben evaluar si Health Connect es adecuado para su uso previsto y para investigar y examinar la fuente y la calidad de los datos de Health Connect relacionados con cualquier objetivo y, en particular, los de uso de investigación, de salud o médico.

- Las aplicaciones que realicen investigaciones de salud en humanos usando los datos obtenidos de Health Connect deben tener el consentimiento de los participantes o, en el caso de menores, de sus padres o tutores. Dicho consentimiento debe incluir: a) la naturaleza, el objetivo y la duración de la investigación; b) los procedimientos, los riesgos y los beneficios para el participante; c) la información sobre la confidencialidad y el tratamiento de los datos (incluida la posibilidad de compartirlos con terceros); d) una persona de contacto para las dudas del participante; y e) el proceso de desistimiento. Las aplicaciones que realicen investigaciones de salud en humanos

usando los datos obtenidos de Health Connect deben recibir la aprobación de una junta independiente para 1) proteger los derechos, la seguridad y el bienestar de los participantes y 2) tener la capacidad de escrutar, modificar y aprobar las investigaciones realizadas en humanos. Se debe proporcionar una prueba de dicha aprobación en el momento de la solicitud.

- Además, es responsabilidad tuya asegurar el cumplimiento de cualquier requisito normativo o legal que pueda aplicarse según el uso previsto de Health Connect y de cualquier dato de Health Connect. Google no respalda el uso ni garantiza la precisión de los datos contenidos en Health Connect para ningún uso o fin, en particular, para usos de investigación, de salud o médicos, salvo que se indique explícitamente en el etiquetado o en la información proporcionada por Google para productos o servicios específicos de Google. Google renuncia a todas las responsabilidades relacionadas con el uso de los datos obtenidos a través de Health Connect.

Uso Limitado

Además de utilizar Health Connect para un uso adecuado, el uso que hagas de los datos a los que accedas a través de Health Connect debe cumplir los requisitos que se indican abajo. Estos requisitos se aplican a los datos sin procesar obtenidos de Health Connect y a los datos agregados, desidentificados o derivados de los datos sin procesar.

- Limitar el uso de los datos de Health Connect a ofrecer o mejorar el uso adecuado o las funciones que sean visibles y destacadas en la interfaz de usuario de la aplicación solicitante.
- Transferir datos de usuario a terceros solo:
  - Para ofrecer o mejorar el uso adecuado o las funciones que sean claras desde la interfaz de usuario de la aplicación solicitante y solo con el consentimiento del usuario.
  - Si es necesario por motivos de seguridad (por ejemplo, para investigar un abuso).
  - Para cumplir las leyes o normativas aplicables.
  - Como parte de una fusión, adquisición o venta de recursos del desarrollador tras obtener el consentimiento previo explícito del usuario.
- No permitir que los humanos lean los datos de usuario a menos que:
  - Se haya obtenido el consentimiento explícito del usuario para leer datos específicos.
  - Sea necesario por motivos de seguridad (por ejemplo, para investigar un abuso).
  - Se haga para cumplir las leyes aplicables.
  - Los datos (incluidas las derivaciones) se agreguen y usen en operaciones internas de acuerdo con la privacidad aplicable y otros requisitos legales de tu jurisdicción.

Se prohíbe cualquier otra transferencia, uso o venta de los datos de Health Connect, incluidas las siguientes:

- Transferencia o venta de datos de usuario a terceros, como plataformas publicitarias, agentes de datos o cualquier distribuidor de información.
- Transferencia, venta o uso de datos de usuario para la publicación de anuncios, incluidos los personalizados o basados en intereses.
- Transferencia, venta o uso de datos de usuario para determinar la solvencia o con fines de préstamo.
- Transferencia, venta o uso de datos de usuario con cualquier producto o servicio que pueda calificarse como dispositivo médico de acuerdo con la Sección 201(h) de la ley federal de alimentos, medicamentos y cosméticos de EE. UU. (Federal Food Drug & Cosmetic Act) en caso de que el dispositivo médico use los datos de usuario para desempeñar su función regulada.
- Transferencia, venta o uso de datos de usuario para cualquier fin o de cualquier manera que esté relacionada con información médica protegida (según la HIPAA) a menos que recibas una aprobación previa por escrito de Google para tal uso.

El acceso a Health Connect no puede infringir esta política u otros términos y condiciones o políticas aplicables de Health Connect, lo que incluye los siguientes fines:

- No uses Health Connect en el desarrollo de aplicaciones, entornos o actividades, o para su incorporación en estas, donde el uso o el error de Health Connect pueda razonablemente suponer la muerte, lesiones personales o daños medioambientales o materiales (como la creación o el funcionamiento de instalaciones nucleares, el control del tráfico aéreo, los sistemas de soporte vital o las armas).
- No accedas a los datos obtenidos a través de Health Connect usando aplicaciones sin interfaz gráfica. Las aplicaciones deben mostrar un icono claramente identificable en la bandeja de aplicaciones, en los ajustes de la aplicación en el dispositivo, en los iconos de notificación, etc.
- No uses Health Connect con aplicaciones que sincronicen los datos entre dispositivos o plataformas no compatibles.
- Health Connect no se puede conectar a aplicaciones, servicios o funciones que estén dirigidas únicamente a niños. Health Connect no está aprobado para su uso en servicios principalmente dirigidos a niños.

Debes publicar en tu aplicación o en el sitio web de tu aplicación o servicio web una declaración afirmativa de que tu uso de los datos de Health Connect cumple las restricciones de Uso Limitado, por ejemplo, un enlace a la página principal de una página específica o una política de privacidad en la que se lea lo siguiente: "El uso de la información recibida de Health Connect cumplirá la Política de Permisos de Health Connect, incluidos los requisitos de Uso Limitado".

Acceso mínimo a los datos

Solo debes solicitar acceso a permisos que son críticos para implementar las funciones de tu aplicación o servicio.

Por lo tanto:

- No solicites acceso a información que no necesites. Solicita acceso solo a los permisos que sean necesarios para implementar las funciones o los servicios de tu producto. No debes solicitar acceso a permisos específicos que tu producto no necesite.

Información y control transparentes y precisos

Health Connect trata datos de salud y estado físico, lo que incluye información personal y sensible. Todas las aplicaciones y servicios deben contener una política de privacidad, donde se debe explicar de forma exhaustiva cómo tu aplicación o servicio recoge, usa y comparte los datos de usuario. Esto incluye los tipos de terceros con los que se comparten los datos de usuario, cómo usas los datos, los almacenas y los proteges, y qué pasa con ellos cuando una cuenta se desactiva o se elimina.

Además de los requisitos establecidos por la ley aplicable, debes cumplir los siguientes:

- Debes incluir un aviso en el que se indique cómo accedes, recoges, usas y compartes los datos. El aviso:
  - Debe representar de forma precisa la identidad de la aplicación o servicio que busca acceder a los datos de usuario.
  - Debe proporcionar información clara y precisa que explique los tipos de datos a los que se accede, se solicitan o se recogen.
  - Debe explicar cómo se usarán o compartirán los datos: si solicitas datos por un motivo, pero también se usarán para otro secundario, debes notificar a los usuarios de ambos usos.
- Debes proporcionar documentación de ayuda al usuario que explique cómo los usuarios pueden gestionar y eliminar sus datos de tu aplicación.

Tratamiento de datos de forma segura

Debes tratar todos los datos de usuario de una forma segura. Adopta medidas razonables y adecuadas para proteger todas las aplicaciones o sistemas que hacen uso de Health Connect contra el acceso, el uso, la destrucción, la pérdida, la alteración o la divulgación no autorizados o ilegales.

Entre las prácticas de seguridad recomendadas se encuentran la implementación y el mantenimiento de un sistema de gestión de seguridad de la información como el descrito en la norma ISO/IEC 27001 y la garantía de que tu aplicación o servicio web es sólido y no tiene problemas de seguridad, tal como se describe en OWASP Top 10.

En función de la API a la que se acceda y el número de usuarios, pediremos que tu aplicación o servicio se someta a una evaluación de seguridad periódica y que obtenga el certificado correspondiente de un tercero designado si tu producto transfiere datos fuera del propio dispositivo del usuario.

Para obtener más información sobre los requisitos para las aplicaciones que se conecten a Health Connect, consulta este artículo de ayuda.

En vigor desde el 1 de noviembre del 2022

Servicio de VPN

VpnService es una clase base que permite que las aplicaciones amplíen y desarrollen sus propias soluciones de VPN. Solo las aplicaciones que usen VpnService y cuya función principal sea proporcionar servicios de VPN pueden crear un túnel seguro a nivel del dispositivo hasta un servidor remoto. Sin embargo, hay algunas excepciones, entre las que se incluyen las aplicaciones que necesitan un servidor remoto para realizar su función principal. A continuación se indican algunos ejemplos:

- Aplicaciones de controles parentales y gestión empresarial.
- Aplicaciones de seguimiento de uso.
- Aplicaciones de seguridad de dispositivos (por ejemplo, antivirus, gestión de dispositivos móviles o cortafuegos).
- Herramientas relacionadas con redes (por ejemplo, aplicaciones de acceso remoto).
- Aplicaciones de navegación web.
- Aplicaciones del operador que requieren el uso de funciones de VPN para proporcionar servicios de telefonía o conectividad.

VpnService no se puede usar para:

- Recoger datos de usuarios personales y sensibles sin aviso destacado y consentimiento.
- Redirigir o manipular el tráfico de usuarios desde otras aplicaciones en un dispositivo para obtener ingresos (por ejemplo, redirigir el tráfico de los anuncios a través de un país diferente al del usuario).
- Manipular anuncios que puedan repercutir en la monetización de las aplicaciones.

Las aplicaciones que utilicen VpnService deben:

- Documentar el uso de VpnService en la ficha de Google Play.
- Cifrar los datos desde el dispositivo hasta el destino del túnel de VPN.
- Respetar todas las Políticas del Programa para Desarrolladores , incluidas las políticas de Fraude publicitario , Permisos y Software malicioso .

En vigor desde el 31 de julio del 2023

Permiso de alarma exacta

Se incorporará un nuevo permiso, USE_EXACT_ALARM, que dará acceso a la función de alarma exacta en las aplicaciones, a partir de Android 13 (nivel de API de destino: 33).

USE_EXACT_ALARM es un permiso restringido y las aplicaciones solo deben declarar este permiso si su función principal requiere una alarma exacta. Las aplicaciones que soliciten este permiso

restringido estarán sujetas a revisión y, si no cumplen los criterios de uso aceptable, no se podrán publicar en Google Play.

Usos aceptables para el permiso de alarma exacta

Tu aplicación solo debe utilizar la función USE_EXACT_ALARM si la función o el propósito principal de tu aplicación para el usuario requiere acciones con pautas de tiempo precisas, como en los casos siguientes:

- Se trata de una aplicación de alarma o temporizador.
- Se trata de una aplicación de calendario que muestra notificaciones de eventos.

Si tu aplicación hace un uso de la función de alarma exacta que no se ajusta a los casos mencionados anteriormente, te recomendamos que evalúes la conveniencia de utilizar SCHEDULE_EXACT_ALARM como opción alternativa.

Para obtener más información sobre la función de alarma exacta, consulta esta guía para desarrolladores .

Uso inadecuado de dispositivos y redes

No admitimos aplicaciones que interfieran de forma no autorizada en el dispositivo del usuario ni con otros dispositivos u ordenadores, servidores, redes, interfaces de programación de aplicaciones (API) o servicios (como otras aplicaciones del dispositivo, cualquier servicio de Google o la red de un operador autorizado). Tampoco se admitirán aplicaciones que interrumpan o dañen los elementos anteriormente citados ni que accedan a los mismos de forma no autorizada.

Las aplicaciones de Google Play deben cumplir los requisitos predeterminados de optimización del sistema Android que se indican en las directrices de calidad básica de las aplicaciones para Google Play .

Una aplicación distribuida a través de Google Play no debe modificarse, reemplazarse ni actualizarse automáticamente con ningún método que no sea el mecanismo de actualización de Google Play. Del mismo modo, una aplicación no debe descargar código ejecutable (por ejemplo, archivos dex, JAR o .so) de ninguna fuente que no sea Google Play. Esta restricción no se aplica al código que se ejecuta en máquinas virtuales o intérpretes cuando cualquiera de ellos permite acceder indirectamente a APIs de Android (como JavaScript en WebView o en un navegador).

Las aplicaciones o el código de terceros (por ejemplo, SDKs) con lenguajes interpretados (JavaScript, Python, Lua, etc.) cargados en el momento de la ejecución (por ejemplo, no incluidos en el paquete de la aplicación) no deben permitir posibles infracciones de las políticas de Google Play.

No admitimos código que introduzca o aproveche vulnerabilidades de seguridad. Consulta el Programa de Mejora de la Seguridad de las Aplicaciones para obtener información sobre los problemas de seguridad más recientes de los que se haya informado a los desarrolladores.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que bloquean una aplicación o interfieren en ella publicando anuncios.
- Aplicaciones para hacer trampas en juegos que afectan a las partidas de otras aplicaciones.
- Aplicaciones que facilitan o dan instrucciones sobre cómo hackear servicios, software o hardware y eludir medidas de seguridad.
- Aplicaciones que accedan a un servicio o a una API y los utilicen de un modo que infrinja los términos del servicio de ese servicio o API.
- Aplicaciones que no cumplan los requisitos para ser incluidas en la lista aprobada e intenten evitar la gestión de energía del sistema .

- Aplicaciones que faciliten servicios de proxy a terceros (solo pueden hacerlo cuando sea el objetivo principal de la aplicación para los usuarios).
- Aplicaciones o código de terceros (por ejemplo, archivos SDK) que descarguen código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play.
- Aplicaciones que instalen otras aplicaciones en un dispositivo sin el consentimiento previo del usuario.
- Aplicaciones que contengan enlaces a software malicioso o que faciliten su distribución o instalación.
- Aplicaciones o código de terceros (por ejemplo, archivos SDK) que contengan un elemento WebView con la interfaz JavaScript añadida y que carguen contenido web que no sea de confianza (por ejemplo, una URL de http://) o URLs no verificadas obtenidas de fuentes que no sean de confianza (por ejemplo, URLs obtenidas de intents que no son de confianza).

En vigor desde el 1 de noviembre del 2022

Requisitos de Flag Secure

FLAG_SECURE es una marca de visualización declarada en el código de una aplicación que indica que su interfaz de usuario contiene datos sensibles que deben limitarse a una superficie segura mientras se usa la aplicación. Esta marca se ha diseñado para evitar que los datos aparezcan en capturas de pantalla o que se visualicen en pantallas no seguras. Los desarrolladores declaran esta marca si el contenido de la aplicación no debe difundirse, visualizarse ni transmitirse de cualquier otra forma fuera de la aplicación o del dispositivo del usuario.

Para fines de seguridad y privacidad, todas las aplicaciones distribuidas en Google Play deben respetar la declaración FLAG_SECURE de otras aplicaciones. Esto quiere decir que las aplicaciones no deben facilitar ni ofrecer alternativas para eludir la configuración de FLAG_SECURE en otras aplicaciones.

Las aplicaciones que puedan considerarse herramientas de accesibilidad están exentas de este requisito siempre y cuando no transmitan, guarden ni almacenen en caché contenido protegido mediante FLAG_SECURE frente al acceso desde fuera del dispositivo del usuario.

Comportamiento engañoso

No admitimos aplicaciones que traten de engañar a los usuarios o facilitar conductas fraudulentas; esto incluye, por ejemplo, aplicaciones que estén diseñadas para no funcionar. Las aplicaciones deben proporcionar contenido informativo, descripciones, imágenes y vídeos precisos sobre sus funciones en los metadatos. Las aplicaciones no deben imitar las funciones ni las advertencias del sistema operativo, ni de otras aplicaciones. Cualquier cambio en la configuración del dispositivo debe hacerse con el conocimiento y el consentimiento del usuario, y este debe poder revertirlo.

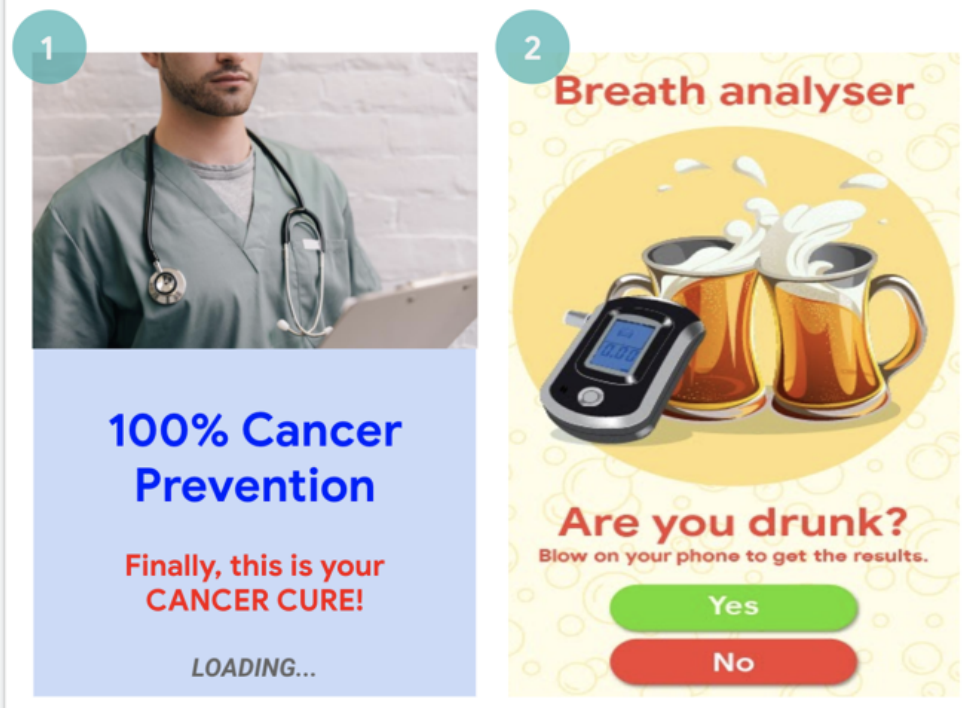
Afirmaciones engañosas

No admitimos aplicaciones que incluyan información ni afirmaciones falsas o engañosas, por ejemplo, en los títulos, los iconos, las descripciones o las capturas de pantalla.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que no describen sus funciones de forma fiel, clara y veraz:
  - Una aplicación que afirma ser un juego de carreras en la descripción y en las capturas de pantalla, pero en realidad es un juego de puzles de bloques que utiliza la imagen de un coche.
  - Una aplicación que afirma ser un antivirus, pero solo contiene una guía de texto explicando cómo eliminar virus.

- Aplicaciones que afirman disponer de funciones que son imposibles de llevar a cabo, como una aplicación repelente de insectos, incluso si se presentan como una broma, un chiste, etc.
- Aplicaciones que están categorizadas de forma incorrecta (entre otros, en cuanto a la clasificación o la categoría de la aplicación).
- Contenido manifiestamente engañoso o falso que puede interferir en procesos electorales.
- Aplicaciones que afirman, sin ser cierto, estar asociadas a una entidad pública o proporcionar servicios públicos para los que no tengan la autorización correspondiente.
- Aplicaciones que afirman falsamente ser la aplicación oficial de una entidad establecida. Los títulos como "Justin Bieber Oficial" no están permitidos si no se cuenta con los permisos o derechos necesarios.



(1) Esta aplicación incluye afirmaciones médicas o relacionadas con la salud que son engañosas (curar el cáncer).
(2) Esta aplicación afirma disponer de funciones que no se pueden llevar a cabo (usar el teléfono como alcoholímetro).

Cambios engañosos de los ajustes del dispositivo

No admitimos aplicaciones que hagan cambios en la configuración o en las funciones del dispositivo del usuario fuera de la aplicación sin su conocimiento ni su consentimiento. La configuración y las funciones del dispositivo incluyen ajustes del sistema y del navegador, así como marcadores, accesos directos, iconos, widgets y la presentación de aplicaciones en la pantalla de inicio.

Tampoco admitimos lo siguiente:

- Aplicaciones que modifiquen los ajustes o las funciones del dispositivo con el consentimiento del usuario, pero que lo hagan de una forma que no sea fácilmente reversible.
- Aplicaciones o anuncios que modifiquen los ajustes o las funciones del dispositivo como servicio a terceros o con fines publicitarios.
- Aplicaciones que engañen a los usuarios para que desinstalen o inhabiliten aplicaciones de terceros o para que modifiquen ajustes o funciones del dispositivo.
- Aplicaciones que animen o incentiven a los usuarios para que desinstalen o inhabiliten aplicaciones de terceros, o para que modifiquen los ajustes o las funciones del dispositivo, a menos que se trate de un servicio de seguridad que se pueda verificar.

Facilitar conductas fraudulentas

No admitimos aplicaciones que ayuden a los usuarios a engañar a otros o que incorporen funciones engañosas, incluidas las aplicaciones que generen o que faciliten la generación de carnés de identidad, números de identificación personal, pasaportes, diplomas, tarjetas de crédito, cuentas bancarias o carnés de conducir. Las aplicaciones deben proporcionar avisos, títulos, descripciones, imágenes y vídeos que reflejen de forma precisa y veraz sus funciones y contenido, y deben poder ejecutarse de una forma correcta y razonable que se corresponda con las expectativas de los usuarios.

Los recursos adicionales de las aplicaciones (por ejemplo, recursos de juegos) solo se pueden descargar si son necesarios para que los usuarios utilicen la aplicación. Estos recursos deben cumplir todas las políticas de Google Play y, antes de comenzar la descarga, la aplicación debe avisar a los usuarios e informarles claramente del tamaño de la descarga.

Cualquier afirmación que diga que una aplicación es una "broma" o se ha desarrollado "con fines de entretenimiento" (u otro sinónimo) no exime a la aplicación de cumplir nuestras políticas.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que imitan otras aplicaciones o sitios web con el objetivo de engañar a los usuarios para que revelen información personal o de autenticación.
- Aplicaciones que representen o muestren números de teléfono, contactos, direcciones o información personal identificable reales o sin verificar de personas o entidades que no hayan dado su consentimiento.
- Aplicaciones con funciones principales diferentes según la ubicación geográfica del usuario, los parámetros del dispositivo u otros datos dependientes del usuario, y en las que esas diferencias no se anuncian de forma destacada en la ficha de Play Store.
- Aplicaciones que cambien significativamente de una versión a otra sin avisar al usuario (por ejemplo, en la sección de novedades) y sin actualizar la ficha de Play Store.
- Aplicaciones que intenten modificar u ofuscar el comportamiento durante la revisión.
- Aplicaciones con descargas facilitadas por una red de distribución de contenido (CDN) que no avisen a los usuarios ni les informen previamente del tamaño de la descarga.

Elementos multimedia manipulados

No permitimos aplicaciones que promuevan o ayuden a crear información o afirmaciones falsas o engañosas mediante imágenes, vídeos o texto. Tampoco permitimos las aplicaciones cuyo objetivo sea promocionar o perpetuar imágenes, vídeos o texto demostrablemente falsos o engañosos que puedan causar daños en relación con acontecimientos sensibles, temas políticos, asuntos sociales u otros temas de interés público.

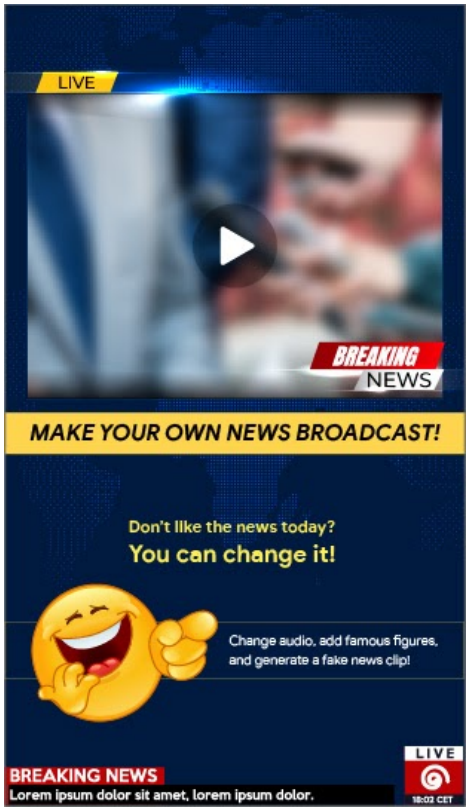
Las aplicaciones que manipulen o alteren elementos multimedia, más allá de los ajustes habituales y aceptables editorialmente en materia de claridad o calidad, deben incluir un aviso visible o una marca de agua en los elementos multimedia alterados cuando sea posible que los usuarios no puedan identificar con claridad que dichos elementos se han manipulado. Se pueden hacer excepciones por interés público o motivos evidentes de sátira o parodia.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que añaden una figura pública a una manifestación durante un evento políticamente sensible.
- Aplicaciones que, en su ficha de Play Store, utilizan personajes públicos o elementos multimedia relativos a un acontecimiento sensible para publicitar la capacidad de manipular elementos

multimedia.

- Aplicaciones que manipulan vídeos para imitar la retransmisión de noticias.



(1) Esta aplicación ofrece la función de modificar vídeos para imitar una retransmisión de noticias y añadir personajes famosos o públicos al vídeo sin una marca de agua.

Información falsa

No admitimos aplicaciones ni cuentas de desarrollador que:

- Suplanten la identidad de una persona u organización, o que oculten o falseen su propiedad o su finalidad principal.
- Participen en actividades coordinadas para engañar a los usuarios. Se incluyen, entre otras, las aplicaciones o cuentas de desarrollador que falseen u oculten su país de origen y que dirijan su contenido a usuarios de otro país.
- Se coordinen con otras aplicaciones, sitios web, desarrolladores u otras cuentas para ocultar o proporcionar información falsa sobre la identidad de la aplicación o del desarrollador, o sobre otros detalles materiales, en los que el contenido de la aplicación esté relacionado con política, problemas sociales o asuntos de interés público.

En vigor desde el 1 de noviembre del 2022

Política de niveles de API de destino de Google Play

Para ofrecer a los usuarios una experiencia segura, Google Play requiere los siguientes niveles de API de destino para **todas las aplicaciones**:

Las nuevas aplicaciones y las actualizaciones de aplicaciones DEBEN orientarse a un nivel de API de Android en el plazo de un año desde el lanzamiento de la última versión principal de Android. Las aplicaciones nuevas y las actualizaciones de aplicaciones que no cumplan este requisito no podrán enviarse en Play Console.

Las aplicaciones de Google Play que no estén actualizadas y que no se orienten a un nivel de API en el plazo de dos años desde el lanzamiento de la última versión principal de Android no estarán disponibles para los nuevos usuarios que tengan dispositivos con versiones más recientes del SO Android. Los usuarios que hayan descargado previamente la aplicación desde Google Play podrán seguir encontrando, descargando y usando la aplicación en cualquier versión del SO Android compatible con la aplicación.

Si necesitas asesoramiento técnico sobre cómo cumplir el requisito del nivel de API de destino, consulta la guía de migración .

Para conocer las fechas exactas, consulta este artículo del Centro de Ayuda .

Software malicioso

Nuestra política sobre software malicioso es simple: no debe existir ningún tipo de conducta maliciosa (es decir, software malicioso) en el ecosistema Android, incluido Google Play Store, ni en los dispositivos de los usuarios. A partir de este principio fundamental, nos esforzamos por garantizar que el ecosistema Android sea seguro para nuestros usuarios y sus dispositivos Android.

El software malicioso es un código que puede poner en riesgo la seguridad de un usuario, de sus datos o sus dispositivos. El software malicioso incluye, entre otras amenazas, aplicaciones potencialmente dañinas, binarios y modificaciones de framework. Dichos elementos se clasifican en categorías (como troyanos, phishing y software espía) que actualizamos y ampliamos constantemente.

Aunque el software malicioso incluye muchos tipos y funciones diferentes, suele tener uno de los siguientes objetivos:

- Comprometer la integridad del dispositivo del usuario.
- Obtener el control del dispositivo del usuario.
- Permitir operaciones controladas de forma remota de un atacante para acceder, usar o explotar de alguna otra forma el dispositivo infectado.
- Transmitir credenciales o datos personales desde el dispositivo sin informar adecuadamente al usuario y sin su consentimiento.
- Difundir spam o comandos desde el dispositivo infectado para afectar a otros dispositivos o redes.
- Defraudar al usuario.

Las aplicaciones, los binarios y las modificaciones de framework pueden ser potencialmente dañinas y, por tanto, pueden generar comportamientos maliciosos aunque sea de forma no intencionada. El motivo es que las aplicaciones, los binarios o las modificaciones de framework pueden funcionar de forma diferente dependiendo de diversas variables. Por lo tanto, lo que es dañino para un dispositivo Android podría no representar ningún riesgo para otro. Por ejemplo, los dispositivos que usan la última versión de Android no se ven afectados por aplicaciones dañinas que usan API obsoletas para realizar acciones maliciosas, pero los dispositivos que aún usen versiones anteriores de Android sí podrían ser vulnerables a estas amenazas. Las aplicaciones, códigos binarios o modificaciones de framework se marcan como software malicioso o aplicaciones potencialmente dañinas si representan una amenaza clara para algunos o para todos los usuarios de Android y sus dispositivos.

Las categorías de software malicioso indicadas más abajo reflejan nuestro convencimiento de que los usuarios deben conocer el uso que hacen las aplicaciones de sus dispositivos, y tienen como objetivo promover un ecosistema seguro que ofrezca tanto una base sólida para la innovación como una experiencia segura para los usuarios.

Puedes consultar más información en Google Play Protect .

Puertas traseras

Código que permite la ejecución en un dispositivo de operaciones no deseadas, potencialmente dañinas y controladas de forma remota.

Estas operaciones pueden incluir comportamientos que harían que la aplicación, el binario o la modificación de framework se incluyeran en una de las categorías de software malicioso si se ejecutaran automáticamente. En general, el término "puerta trasera" hace referencia a operaciones potencialmente dañinas que se pueden ejecutar en un dispositivo y, por tanto, no se corresponde completamente con categorías como el fraude de facturación o el software espía comercial. Como resultado, en algunos casos, Google Play Protect trata a un subgrupo de aplicaciones de puerta trasera como una vulnerabilidad.

Fraude de facturación

Código que cobra automáticamente al usuario de una forma intencionadamente engañosa.

El fraude de facturación móvil se divide en tres categorías: por SMS, por llamadas y por tarificación.

Fraude por SMS
Código que cobra a los usuarios por enviar SMS de tarificación especial sin su consentimiento, o que intenta encubrir sus actividades de SMS al ocultar los acuerdos de confidencialidad o los mensajes SMS del operador móvil, al notificar al usuario sobre cargos o al confirmar suscripciones.

Algunos códigos, aunque técnicamente revelan el envío de los SMS, introducen un comportamiento adicional que permite realizar el fraude por SMS. Por ejemplo, ocultan al usuario partes de un acuerdo de confidencialidad, hacen que estos resulten ininteligibles o suprimen condicionalmente los mensajes SMS del operador móvil que informan al usuario sobre cargos o confirman suscripciones.

Fraude por llamada
Código que cobra a los usuarios haciendo llamadas a números de tarificación especial sin su consentimiento.

Fraude por tarificación
Código que engaña a los usuarios adquiriendo contenido o suscribiéndoles a servicios a través de la factura de sus teléfonos móviles.

Los fraudes por tarificación incluyen cualquier tipo de facturación, excepto los SMS y las llamadas de tarificación especial. Algunos ejemplos de este fraude son la facturación directa del operador, los puntos de acceso inalámbricos (WAP) y las transferencias de tiempo de conexión móvil. Los fraudes de puntos de acceso inalámbricos son uno de los fraudes por tarificación más comunes. Este tipo de fraudes incluye engañar a los usuarios para que hagan clic en un botón en un WebView transparente cargado de forma silenciosa. Una vez realizada esta acción, se inicia una suscripción recurrente, y el SMS o el correo electrónico de confirmación se suele interceptar para impedir que los usuarios se den cuenta de la transacción financiera.

Fecha de entrada en vigor: 15 de febrero del 2023

Stalkerware

Se trata de un código que recopila datos personales o sensibles del usuario desde un dispositivo y los transmite a un tercero (empresa o persona física) para su monitorización.

Las aplicaciones deben mostrar un aviso destacado adecuado y recabar el consentimiento de los usuarios conforme a la Política de Datos de Usuario .

Directrices de monitorización de aplicaciones

Las aplicaciones diseñadas y promocionadas exclusivamente para monitorizar a otro individuo, por ejemplo, padres que quieren monitorizar a sus hijos, o en el ámbito de la gestión de empresas, para monitorizar a empleados concretos, siempre que cumplan todos los requisitos que se detallan a continuación, son las únicas aplicaciones de monitorización aceptables. Estas aplicaciones no se pueden utilizar para consultar la ubicación de otras personas (la pareja del usuario, por ejemplo)

incluso con su conocimiento y permiso, independientemente de si se muestra una notificación permanente. Estas aplicaciones deben usar la marca de metadatos IsMonitoringTool en su archivo de manifiesto para calificarse adecuadamente a sí mismas como aplicaciones de monitorización.

Las aplicaciones de monitorización deben cumplir los siguientes requisitos:

- Las aplicaciones no se deben presentar como soluciones de espionaje o vigilancia secreta.
- Las aplicaciones no deben ocultar o encubrir el seguimiento ni intentar engañar a los usuarios sobre estas funciones.
- Las aplicaciones deben exhibir una notificación permanente a los usuarios en todo momento mientras estén en funcionamiento y mostrar un icono distintivo que permita identificar claramente la aplicación.
- Las aplicaciones deben avisar de la función de monitorización o rastreo en la descripción de Google Play Store.
- Las aplicaciones y sus fichas de Google Play no deben proporcionar medios para activar o acceder a funciones que infrinjan estos términos, como enlazar a un APK que no cumpla los requisitos y que esté alojado fuera de Google Play.
- Las aplicaciones deben respetar todas las leyes aplicables. Eres el único responsable de determinar la legalidad de tu aplicación en el mercado de destino.

Denegación de servicio (DoS)

Código que, sin el conocimiento del usuario, ejecuta un ataque de denegación de servicio (DoS) o forma parte de un ataque DoS distribuido contra otros sistemas y recursos.

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

Software de descarga hostil

Código que no es potencialmente dañino en sí mismo, pero que descarga otras aplicaciones potencialmente dañinas.

El código puede considerarse software de descarga hostil si:

- Hay motivos para creer que se creó para difundir aplicaciones potencialmente dañinas y que ha descargado aplicaciones de este tipo, o contiene código que podría descargar e instalar aplicaciones.
- Al menos el 5 % de las aplicaciones descargadas por este tipo de código son potencialmente dañinas, con un umbral mínimo de 500 aplicaciones descargadas (de las cuales 25 son potencialmente dañinas).

Los principales navegadores y aplicaciones que comparten archivos no se consideran software hostil siempre que:

- No inicien las descargas sin la interacción del usuario.
- Todas las descargas de aplicaciones potencialmente dañinas se inicien con el consentimiento de los usuarios.

Amenaza no relacionada con Android

Código que contiene amenazas no relacionadas con Android.

Estas aplicaciones no pueden causar daños a los usuarios de Android ni a sus dispositivos, pero incluyen componentes que pueden ser dañinos para otras plataformas.

Suplantación de identidad (phishing)

Código que finge provenir de una fuente de confianza, solicita las credenciales de autenticación o los datos de facturación del usuario y, a continuación, envía esa información a un tercero. Esta categoría también se aplica al código que intercepta las credenciales de los usuarios durante su transmisión.

Entre los objetivos del phishing, se incluyen credenciales bancarias y números de tarjetas de crédito, así como credenciales de cuentas online de redes sociales y juegos.

Abuso de privilegios

Código que pone en peligro la integridad del sistema accediendo sin autorización a la zona de pruebas de la aplicación, obteniendo privilegios avanzados, o bien cambiando o inhabilitando el acceso a funciones básicas de seguridad.

A continuación se incluyen algunos ejemplos:

- Aplicaciones que infringen el modelo de permisos de Android o roban credenciales (como los tokens de OAuth) de otras aplicaciones
- Aplicaciones que abusan de funciones para impedir que se puedan desinstalar o detener
- Aplicaciones que inhabilitan SELinux

Las aplicaciones que se apropian de privilegios y rootean dispositivos sin el permiso de los usuarios se conocen como aplicaciones de rooteado.

Ransomware

Código que toma el control de forma parcial o general de un dispositivo o de sus datos, tras lo que exige al usuario que haga un pago o realice una acción para recuperar el control sobre ellos.

Algunos programas de ransomware encriptan los datos del dispositivo y exigen un pago para desencriptarlos, y utilizan las funciones administrativas del dispositivo para que los usuarios ordinarios no puedan eliminarlos. A continuación se incluyen algunos ejemplos:

- Bloquear el acceso de un usuario a su dispositivo y exigirle dinero para que recupere el control.
- Encriptar los datos de un dispositivo y exigir un pago (presumiblemente para desencriptarlos).
- Impedir que el usuario pueda eliminar el código utilizando las funciones del administrador de políticas del dispositivo.

Es posible que los códigos distribuidos con el dispositivo cuya finalidad principal sea la gestión de dispositivos subvencionados se excluyan de la categoría de ransomware, siempre que cumplan los requisitos de gestión y bloqueo de seguridad, así como los de informar al usuario y obtener su consentimiento.

Rooteo

Código que rootea el dispositivo.

Hay una diferencia entre el código de rooteo no malicioso y el malicioso. Por ejemplo, las aplicaciones de rooteo no maliciosas avisan al usuario con antelación de que van a rootear el dispositivo y no ejecutan otras acciones propias de las aplicaciones potencialmente dañinas.

Las aplicaciones de rooteo maliciosas no informan al usuario de que van a rootear el dispositivo, o le informan del rooteo con antelación, pero también ejecutan otras acciones propias de las aplicaciones potencialmente dañinas.

Spam

Código que envía mensajes no solicitados a los contactos del usuario o usa el dispositivo como un relay de spam por correo electrónico.

Software espía

Código que transmite datos personales desde el dispositivo sin informar adecuadamente al usuario y sin obtener su consentimiento.

Por ejemplo, para que un código se considere software espía, basta con que transmita cualquiera de los siguientes datos sin previo aviso o de una forma inesperada para el usuario:

- Lista de contactos
- Fotos u otros archivos de la tarjeta SD o que no sean propiedad de la aplicación
- Contenido del correo electrónico del usuario
- Registro de llamadas
- Registro de SMS
- El historial web o los marcadores del navegador predeterminado
- Información de los directorios /data/ de otras aplicaciones

Los comportamientos que se consideren espiar al usuario también se podrán marcar como software espía. Por ejemplo, grabar audio o llamadas al teléfono, o robar datos de aplicaciones.

Troyano

Código que parece inofensivo, como un juego del que se asegura que es tan solo un juego, pero que ejecuta acciones no deseadas y perjudiciales para el usuario.

Esta clasificación se suele utilizar en combinación con otras categorías de aplicaciones potencialmente dañinas. Un troyano tiene un componente inofensivo y otro dañino. Por ejemplo, un juego que envía mensajes SMS premium desde el dispositivo del usuario en segundo plano y sin el conocimiento del usuario.

Una nota sobre aplicaciones poco comunes

Las aplicaciones nuevas o poco frecuentes se clasifican como poco comunes si Google Play Protect no dispone de suficiente información para garantizar que son seguras. Esta clasificación no implica necesariamente que la aplicación sea dañina, pero, sin una revisión más exhaustiva, tampoco podemos garantizar que sea segura.

Una nota sobre la categoría de puerta trasera

La clasificación de la categoría de software malicioso de puerta trasera depende de cómo actúe el código. Una condición necesaria para que un código se clasifique como software de puerta trasera es que permita un comportamiento que lo incluiría en una de las categorías de software malicioso si se ejecutara automáticamente. Por ejemplo, si una aplicación permite la carga dinámica de código, y el código cargado dinámicamente extrae mensajes de texto, se clasificará como software malicioso de puerta trasera.

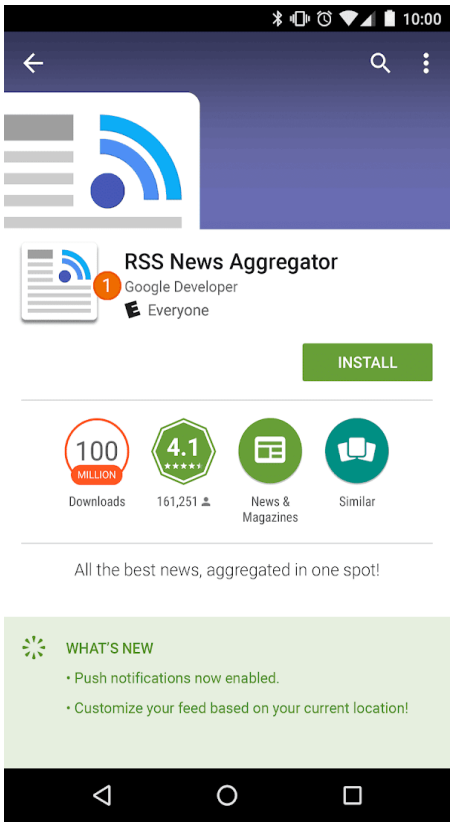
Sin embargo, si una aplicación permite la ejecución de código arbitrario y no tenemos ningún motivo para creer que la ejecución de ese código se añadió con un objetivo malicioso, la aplicación no se tratará como un software malicioso de puerta trasera, sino como una aplicación que tiene una vulnerabilidad, y se pedirá al desarrollador que le aplique un parche.

Suplantación de identidad

No admitimos aplicaciones que engañen a los usuarios suplantando la identidad de alguien (por ejemplo, de otro desarrollador, empresa o entidad) o de otra aplicación. No insinúes que tu aplicación está relacionada con alguien o autorizada por alguien si no lo está. Procura no utilizar iconos, descripciones ni títulos de aplicaciones, ni elementos en la aplicación, que puedan confundir a los usuarios sobre la relación de tu aplicación con otra persona o aplicación.

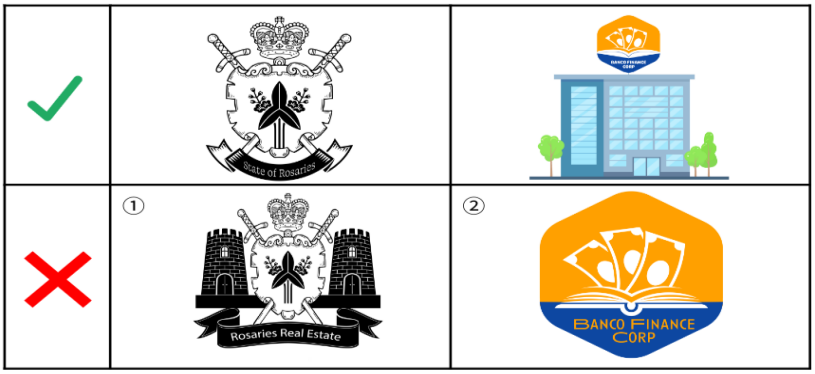
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Desarrolladores que insinúan falsamente que existe una relación con otra empresa / entidad / organización o con otro desarrollador.



① El nombre del desarrollador que aparece en esta aplicación sugiere una relación oficial con Google, pero esta relación no existe.

- Aplicaciones cuyos iconos y títulos insinúen falsamente que existe una relación con otra empresa, entidad, organización o desarrollador.



①La aplicación utiliza un emblema nacional y engaña a los usuarios haciéndoles creer que está vinculada al gobierno.
②La aplicación copia el logotipo de una entidad empresarial para sugerir falsamente que es una aplicación oficial de la empresa.

- Títulos e iconos de aplicaciones que son tan parecidos a los de otros productos o servicios que pueden llevar a error a los usuarios:

①La aplicación utiliza el logotipo del sitio web de una criptomoneda conocida en el icono de la aplicación para sugerir que es el sitio web oficial.
②La aplicación copia el personaje y el título de un famoso programa o serie de televisión en el icono de la aplicación y engaña a los usuarios para que crean que está vinculada a un programa o serie de televisión.

- Aplicaciones que afirman falsamente ser la aplicación oficial de una entidad establecida. Los títulos como "Justin Bieber Oficial" no están permitidos sin contar con los permisos o derechos necesarios.
- Aplicaciones que infringen las Directrices de marca de Android .

Mobile Unwanted Software

En Google creemos que si nos centramos en el usuario, todo lo demás vendrá solo. En nuestros Principios de Software y en nuestra Política de Software No Deseado, incluimos una serie de recomendaciones generales para crear un software que ofrezca una gran experiencia al usuario. Esta política se basa en la Política de Google de Software No Deseado y describe los principios del ecosistema de Android y de Google Play Store. El software que infrinja estos principios se considerará potencialmente perjudicial para la experiencia de usuario, y tomaremos medidas para proteger de él a nuestros usuarios.

Tal como se menciona en la Política de Software No Deseado, hemos constatado que la mayoría del software no deseado presenta una o varias de las mismas características básicas:

- Es engañoso, ya que promete una propuesta de valor que no cumple.
- Trata de engañar a los usuarios para que lo instalen o usa la técnica del piggybacking cuando se instala otro programa.
- No informa al usuario de cuáles son sus funciones más importantes y significativas.
- Afecta al sistema del usuario de formas inesperadas.
- Recoge o transmite información privada sin el conocimiento de los usuarios.
- Recoge o transmite información privada sin gestionarla de forma segura (por ejemplo, utilizando la transmisión a través de HTTPS).

- Se incluye en un paquete de software, pero no se informa de su presencia.

En los dispositivos móviles, el software puede ser código de aplicación, código binario, código para modificar marcos, etc. Con el objetivo de evitar el software que dañe el ecosistema o que entorpezca la experiencia de usuario, tomaremos medidas frente al código que infrinja estos principios.

A continuación nos basamos en la Política de Software No Deseado para ampliar su aplicación al software para móviles. Al igual que hacemos con dicha política, seguiremos mejorando la Política de Software No Deseado para Móviles con el objetivo de hacer frente a nuevos tipos de usos inadecuados.

Comportamiento transparente e información clara

Todo el código debe cumplir las promesas que se le hagan al usuario. Las aplicaciones deben proporcionar todas las funciones de las que se informe. Las aplicaciones no deben confundir a los usuarios.

- Las aplicaciones deben indicar de forma clara cuáles son sus funciones y objetivos.
- Las aplicaciones deben explicar de forma explícita y clara al usuario qué cambios van a realizar en el sistema. También deben permitir que los usuarios revisen y aprueben todas las opciones de instalación y los cambios importantes.
- El software no debe mostrar información falsa sobre el estado del dispositivo del usuario; por ejemplo, no debe afirmar que la seguridad del sistema se encuentra en estado crítico o que el sistema está infectado por virus.
- No utilices actividades no válidas que se hayan diseñado para aumentar el tráfico de los anuncios o las conversiones.
- No admitimos aplicaciones que engañen a los usuarios suplantando la identidad de alguien (por ejemplo, de otro desarrollador, empresa o entidad) o de otra aplicación. No insinúes que tu aplicación está relacionada con alguien o autorizada por alguien si no lo está.

Ejemplos de infracciones:

- Fraude publicitario
- Ingeniería social

Protege los datos de los usuarios

Explica con claridad y transparencia cómo se accede a los datos personales y sensibles de los usuarios, y cómo se recogen, se usan y se comparten. El uso de los datos de usuario debe cumplir todas las políticas sobre datos de usuario pertinentes, según corresponda, y deben tomarse todas las precauciones necesarias para proteger los datos.

- Proporciona a los usuarios la opción de aceptar la recogida de sus datos antes de empezar a recogerlos y enviarlos desde el dispositivo, incluidos los datos de cuentas de terceros, correo electrónico, número de teléfono, aplicaciones instaladas, archivos, ubicación y otros datos personales y sensibles que los usuarios no esperan que se recojan.
- Los datos de usuario personales y sensibles recogidos deben gestionarse de forma segura, incluida su transmisión a través de un cifrado actual (por ejemplo, mediante HTTPS).
- El software, incluidas las aplicaciones para móviles, solo debe transmitir datos de usuario personales y sensibles a servidores que estén relacionados con las funciones de la aplicación.

Ejemplos de infracciones:

- Recogida de datos (ver también Software espía)
- Uso inadecuado de los permisos restringidos

Ejemplos de políticas de datos de usuario:

- *Política de Datos de Usuario de Google Play*
- *Política de Datos de Usuario de los Requisitos de GMS*

- *Política de Datos de Usuario del Servicio de API de Google*

No empeores la experiencia móvil

La experiencia de usuario debe ser sencilla y fácil de entender, y debe basarse en decisiones claras del usuario. Debe presentar una propuesta de valor clara al usuario y no debe entorpecer la experiencia de usuario anunciada o deseada.

- No muestres a los usuarios anuncios que aparezcan de forma inesperada, como los que puedan afectar o interferir en el uso de las funciones del dispositivo o mostrarse fuera del entorno de la aplicación que los haya activado sin que se puedan rechazar fácilmente y sin el consentimiento o la atribución adecuados.
- Las aplicaciones no deben interferir en otras aplicaciones ni en el uso del dispositivo.
- La desinstalación, si procede, debe ser clara.
- El software para móviles no debe imitar los mensajes del sistema operativo del dispositivo ni de otras aplicaciones. No suprimas las alertas que recibe el usuario desde otras aplicaciones o desde el sistema operativo, especialmente las que informen al usuario sobre cambios en su sistema operativo.

Ejemplos de infracciones:

- Anuncios invasivos
- Uso no autorizado o imitación de funciones del sistema

Software de descarga hostil

Código que no es software no deseado en sí mismo, pero que descarga otro software no deseado para móviles.

El código puede considerarse software de descarga hostil si:

- Hay motivos para creer que se diseñó para difundir software no deseado para móviles y que ha descargado software de este tipo, o contiene código que podría descargar e instalar aplicaciones.
- O bien, si al menos el 5 % de las aplicaciones descargadas por el código son software no deseado para móviles, con un umbral mínimo de 500 aplicaciones descargadas (de las cuales 25 son software no deseado para móviles).

Los principales navegadores y aplicaciones que comparten archivos no se consideran software de descarga hostil siempre que:

- No inicien las descargas sin la interacción del usuario.
- Todas las descargas de software se inicien con el consentimiento de los usuarios.

Fraude publicitario

El fraude publicitario está prohibido. Las interacciones publicitarias generadas para engañar a una red publicitaria con el fin de que interprete que el tráfico es consecuencia del interés real de los usuarios son un fraude publicitario, que es un tipo de tráfico no válido. El fraude publicitario puede ser consecuencia de que los desarrolladores implementen anuncios con métodos no permitidos, como mostrar anuncios ocultos, hacer clic automáticamente en anuncios, alterar o modificar información o aprovechar acciones no humanas (arañas, bots, etc.) o actividades humanas diseñadas para producir tráfico de anuncios no válido. El tráfico no válido y el fraude publicitario son perjudiciales para los anunciantes, los desarrolladores y los usuarios, y provocan una pérdida de confianza a largo plazo en el ecosistema de anuncios para móviles.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

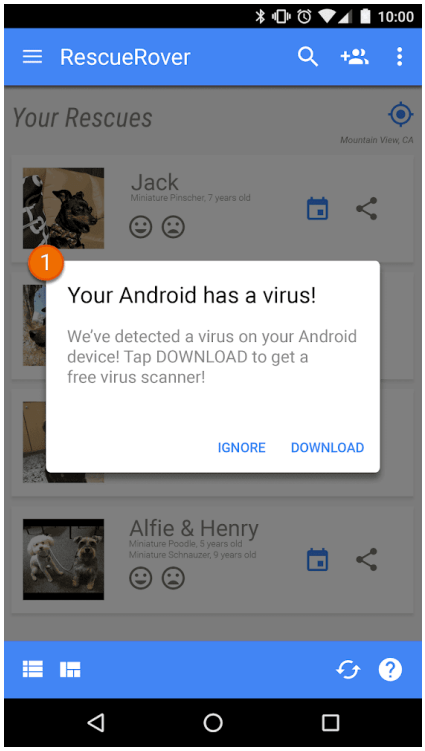
- Una aplicación que muestra anuncios que los usuarios no pueden ver.
- Una aplicación que genera automáticamente clics en anuncios sin la intervención del usuario, o que genera tráfico de red equivalente para ofrecer créditos de clics de forma fraudulenta.
- Una aplicación que envía clics de atribución de instalación falsos para recibir pagos por instalaciones que no proceden de la red del remitente.
- Una aplicación que muestra anuncios emergentes cuando el usuario no está en la interfaz de la aplicación.
- Información falsa sobre el inventario publicitario de una aplicación; por ejemplo, una aplicación que comunique a las redes publicitarias que se ejecuta en un dispositivo iOS cuando en realidad lo hace en un dispositivo Android, o una aplicación que proporcione información falsa sobre el nombre del paquete que se está monetizando.

Uso no autorizado o imitación de funciones del sistema

No admitimos aplicaciones o anuncios que interfieran en las funciones del sistema o las imiten, como notificaciones o advertencias. Las notificaciones del sistema solo se pueden usar para las funciones integrales de la aplicación, como la aplicación de una compañía aérea que avisa de ofertas especiales a los usuarios o un juego que informa a los usuarios de promociones integradas en el juego.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones o anuncios que se muestren mediante una alerta o una notificación del sistema:



① La notificación del sistema de esta aplicación se está usando para publicar un anuncio.

Para ver más ejemplos de anuncios, consulta la Política de Anuncios.

Social Engineering

We do not allow apps that pretend to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

No admitimos aplicaciones que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los publica. Consideramos los servicios de anuncios como parte de la aplicación. Los anuncios que se muestran en las aplicaciones deben cumplir todas nuestras políticas. Consulta las políticas sobre anuncios de juegos de apuestas.

Con el objetivo de beneficiar a desarrolladores y usuarios, Google Play ofrece varias estrategias de monetización, como la distribución de pago, los productos de compra en la aplicación, las suscripciones o los modelos basados en anuncios. Debes cumplir estas políticas para ofrecer la mejor experiencia de usuario.

Pagos

1. Los desarrolladores que apliquen cargos por las descargas de aplicaciones de Google Play deben usar el sistema de facturación de Google Play como método de pago para esas transacciones.
2. Las aplicaciones distribuidas a través de Google Play que requieran pagar o cobren por acceder a funciones o servicios en la aplicación, incluida cualquier funcionalidad de la aplicación, contenido o productos digitales (en conjunto, "compras en la aplicación"), deben usar el sistema de facturación de Google Play para esas transacciones, a menos que se aplique la Sección 3 o la Sección 8.

   Algunos ejemplos de funciones o servicios de aplicaciones que requieren el uso del sistema de facturación de Google Play son las compras en la aplicación de:

   - Artículos digitales (como monedas virtuales, vidas extra, tiempo de juego adicional, complementos, personajes o avatares).
   - Servicios de suscripción (como aplicaciones de fitness, juegos, citas, educación, música, vídeo, mejoras del servicio u otros servicios de suscripción de contenido).
   - Funcionalidad o contenido de aplicaciones (como la versión sin anuncios de una aplicación o nuevas funciones no disponibles en la versión gratuita).
   - Software y servicios en la nube (como servicios de almacenamiento de datos, software de productividad empresarial y software de gestión financiera).

3. El sistema de facturación de Google Play no debe usarse en los siguientes casos:
   a. Si el pago es, principalmente:
      - Para comprar o alquilar productos físicos, como artículos de alimentación, ropa, menaje y electrónica.
      - Para contratar servicios físicos, como servicios de transporte, servicios de limpieza, billetes de avión, suscripciones a gimnasios, reparto de comida o entradas para eventos en directo.
      - Para pagar facturas de tarjeta de crédito o de suministros, como servicios de televisión por cable o telecomunicaciones.

   b. Si se incluyen pagos de punto a punto, subastas online y donaciones exentas de impuestos.
   c. Si los pagos se realizan para adquirir contenido o servicios que ofrezcan juegos de apuestas online, tal como se describe en la sección Aplicaciones de juegos de apuestas de la política sobre Juegos de Apuestas, Juegos y Concursos con Dinero Real..
   d. Si el pago se realiza por un producto cuya categoría se considera inaceptable según las Políticas de Contenido del Centro de Pagos de Google.

      Nota: En algunos mercados, ofrecemos Google Pay para las aplicaciones que venden productos o servicios físicos. Para consultar más información, visita la página del desarrollador de Google Pay.

4. Aparte de las condiciones descritas en la Sección 3 y en la Sección 8, las aplicaciones no pueden llevar a los usuarios a un método de pago que no sea el sistema de facturación de Google Play. Esta

prohibición incluye, por ejemplo, dirigir a los usuarios a otros métodos de pago a través de:

- La ficha de una aplicación en Google Play.
- Promociones en la aplicación relacionadas con contenido en venta.
- Elementos WebView, botones, enlaces, mensajes, anuncios u otras llamadas a la acción en la aplicación.
- Flujos de la interfaz de usuario en la aplicación, incluidos los flujos de creación de cuentas o de registro que dirijan a los usuarios desde una aplicación a un método de pago distinto al sistema de facturación de Google Play.

5. Las monedas virtuales en aplicaciones solo se deben utilizar en la aplicación o el juego para los que se hayan comprado.

6. Los desarrolladores deben informar de forma clara y precisa a los usuarios sobre los términos y precios de su aplicación, o sobre las suscripciones o funciones en la aplicación que se puedan comprar. Los precios en la aplicación deben coincidir con los que aparecen en la interfaz de facturación de Play que ven los usuarios. Si la descripción de tu producto en Google Play hace referencia a funciones en la aplicación que puedan requerir un cargo concreto o adicional, debes indicar claramente en la ficha de la aplicación que los usuarios tienen que pagar para acceder a esas funciones.

7. Las aplicaciones y los juegos que ofrezcan mecanismos para recibir elementos virtuales de forma aleatoria al hacer una compra (por ejemplo, las cajas de recompensas) deben indicar de forma clara, antes de hacer la compra y en un momento oportuno y próximo a la adquisición, la probabilidad de recibir estos elementos.

8. A menos que se apliquen las condiciones descritas en la Sección 3, los desarrolladores de aplicaciones para teléfonos móviles y tablets distribuidas a través de Google Play que requieran pagar o que cobren de usuarios de Corea del Sur para acceder a compras en aplicaciones pueden ofrecer a los usuarios, además del sistema de facturación de Google Play, un sistema de facturación por compras en aplicaciones para las citadas transacciones si completan correctamente el formulario de declaración de sistemas adicionales de facturación por compras en aplicaciones y aceptan los términos adicionales y los requisitos del programa que se incluyen en él.

Nota: Puedes consultar los plazos y las preguntas frecuentes relacionadas con esta política en nuestro Centro de Ayuda.

No admitimos aplicaciones que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los publica. Consideramos los servicios de anuncios como parte de la aplicación. Los anuncios que se muestran en las aplicaciones deben cumplir todas nuestras políticas. Consulta las políticas sobre anuncios de juegos de apuestas.

No admitimos aplicaciones que contengan publicidad engañosa o perturbadora. Los anuncios solo deben mostrarse dentro de la aplicación que los publica. Consideramos que los anuncios y las ofertas asociadas que se publican en tu aplicación forman parte de la aplicación. Los anuncios que se muestren en tu aplicación deben cumplir todas nuestras políticas. Consulta las políticas sobre anuncios de juegos de azar y apuestas .

Uso de los datos de ubicación para anuncios

Las aplicaciones que aumentan el uso de los datos de la ubicación del dispositivo basada en permisos para ofrecer anuncios están sujetas a la política de Información personal y Sensible y deben cumplir los siguientes requisitos:

- Los usuarios deben poder identificar con claridad el uso o la recopilación de los datos de la ubicación del dispositivo basada en permisos con fines publicitarios. Además, este proceso debe estar documentado en la política de privacidad obligatoria de la aplicación, incluidas las asociaciones con cualquier política de privacidad de una red publicitaria de relevancia que aborde el uso de datos de ubicación.

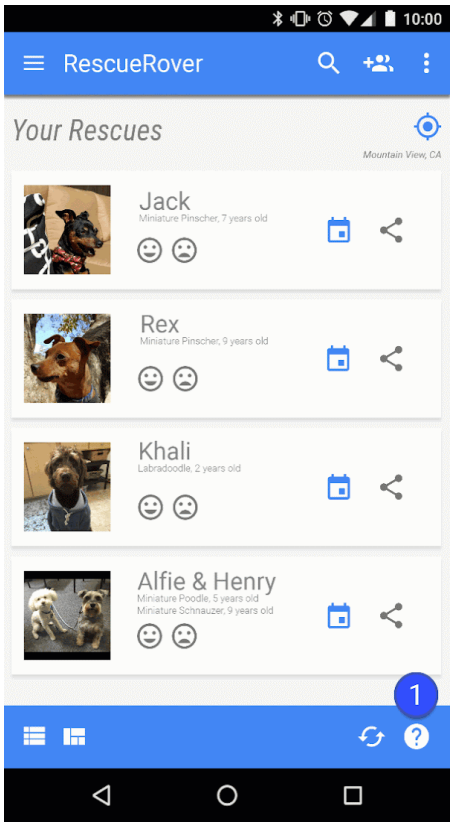
- De acuerdo con los requisitos de los permisos de ubicación, este tipo de permisos solo se puede solicitar para implementar los servicios o las funciones actuales en la aplicación. Del mismo modo, no se pueden solicitar permisos de ubicación del dispositivo solo para el uso de anuncios.

Publicidad engañosa

Los anuncios no deben imitar ni suplantar la interfaz de usuario de ninguna aplicación, ni tampoco las advertencias o las notificaciones de un sistema operativo. Los usuarios deben poder identificar con claridad qué aplicación publica cada anuncio.

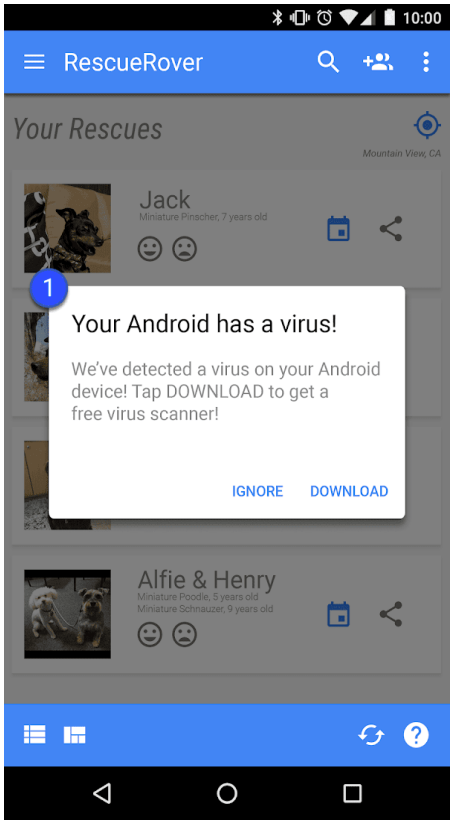
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

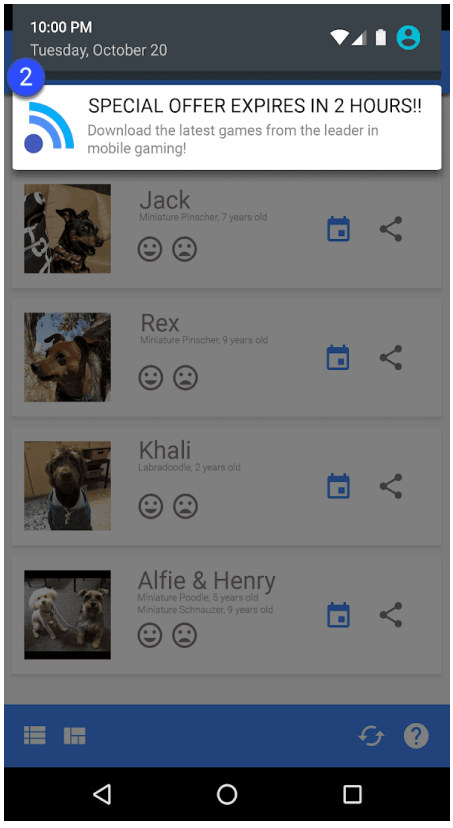
- Anuncios que imitan la interfaz de usuario de una aplicación:



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

- Anuncios que imitan una notificación del sistema:





① ② Los ejemplos anteriores muestran anuncios que imitan diferentes notificaciones del sistema.

Obtener ingresos a través de la pantalla de bloqueo

A menos que el único objetivo de la aplicación sea proporcionar una pantalla de bloqueo, las aplicaciones no pueden incluir anuncios o funciones para obtener ingresos procedentes de la pantalla de bloqueo de un dispositivo.

Anuncios invasivos

Los anuncios invasivos son anuncios que se muestran a los usuarios de formas inesperadas, por lo que pueden provocar clics accidentales o afectar al uso de las funciones del dispositivo.

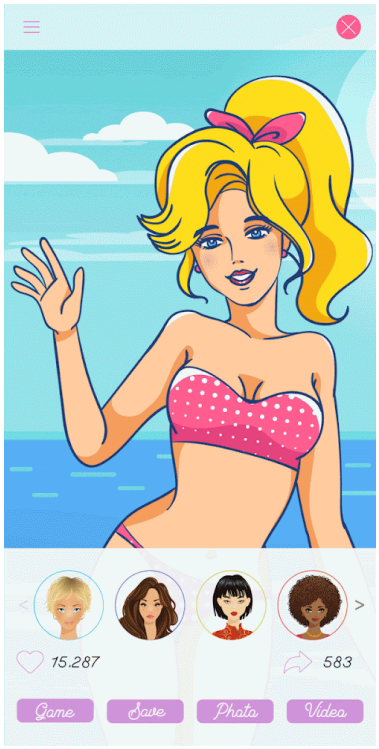
Tu aplicación no puede obligar a un usuario a que haga clic en anuncios o envíe información personal con fines publicitarios como condición para utilizar al completo una aplicación. Los anuncios intersticiales solo se pueden mostrar dentro de la aplicación que los publique. Si tu aplicación muestra anuncios intersticiales u otros anuncios que interfieran con el uso normal, el usuario debe poder cerrarlos fácilmente sin ninguna penalización.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

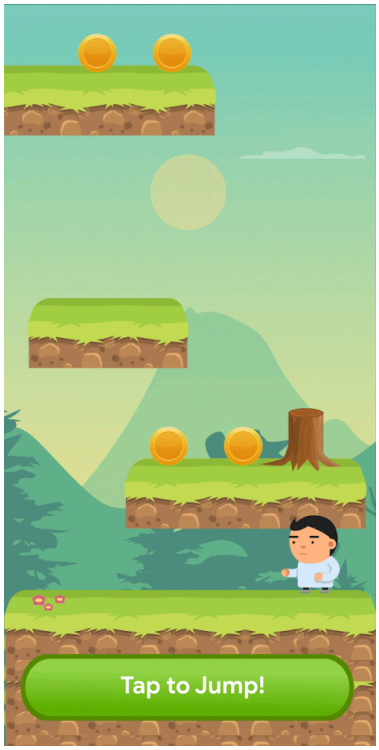
- Anuncios que ocupan toda la pantalla o interfieren en el uso normal y no ofrecen ningún medio claro para ignorarlos:

① Este anuncio no tiene ningún botón para ignorarlo.

- Anuncios que obligan al usuario a hacer clic en ellos mediante un botón de cierre falso, o anuncios que aparecen de repente en zonas de la aplicación en las que el usuario toca habitualmente para usar otra función.



- Un anuncio que utiliza un botón de cierre falso.



Un anuncio que aparece de repente en una zona en la que el usuario está acostumbrado a tocar para usar funciones en la aplicación.

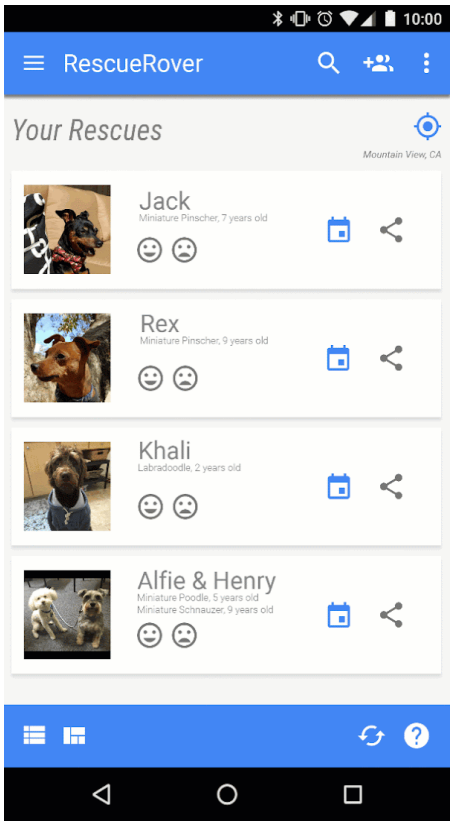
Interferir en aplicaciones, anuncios de terceros o funciones del dispositivo

Los anuncios asociados a tu aplicación no deben interferir en otras aplicaciones, en otros anuncios o en el funcionamiento del dispositivo (incluidos el sistema y los puertos y botones del dispositivo). Estas interferencias incluyen superposiciones, funciones complementarias o bloques de anuncios con widgets. Los anuncios solo deben mostrarse dentro de la aplicación que los publica.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros

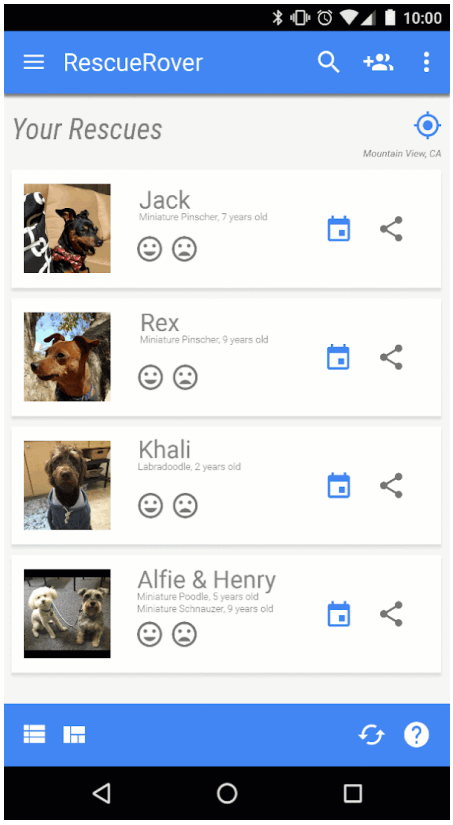
usuarios.

- Anuncios que se muestran fuera de la aplicación que los publica.



Descripción: el usuario accede a la pantalla de inicio desde esta aplicación y de repente aparece un anuncio en la pantalla de inicio.

- Anuncios que se activan al pulsar el botón de inicio u otras funciones diseñadas específicamente para salir de la aplicación.

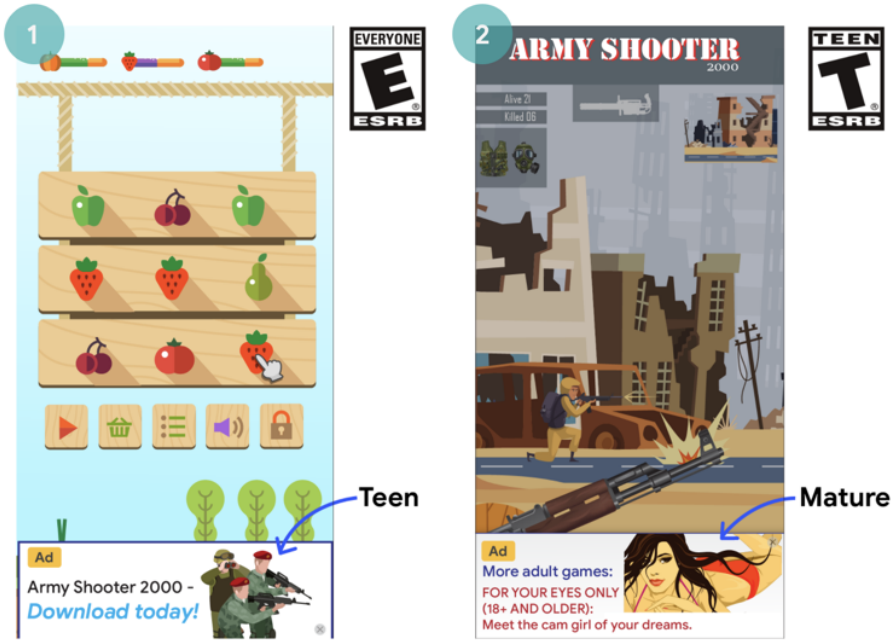


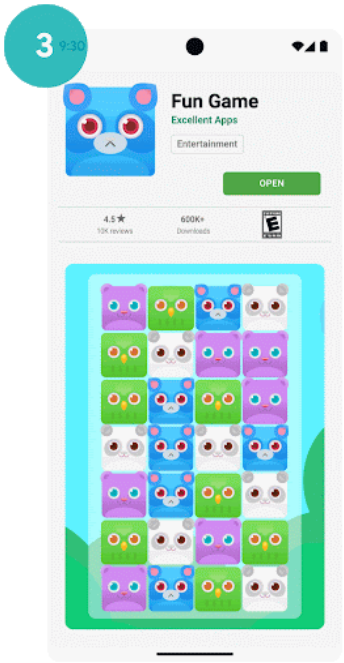
Descripción: el usuario intenta salir de la aplicación y acceder a la pantalla de inicio, pero el proceso se interrumpe con un anuncio.

Anuncios inadecuados

Los anuncios y las ofertas asociadas (por ejemplo, los anuncios que promocionen la descarga de otra aplicación) que se muestren dentro de tu aplicación deben ser apropiados para la clasificación del contenido de tu aplicación, aunque el contenido en sí mismo cumpla nuestras políticas.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.





① Este anuncio es inadecuado para la clasificación del contenido de la aplicación: el anuncio está orientado a adolescentes, pero la aplicación es para todos los públicos.
② Este anuncio es inadecuado para la clasificación del contenido de la aplicación: el anuncio está orientado a adultos, pero la aplicación es para adolescentes.
③La oferta del anuncio (promoción de la descarga de una aplicación para adultos) es inadecuada para la clasificación del contenido de la aplicación de videojuegos en la que se ha mostrado el anuncio, que está dirigida a todos los públicos.

Uso del ID de publicidad de Android

En la versión 4.0 de los Servicios de Google Play se presentan nuevas API y un ID que pueden utilizar los proveedores de análisis y de publicidad. A continuación se indican las condiciones de uso de este ID.

- **Uso:** el identificador de publicidad de Android (AAID) solo debe utilizarse para analizar los anuncios y los usuarios. El estado de la opción "Inhabilitar anuncios basados en intereses" o de la opción "Inhabilitar Personalización de Anuncios" se debe verificar en cada acceso del ID.
- **Asociación a información personal identificable u otros identificadores**.
  - Uso de publicidad: el identificador de publicidad no debe vincularse a identificadores de dispositivo persistentes (por ejemplo: SSAID, dirección MAC, IMEI, etc.) para fines publicitarios. El identificador de publicidad solo debe vincularse a información personal identificable con el consentimiento explícito del usuario.
  - Uso de análisis: el identificador de publicidad no debe vincularse a información personal identificable ni asociarse a ningún identificador de dispositivo persistente (por ejemplo: SSAID, dirección MAC, IMEI, etc.) para fines analíticos. Lee la política de datos de los usuarios para consultar más directrices relativas a los identificadores de dispositivo persistentes.
- **Respeto hacia las decisiones de los usuarios.**
  - Si se crea un nuevo identificador de publicidad, no debe vincularse a uno anterior o a sus datos derivados sin el consentimiento explícito del usuario.
  - Se debe respetar la decisión del usuario si ha seleccionado las opciones "Inhabilitar anuncios basados en intereses" o "Inhabilitar Personalización de Anuncios". En tal caso, no puedes utilizar el identificador de publicidad para crear perfiles de usuario con fines publicitarios ni para orientar publicidad personalizada a los usuarios. Entre las actividades permitidas, se incluyen la publicidad contextual, la limitación de frecuencia, el seguimiento de conversiones, la elaboración de informes y la detección del fraude y de problemas de seguridad.

    - En dispositivos más nuevos, el identificador se eliminará cuando el usuario elimine el identificador de publicidad de Android. Si se intenta acceder al identificador, se recibirá una cadena de ceros. Los dispositivos que no tengan un identificador de publicidad no deben conectarse a datos vinculados a un identificador de publicidad anterior ni a los datos que se deriven de él.
- **Transparencia para los usuarios.** Los usuarios deben estar informados sobre la recopilación de datos y el uso del identificador de publicidad, así como sobre el cumplimiento de estas condiciones, a través de una notificación de privacidad adecuada de carácter legal. Para obtener más información sobre nuestros estándares de privacidad, consulta nuestra política de datos de los usuarios .
- **Cumplimiento de los términos de uso**. El identificador de publicidad solo podrá utilizarse de acuerdo con la Política del Programa para Desarrolladores de Google Play, incluido el uso que haga de él un tercero con el que lo hayas compartido durante la actividad comercial. Todas las aplicaciones subidas o publicadas en Google Play deben utilizar el ID de publicidad (si está disponible en un dispositivo) en lugar de cualquier otro identificador de dispositivo con fines publicitarios.

Estándares Better Ads Experiences

Los desarrolladores deben cumplir las siguientes directrices sobre anuncios para ofrecer experiencias de alta calidad a los usuarios cuando usen aplicaciones de Google Play. Tus anuncios no deben mostrarse de las siguientes formas inesperadas a los usuarios:

- No están permitidos los anuncios intersticiales a pantalla completa de ningún formato (vídeos, archivos GIF, anuncios estáticos, etc.) que aparezcan de forma inesperada, por lo general, cuando el usuario haya elegido hacer otra cosa.
    - No están permitidos los anuncios que aparezcan mientras se juega a un videojuego al principio de un nivel o durante el comienzo de un segmento de contenido.
    - No están permitidos los anuncios intersticiales de vídeo a pantalla completa que aparezcan antes de la pantalla de carga (pantalla de inicio) de una aplicación.
- No están permitidos los anuncios intersticiales a pantalla completa de ningún formato que no se puedan cerrar después de 15 segundos. Los anuncios intersticiales de solicitud de aceptación a pantalla completa o los anuncios intersticiales a pantalla completa que no interrumpan las acciones de los usuarios (por ejemplo, los que se aparezcan después de la pantalla de puntuación en una aplicación de videojuegos) pueden mostrarse durante más de 15 segundos.

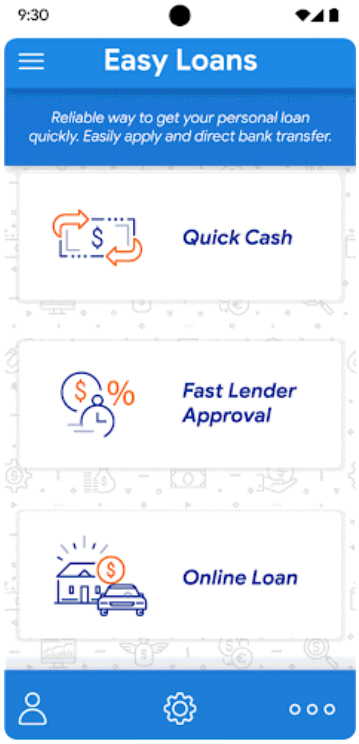
Esta política no se aplica a los anuncios bonificados, que requieren la aceptación explícita de los usuarios (por ejemplo, un anuncio que los desarrolladores ofrezcan de forma explícita a un usuario para que lo visualice a cambio de desbloquear una función o un contenido específicos de un videojuego). Esta política tampoco se aplica a la monetización ni a la publicidad que no interfieran con el uso normal de la aplicación o el juego (por ejemplo, contenido de vídeo con anuncios integrados o anuncios de banner que no se muestren a pantalla completa).

Estas directrices se basan en los estándares Better Ads Experiences . Para consultar más información sobre los estándares Better Ads, visita el sitio web de Coalition for Better Ads .

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

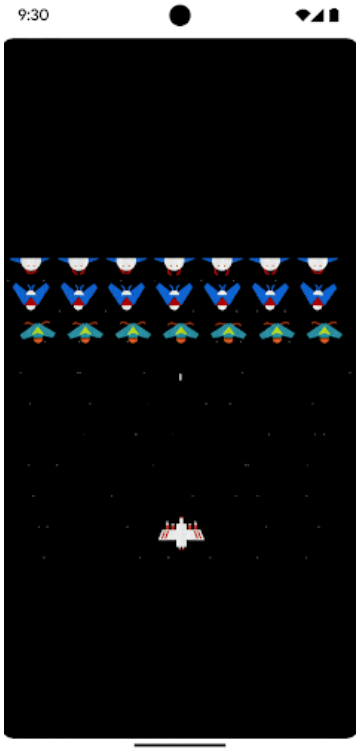
- Anuncios inesperados que aparezcan mientras se juega a un videojuego o al principio de un segmento de contenido (por ejemplo, después de que un usuario haga clic en un botón y antes de que la acción que se pretendía realizar al hacer clic en el botón haya surtido efecto). Estos anuncios son inesperados para los usuarios, ya que estos esperan interactuar con un contenido o empezar a jugar.

① Un anuncio estático inesperado aparece mientras se juega a un videojuego al principio de un nivel.



② Un anuncio en vídeo inesperado aparece durante el comienzo de un segmento de contenido.

- Un anuncio a pantalla completa que aparece mientras se juega a un videojuego y no se puede cerrar después de 15 segundos.



① Un anuncio intersticial aparece mientras se juega a un videojuego y no se ofrece a los usuarios la opción de saltárselo en un plazo de 15 segundos.

Suscripciones

Como desarrollador, no debes confundir a los usuarios sobre el contenido o los servicios de suscripción que ofreces en tu aplicación. Es fundamental que te comuniques con claridad en las pantallas de inicio o las promociones en la aplicación. No admitimos aplicaciones que permitan que los usuarios tengan experiencias de compra engañosas o manipuladoras (incluyendo las compras en la aplicación o las suscripciones).

Debes informar con transparencia sobre lo que ofreces. Esto incluye que comuniques de forma explícita los términos de la oferta, el coste de la suscripción, la frecuencia del ciclo de facturación y si hay que suscribirse para usar la aplicación. Los usuarios no deberían tener que realizar ninguna acción adicional para consultar esa información.

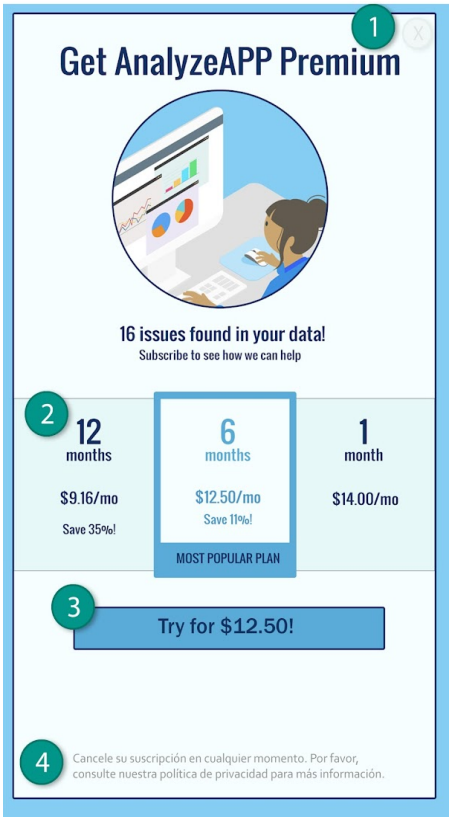
Las suscripciones deben proporcionar a los usuarios un valor constante y recurrente a lo largo de su duración, y no se pueden usar para ofrecer a los usuarios ventajas que en la práctica sean de un solo uso (por ejemplo, SKUs que ofrezcan un pago único de saldo o dinero en la aplicación, o potenciadores de un solo uso para el juego). Tu suscripción puede ofrecer bonificaciones incentivadoras o promocionales, pero estas deben ser un complemento al valor constante o recurrente proporcionado a lo largo de la duración de la suscripción**.** Los productos que no ofrezcan un valor constante y recurrente deben ser productos de compra en la aplicación en lugar de productos de suscripción.

No debes falsear ni describir de forma inexacta ventajas de un solo uso para que los usuarios crean que son suscripciones. Esto incluye modificar una suscripción para convertirla en una oferta de un solo uso (por ejemplo, cancelando, desactivando o minimizando el valor recurrente) después de que el usuario haya comprado la suscripción.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Suscripciones mensuales en las que no se informa a los usuarios de que se renovarán automáticamente y se cobrarán todos los meses.
- Suscripciones anuales en las que se destaca de forma más prominente el precio mensual.
- Términos y precios de suscripciones que no están localizados por completo.
- Promociones en la aplicación que no indican de forma clara que el usuario puede acceder al contenido sin suscribirse (si existe dicho acceso sin suscripción).
- Nombres de SKU que no representan de forma fiel el tipo de suscripción (como "Prueba gratuita" o "Prueba la suscripción premium gratis durante 3 días") en una suscripción que se cobre periódicamente.
- Mostrar varias pantallas durante el flujo de compra que lleven al usuario a hacer clic involuntariamente en el botón para suscribirse.
- Suscripciones que no proporcionan un valor constante ni recurrente, como ofrecer 1000 gemas durante el primer mes y, después, reducir la oferta a 1 gema en los siguientes meses de la suscripción.
- Requerir que el usuario se registre en una suscripción que se renueva de forma automática para conseguir una ventaja de un solo uso y cancelar la suscripción del usuario sin que lo solicite después de la compra.

Ejemplo 1:



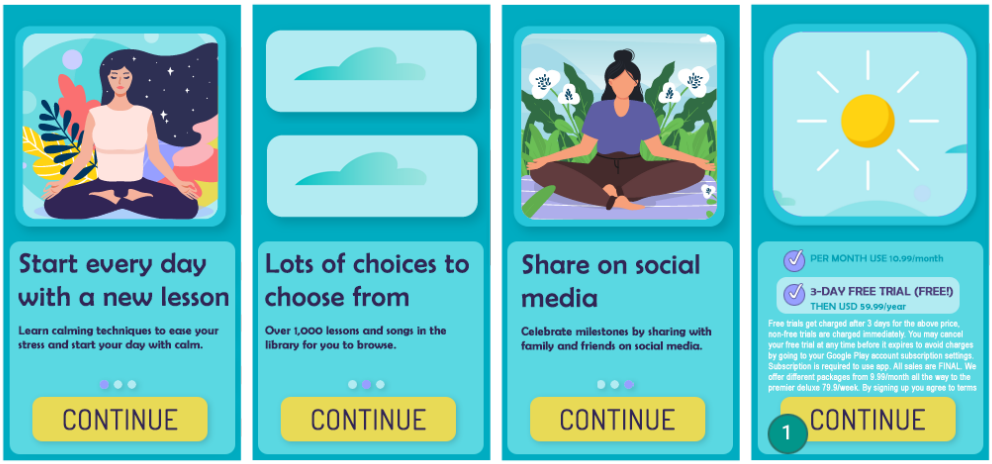
① El botón para cerrar no se ve con claridad y es posible que los usuarios no entiendan que pueden acceder a las funciones sin aceptar la oferta de suscripción.

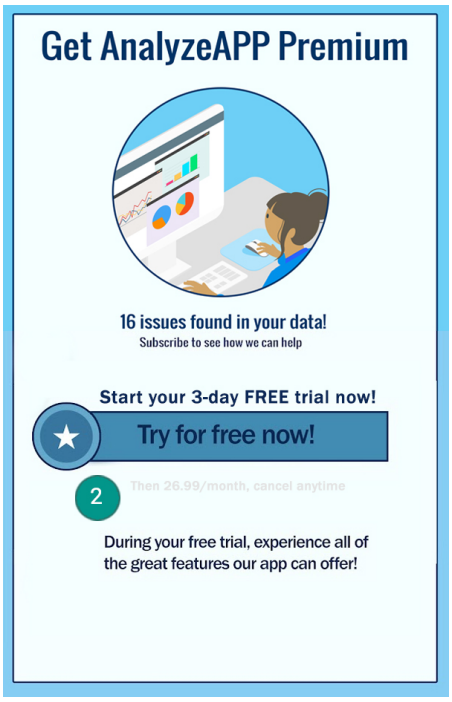
② La oferta solo muestra el precio mensual y es posible que los usuarios no entiendan que se les cobrará el importe correspondiente a seis meses al suscribirse.

③ La oferta solo muestra el precio de lanzamiento y es posible que los usuarios no sepan el importe del cargo que se realizará automáticamente al finalizar el periodo promocional.

④ La oferta debe estar localizada en el mismo idioma que los términos y condiciones para que los usuarios puedan entenderla por completo.

Ejemplo 2:





① El usuario hace clic varias veces en la misma área de botones y termina haciendo clic accidentalmente en el último botón "Continuar" para suscribirse.

② Resulta tan difícil leer el importe que se les cobrará a los usuarios cuando termine el periodo de prueba que pueden pensar que el plan no tiene ningún coste económico.

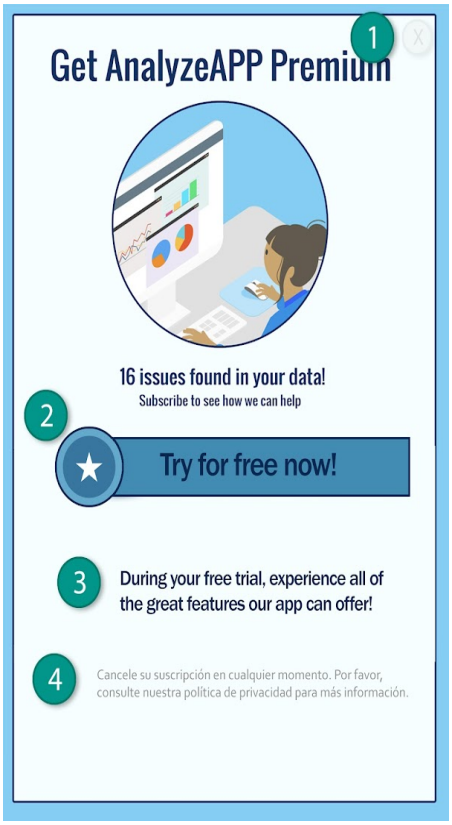
Pruebas gratuitas y precios promocionales

Antes de que un usuario se suscriba a tu contenido, debes describir de forma clara y precisa los términos de tu oferta, como la duración, el precio y la descripción del contenido o los servicios a los que podrá acceder. Asegúrate de que tus usuarios conocen cómo y cuándo se convertirá la prueba gratuita en una suscripción de pago, cuánto cuesta esta suscripción y la posibilidad de cancelar la prueba si no quieren que se convierta en una suscripción de pago.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Ofertas en las que no se especifique de forma clara la duración de la prueba gratuita ni del precio de lanzamiento.

Ofertas en las que no se explique de forma clara que el usuario se dará de alta automáticamente en una suscripción de pago al final del periodo de la oferta.
- Ofertas en las que no se indique claramente que el usuario puede acceder al contenido sin pasar por un periodo de prueba.
- Términos y precios de ofertas que no estén localizados por completo.



① El botón Cerrar no se ve con claridad y es posible que los usuarios no entiendan que pueden acceder a las funciones sin registrarse en la prueba gratuita.

② La oferta pone el énfasis en la prueba gratuita y es posible que los usuarios no entiendan que se les cobrará automáticamente al finalizar la prueba.

③ La oferta no hace referencia a un periodo de prueba y es posible que los usuarios no sepan durante cuánto tiempo tendrán acceso gratuito al contenido de la suscripción.

④ La oferta debe estar localizada en el mismo idioma que los términos y condiciones para que los usuarios puedan entenderla por completo.

Gestión de suscripciones, cancelación y reembolsos

Si vendes suscripciones en tus aplicaciones, debes asegurarte de que tus aplicaciones indiquen claramente cómo puede un usuario gestionar o cancelar su suscripción. También debes incluir en tu aplicación un acceso a un método online y fácil de usar para cancelar la suscripción. En la configuración de la cuenta de tu aplicación (u otra página equivalente), puedes cumplir este requisito incluyendo lo siguiente:

- Un enlace al Centro de Suscripciones de Google Play (en el caso de las aplicaciones que usen el sistema de facturación de Google Play); o
- Un acceso directo a tu proceso de cancelación.

Si un usuario cancela una suscripción comprada a través del sistema de facturación de Google Play, no recibirá ningún reembolso correspondiente a ese periodo de facturación, pero seguirá recibiendo el contenido vinculado a la suscripción durante el tiempo que quede de esta (independientemente de

la fecha de su cancelación), conforme a lo indicado en nuestra política. La cancelación se aplicará cuando termine el periodo de facturación actual.

Como proveedor del contenido o del acceso, puedes implementar una política de reembolsos más flexible directamente con tus usuarios. Eres responsable de notificar a los usuarios los cambios que hagas en tus políticas de suscripción, cancelación y reembolsos, así como de garantizar que estas cumplan la legislación aplicable.

En vigor desde el 1 de noviembre del 2022

Programa de SDKs de anuncios autocertificados para familias

Si publicas anuncios en tu aplicación y tu audiencia objetivo solo incluye menores de edad, tal y como se indica en la Política de Familias , entonces solo debes usar los SDKs de anuncios que cumplan los requisitos de autocertificación de las políticas de Google Play, incluidos los requisitos que se indican más abajo sobre autocertificación de SDKs de anuncios.

Si la audiencia objetivo de tu aplicación incluye tanto a menores de edad como a adultos, debes asegurarte de que los anuncios que se muestren a los menores de edad procedan exclusivamente de uno de los SDKs de anuncios autocertificados (por ejemplo, mediante la aplicación de medidas de pantalla de edad neutral). Las aplicaciones del programa Diseñado para Familias solo deben usar SDKs de anuncios autocertificados.

Recuerda que es tu responsabilidad asegurarte de que todas las versiones de SDK que implementes en tu aplicación, incluidos los SDKs de anuncios autocertificados, cumplan todas las políticas, leyes y normativas locales aplicables. Google no formula ninguna declaración ni garantía con respecto a la veracidad de la información que ofrezcan los SDKs de anuncios durante el proceso de autocertificación.

El uso de los SDKs de anuncios autocertificados para familias solo es obligatorio si utilizas SDKs de anuncios para mostrar anuncios a menores. Sin una autocertificación de Google Play de los SDKs de anuncios, está permitido hacer lo que se enumera a continuación. Sin embargo, seguirás siendo responsable de asegurarte de que el contenido de los anuncios que se publiquen y las prácticas de recogida de datos cumplan la Política de Datos de Usuario y la Política de Familias .

- Mostrar publicidad interna, si utilizas SDKs para gestionar la promoción cruzada de tus aplicaciones u otros medios y merchandising propios.
- Llegar a acuerdos directos con anunciantes por los cuales utilices SDKs para fines de gestión de inventario.

Requisitos de los SDKs de anuncios autocertificados para familias

- Define el contenido de los anuncios y los comportamientos inadecuados, y prohíbelos en los términos o las políticas de los SDKs de anuncios. Las definiciones deben cumplir las Políticas del Programa para Desarrolladores de Google Play.
- Crea un método para clasificar las creatividades de anuncio por grupos de edad. Los grupos de edad deben incluir al menos las clasificaciones Para todos y Adultos. La metodología de clasificación debe estar en consonancia con la metodología para SDKs que Google facilita cuando los desarrolladores rellenan el formulario de interés que se incluye abajo.
- Permite que los editores soliciten, bien por aplicación o mediante solicitudes individuales, la clasificación de contenido dirigido a menores de edad a la hora de publicar anuncios. Este tratamiento debe cumplir la legislación aplicable, como la ley de protección de la privacidad infantil online de EE. UU. (US Children's Online Privacy Protection Act, abreviada como COPPA) y el Reglamento General de Protección de Datos de la UE (RGPD) . Google Play requiere que los SDKs de anuncios inhabiliten los anuncios personalizados, la publicidad basada en intereses y el remarketing para obtener la clasificación de contenido dirigido a menores de edad.
- Permite que los editores seleccionen formatos de anuncio que cumplan la Política sobre Anuncios y Monetización para Familias de Google Play y los requisitos del Programa Aprobada por

profesores .

- Si se utilizan las pujas en tiempo real para mostrar anuncios a menores de edad, las creatividades deben haberse revisado y los indicadores de privacidad deben haberse propagado a los postores.
- Proporciona a Google suficiente información, por ejemplo, enviando una aplicación de prueba y la información indicada en el formulario de interés que encontrarás abajo para verificar que el SDK de anuncios cumple todos los requisitos de autocertificación de la política, y responde lo antes posible a cualquier solicitud de información posterior, como el envío de nuevas versiones para verificar que la versión del SDK de anuncios cumple todos los requisitos de autocertificación.
- Utiliza la autocertificación para acreditar que las nuevas versiones publicadas cumplen las Políticas del Programa para Desarrolladores de Google Play más recientes, incluidos los Requisitos de la política de familias.

Nota: los SDKs de anuncios autocertificados para familias deben admitir tecnologías de servicio de anuncios que cumplan todas las leyes y normativas relativas a menores de edad que puedan aplicarse a sus editores.

A continuación, incluimos los requisitos de mediación para las plataformas que muestran anuncios a menores de edad:

- Utiliza solo SDKs de anuncios autocertificados para familias de Google Play, o bien implementa las medidas de protección necesarias para que los anuncios publicados por los sistemas de mediación cumplan estos requisitos.
- Transfiere la información necesaria a las plataformas de mediación para indicar la clasificación de contenido de los anuncios y cualquier tratamiento aplicable al contenido dirigido a menores de edad.

Los desarrolladores pueden consultar la lista de SDKs de anuncios autocertificados para familias aquí .

Asimismo, los desarrolladores pueden compartir este formulario de interés con los SDKs de anuncios que quieran autocertificar.

Ficha de Play Store y promoción

La promoción y la visibilidad de tu aplicación afectan considerablemente a la calidad del servicio. Evita incluir contenido fraudulento en la ficha de Play Store, no hagas promociones de baja calidad ni intentes aumentar la visibilidad de las aplicaciones en Google Play de forma artificial.

Promoción de aplicaciones

No admitimos aplicaciones que, de forma directa o indirecta, formen parte o se beneficien de anuncios u otras actividades promocionales que resulten engañosas o dañinas para los usuarios o para el ecosistema de desarrolladores. Las actividades promocionales son engañosas o dañinas si su comportamiento o contenido infringe nuestras Políticas del Programa para Desarrolladores.

Ejemplos de infracciones habituales:

- Uso de publicidad engañosa en sitios web, aplicaciones u otras propiedades, como notificaciones que sean similares a las del sistema y las alertas.
- Uso de anuncios sexualmente explícitos con el fin de dirigir a los usuarios a la ficha de Play Store de tu aplicación para que la descarguen.
- Técnicas de promoción o instalación que redireccionen a los usuarios a Google Play o que descargan aplicaciones sin informar al usuario.
- Promociones no solicitadas a través de servicios SMS.

Debes asegurarte de que las redes publicitarias, los afiliados o los anuncios asociados a tu aplicación cumplan estas políticas.

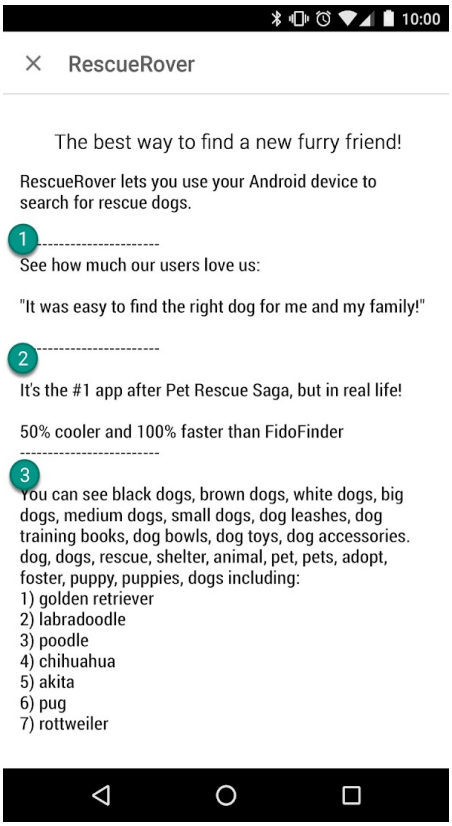
Metadatos

No admitimos aplicaciones con metadatos irrelevantes, excesivos, inadecuados, no descriptivos, engañosos o con formato erróneo, lo que incluye la descripción, el nombre del desarrollador, el título, el icono, las capturas de pantalla y las imágenes promocionales de la aplicación, entre otros. Los desarrolladores deben proporcionar una descripción clara y bien redactada de su aplicación. Tampoco admitimos que en la descripción de la aplicación aparezcan testimonios de usuarios anónimos o no atribuidos a nadie.

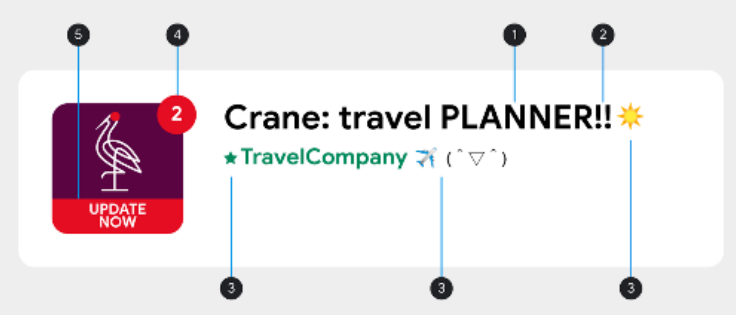
El título, el icono y el nombre del desarrollador de tu aplicación sirven especialmente de ayuda a los usuarios a la hora de encontrar tu aplicación e informarse sobre ella. No uses emojis, emoticonos ni caracteres especiales repetidos en estos elementos de metadatos. Evita escribir todo en MAYÚSCULAS a menos que aparezca así en el nombre de tu marca. No se admiten símbolos engañosos en los iconos de las aplicaciones, como, por ejemplo, un punto que indique que hay nuevos mensajes cuando no hay mensajes nuevos o símbolos de descarga o instalación cuando la aplicación no tiene relación con la descarga de contenido. El título de tu aplicación debe tener 30 caracteres como máximo.

Además de los requisitos aquí indicados, es posible que debas proporcionar información adicional sobre metadatos de acuerdo con la Política para Desarrolladores de Play.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.



① Testimonios de usuarios no atribuidos a nadie o anónimos
② Comparación de datos de aplicaciones o marcas
③ Bloques de palabras y listas de palabras horizontales y verticales



① Escribir en MAYÚSCULAS sin que el nombre de la marca esté así
② Secuencias de caracteres especiales que no son relevantes para la aplicación
③ Uso de emojis, emoticonos (incluidos kaomojis) y caracteres especiales
④ Símbolos engañosos
⑤ Texto engañoso

A continuación te indicamos algunos ejemplos de texto, imágenes o vídeos inadecuados de tu ficha:

- Imágenes o vídeos de carácter sexual. Evita imágenes sugerentes que incluyan pechos, nalgas, genitales u otro tipo de zona corporal o de contenido que se consideren fetiche, ya sea de forma ilustrada o real.
- Usar palabras malsonantes o lenguaje vulgar o de otro tipo inapropiado para la audiencia general en la ficha de Play Store de tu aplicación.
- Violencia gráfica representada de forma clara en iconos de aplicaciones, imágenes promocionales o vídeos.
- Representación del consumo ilícito de drogas. Incluso el contenido pedagógico, documental, científico o artístico debe ser adecuado para todos los públicos en la ficha de Play Store.

A continuación te mostramos algunos ejemplos de prácticas recomendadas:

- Destaca las virtudes de tu aplicación. Comparte información interesante y atractiva sobre tu aplicación para que los usuarios comprendan por qué es especial.
- Comprueba que el título y la descripción de tu aplicación describan de forma precisa sus funciones.
- Evita el uso de palabras clave y referencias que se repitan o que no guarden relación con la aplicación.
- La descripción de tu aplicación debe ser concisa y clara. Las descripciones breves suelen mejorar la experiencia de usuario, especialmente en los dispositivos con pantallas pequeñas. La información excesiva, un texto demasiado largo, el formato inadecuado y las repeticiones pueden suponer una infracción de esta política.
- Recuerda que la ficha debe ser apta para todos los públicos. Evita utilizar texto, imágenes o vídeos inadecuados en la ficha y cumple las directrices que se indican arriba.

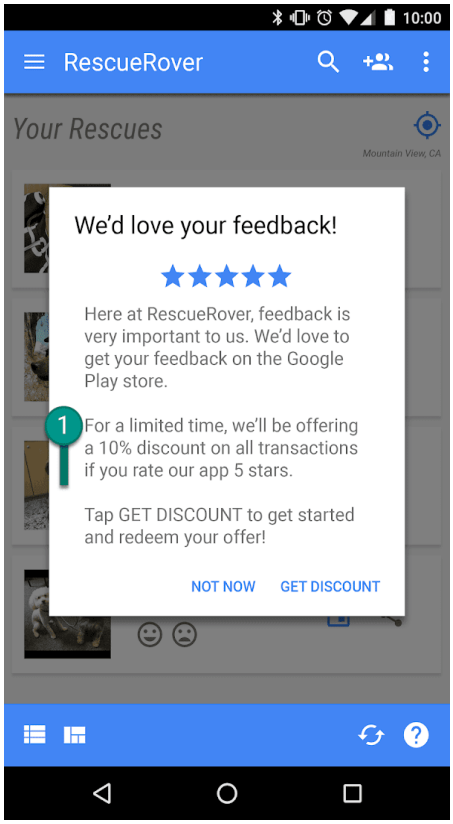
Valoraciones de los usuarios, reseñas y descargas

Los desarrolladores no deben intentar amañar el posicionamiento de ninguna aplicación en Google Play. Esto significa que, entre otras cosas, no se deben inflar de forma ilegítima los datos sobre las valoraciones, las reseñas ni los recuentos de descargas de productos (por ejemplo, mediante valoraciones, reseñas o descargas fraudulentas o incentivadas). Las descargas, reseñas y valoraciones incentivadas incluyen el uso de texto o imágenes en el título, el icono o el nombre del desarrollador de tu aplicación para indicar el precio u otra información promocional.

Los desarrolladores no deben añadir texto ni imágenes que hagan referencia al rendimiento o la clasificación de la aplicación en Play Store, ni sugerir vínculos con otros programas de Google Play en el título, el icono o el nombre del desarrollador de la aplicación.

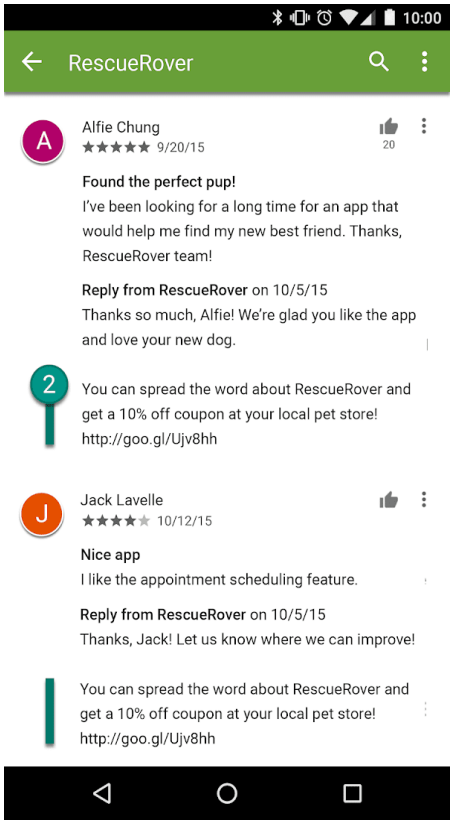
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- En este ejemplo se pide a los usuarios que valoren la aplicación a cambio de un incentivo:



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

- Valorar repetidamente la aplicación para modificar su ubicación en Google Play.
- Publicar reseñas que incluyan contenido inadecuado (o animar a los usuarios a hacerlo). Esto incluye entidades asociadas, cupones, códigos de juegos, direcciones de correo electrónico y enlaces a sitios web o a otras aplicaciones:



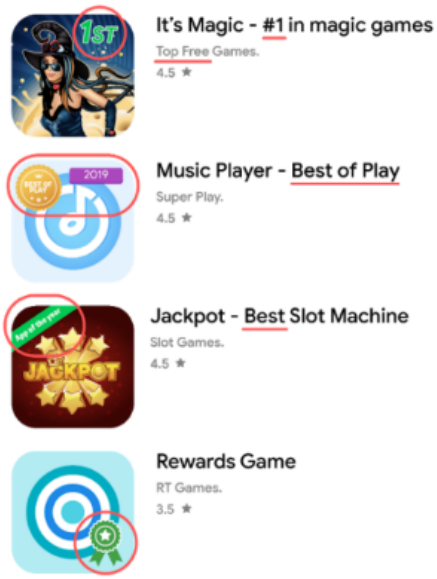
② Esta reseña ofrece un cupón para animar a los usuarios a promocionar la aplicación RescueRover.

Las valoraciones y las reseñas son referencias sobre la calidad de una aplicación; por lo tanto, los usuarios deben poder considerarlas auténticas y relevantes. A continuación te mostramos algunas prácticas recomendadas para responder a las opiniones de los usuarios:

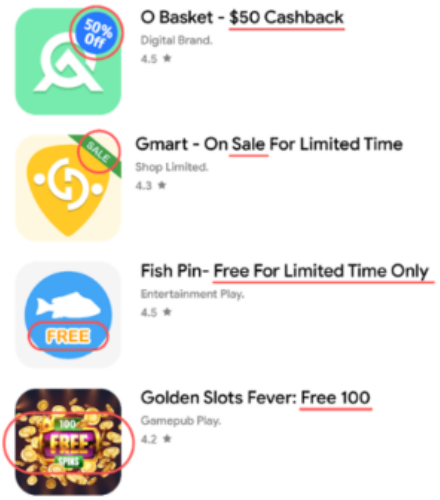
- Centra tu respuesta en solucionar los problemas que comentan los usuarios y no pidas una valoración más alta.
- Incluye referencias a recursos útiles, como una dirección de asistencia o una página de preguntas frecuentes.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

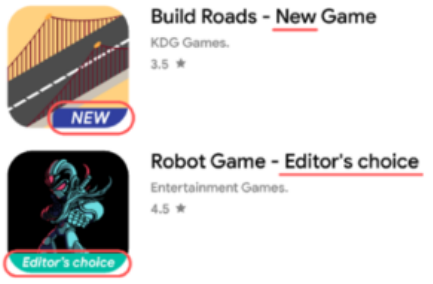
- Imágenes o texto que hagan referencia al rendimiento o la clasificación de la aplicación en Play Store, como "Aplicación del año", "N.º 1", "Lo mejor de Play en el 20XX", iconos de reconocimiento de tipo "Popular", etc.



- Imágenes o texto que indiquen el precio o información promocional, como "Descuento del 10 %", "Devolución de 50 $ en efectivo", "Gratis solo durante un tiempo limitado", etc.



- Imágenes o texto que hagan referencia a programas de Play, como "Selección de nuestros expertos", "Novedad", etc.



Clasificaciones del contenido

Las clasificaciones del contenido que aparecen en Google Play las proporciona la Coalición Internacional de Clasificación por Edad (IARC) y están diseñadas para que los desarrolladores puedan ofrecer a los usuarios clasificaciones del contenido pertinentes según su ubicación. Las autoridades regionales de la IARC disponen de directrices que se usan para determinar el nivel de madurez del contenido de una aplicación. No admitimos aplicaciones sin clasificación del contenido en Google Play.

Cómo se utilizan las clasificaciones del contenido

Las clasificaciones del contenido se utilizan para informar a los consumidores, especialmente a madres, padres o tutores, del contenido potencialmente inadecuado que incluye una aplicación. También ayudan a filtrar o bloquear tu contenido en territorios concretos o para usuarios específicos cuando la ley así lo exija y para determinar si tu aplicación cumple los requisitos para participar en programas especiales para desarrolladores.

Cómo se asignan las clasificaciones del contenido

Para recibir la clasificación del contenido, debes rellenar un cuestionario de clasificación en Play Console sobre la naturaleza del contenido de tus aplicaciones. En función de tus respuestas, se asignará a la aplicación una clasificación del contenido de distintas autoridades de clasificación. Si incluyes información falsa sobre el contenido de la aplicación, esta se podrá suspender o retirar, por lo que es importante que proporciones respuestas precisas en el cuestionario de clasificación de contenido.

Para evitar que tu aplicación incluya la etiqueta "Sin clasificar", debes completar el cuestionario de clasificación del contenido para cada aplicación nueva que envíes a Play Console, así como para todas las aplicaciones que ya estén activas en Google Play. Las aplicaciones sin clasificación del contenido se retirarán de Play Store.

Si haces cambios en el contenido o en las funciones de la aplicación, y estos cambios afectan a las respuestas del cuestionario de clasificación, deberás rellenar y enviar un nuevo cuestionario en Play Console.

Visita el Centro de Ayuda para consultar más información sobre las diferentes autoridades de clasificación y sobre cómo completar el cuestionario de clasificación del contenido.

Apelaciones de clasificaciones

Si no estás de acuerdo con la clasificación que se ha asignado a tu aplicación, puedes apelar directamente a la autoridad de clasificación IARC a través del enlace proporcionado en el correo electrónico del certificado.

Noticias

Una aplicación de noticias es una aplicación que:

- O bien se declara como aplicación de "Noticias" en Google Play Console.
- O bien se incluye en la categoría "Noticias y revistas" de Google Play Store y se describe como aplicación de noticias en el título, el icono, el nombre de desarrollador o la descripción de la aplicación.

Ejemplos de aplicaciones en la categoría "Noticias y revistas" que cumplen los requisitos para considerarse como de noticias:

- Las aplicaciones que se describen como de "noticias" en su descripción, entre los que se incluyen los siguientes ejemplos:
  - Últimas noticias
  - Periódico
  - Noticias de última hora
  - Noticias locales
  - Noticias del día
- Aplicaciones con la palabra "noticias" en el título, el icono o el nombre del desarrollador de la aplicación.

Sin embargo, si las aplicaciones incluyen principalmente contenido generado por usuarios (como las aplicaciones de redes sociales), no se deben declarar como aplicación de noticias, y no se consideran como tales.

Las aplicaciones de noticias que requieren que el usuario compre una suscripción deben proporcionar a los usuarios una vista previa del contenido en la aplicación antes de la compra.

Las aplicaciones de noticias deben, en todos los casos:

- Proporcionar información sobre la propiedad de la aplicación y la fuente de los artículos de noticias, incluidos, entre otros, el editor o el autor originales de cada artículo. En los casos en los que no sea habitual añadir los autores de cada artículo, la aplicación de noticias debe ser el editor original de los artículos. Ten en cuenta que los enlaces a cuentas de redes sociales no son una forma suficiente de publicar información de los autores o editores.
- Tener un sitio web específico o una página en la aplicación en los que se indique claramente que se incluye información de contacto, que sean fáciles de encontrar (por ejemplo, mediante un enlace al final de la página principal o en la barra de navegación del sitio) y que proporcionen información de contacto válida del editor de prensa, incluidos una dirección de correo o un número de teléfono de contacto. Ten en cuenta que los enlaces a cuentas de redes sociales no son una forma aceptable de publicar información de contacto de los editores.

Las aplicaciones de noticias no deben, en ningún caso:

- Contener errores ortográficos ni gramaticales graves.
- Incluir solamente contenido estático (por ejemplo, contenido con más tres meses de antigüedad).
- Tener como propósito principal el marketing de afiliación ni los ingresos publicitarios.

Ten en cuenta que las aplicaciones de noticias *pueden* usar anuncios y otros contenidos de marketing para obtener ingresos, siempre y cuando el propósito principal de la aplicación no sea vender productos y servicios ni generar ingresos publicitarios.

Las Aplicaciones de Noticias que agregan contenido de diferentes fuentes deben ser transparentes con respecto a la fuente de publicación del contenido incluido en la aplicación, y cada una de las fuentes debe cumplir los requisitos de la política para Aplicaciones de Noticias.

Consulta este artículo para ver la mejor forma de proporcionar la información necesaria.

Spam y funcionalidad mínima

At a minimum, apps should provide users with a basic degree of functionality and a respectful user experience. Apps that crash, exhibit other behavior that is not consistent with a functional user experience, or that serve only to spam users or Google Play are not apps that expand the catalog in a meaningful way.

Spam

No admitimos aplicaciones que envíen spam a los usuarios o a Google Play, como aplicaciones que manden mensajes no deseados a los usuarios o aplicaciones que estén repetidas o sean de baja calidad.

Spam a través de mensajes

No admitimos aplicaciones que envíen SMS, correos electrónicos ni otros mensajes en nombre del usuario sin ofrecerle la posibilidad de confirmar el contenido y los destinatarios.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

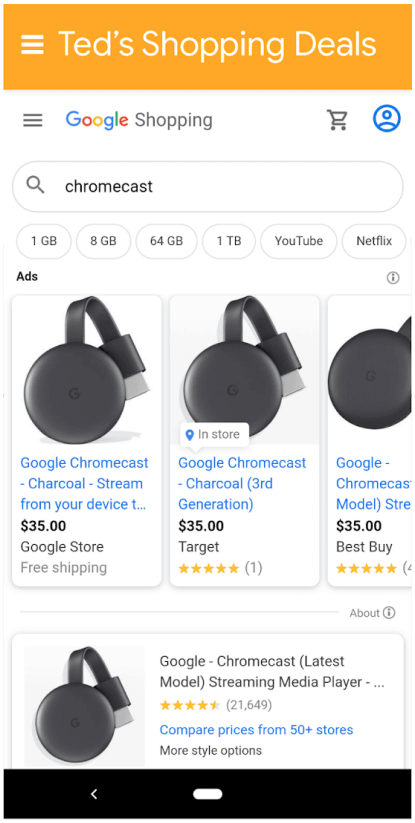
- Cuando el usuario pulsa el botón "Compartir", la aplicación envía mensajes en nombre del usuario sin ofrecerle la posibilidad de confirmar el contenido ni los destinatarios.

Spam de afiliados y de vistas web

No admitimos aplicaciones cuyo fin principal sea redirigir el tráfico a un sitio web o proporcionar una vista web de un sitio sin permiso de su propietario o administrador.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Una aplicación cuyo fin principal sea redirigir el tráfico de referencia a un sitio web para obtener el crédito por los registros o las compras de ese sitio web
- Aplicaciones cuyo fin principal sea proporcionar una WebView de un sitio web sin permiso:



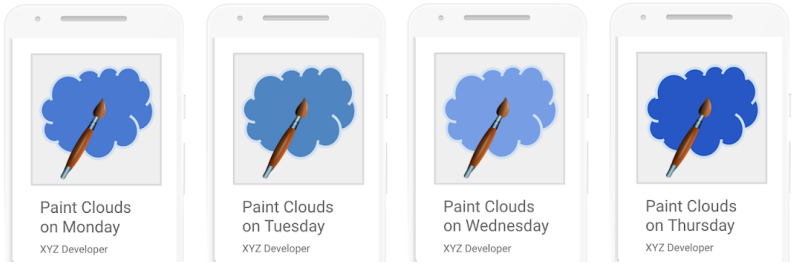
① Esta aplicación se llama "Ted's Shopping Deals" y lo único que hace es proporcionar una WebView de Google Shopping.

Contenido repetitivo

No admitimos aplicaciones que simplemente proporcionen la misma experiencia que otras aplicaciones ya disponibles en Google Play. Las aplicaciones deben ofrecer valor a los usuarios mediante la creación de contenido o servicios únicos.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Copiar contenido de otras aplicaciones sin añadir valor ni contenido original.
- Crear varias aplicaciones con funcionalidad, contenido y experiencia de usuario muy similares. Si estas aplicaciones ofrecen poco contenido, se recomienda a los desarrolladores que creen una sola aplicación que englobe todo el contenido.



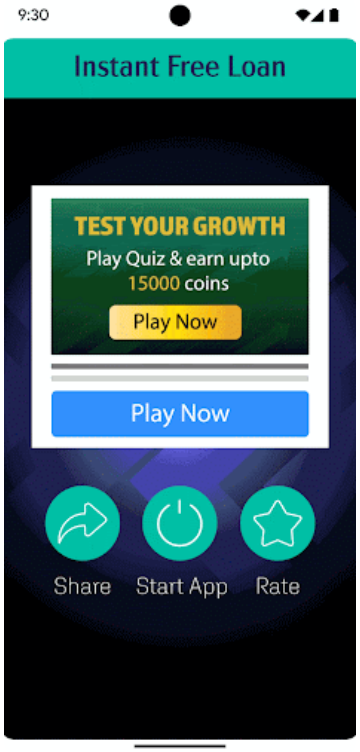
Contenido de anuncios

No admitimos aplicaciones que muestren anuncios intersticiales repetidamente que desvíen la atención de los usuarios al interactuar con la aplicación y realizar tareas dentro de esta.

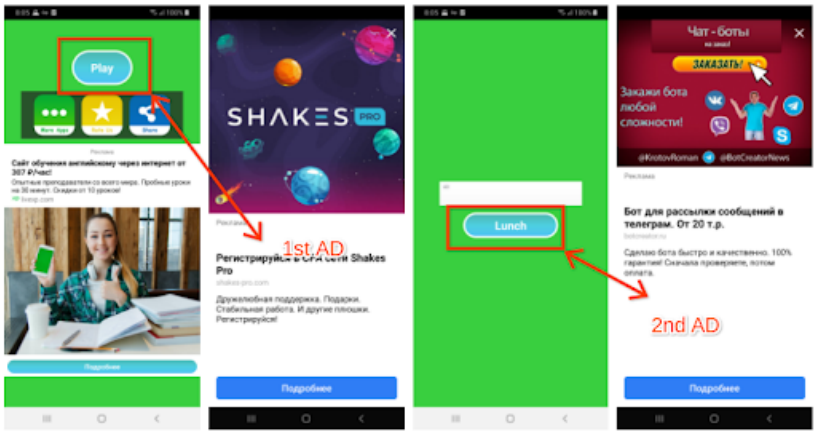
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros

usuarios.

- Las aplicaciones en las que se coloque un anuncio intersticial después de una acción del usuario (incluidas, entre otras, hacer clic, deslizar el dedo, etc.) de forma consecutiva.



La primera página dentro de la aplicación tiene varios botones para interactuar. Cuando el usuario hace clic en **Iniciar app** para usar la aplicación, aparece un anuncio intersticial emergente. Después de cerrar el anuncio, el usuario vuelve a la aplicación y hace clic en **Servicio** para comenzar a usar el servicio, pero entonces aparece otro anuncio intersticial.



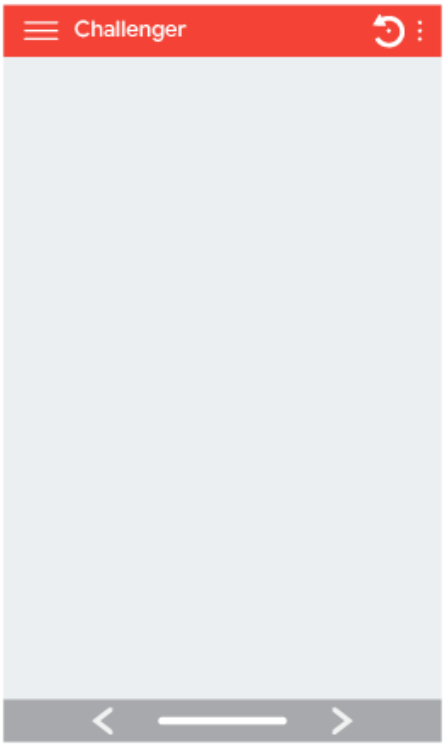
En la primera página, se guía al usuario para que haga clic en **Jugar** porque este es el único botón disponible para usar la aplicación. Cuando el usuario hace clic en ese botón, aparece un anuncio intersticial. Después de cerrar el anuncio, el usuario hace clic en **Iniciar**, porque es el único botón con el que se puede interactuar, y aparece otro anuncio intersticial emergente.

Funcionalidad mínima

Tu aplicación debe ofrecer una experiencia de usuario atractiva, estable y adaptable.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que están diseñadas para no hacer nada o que no tienen ninguna función



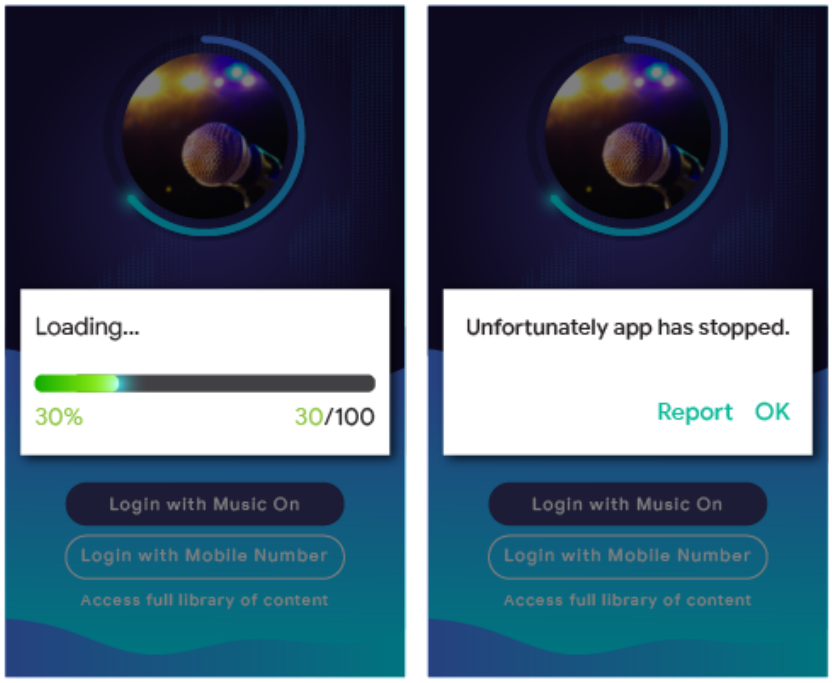
Funcionalidad defectuosa

No admitimos aplicaciones que fallen, se cierren, se bloqueen o no funcionen con normalidad.

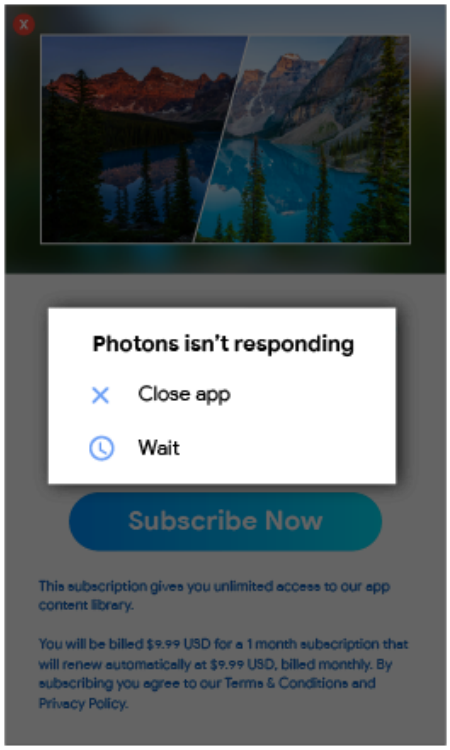
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que **no se instalan**

- Aplicaciones que se instalan, pero **no se cargan**



- Aplicaciones que se cargan, pero **no responden**



Otros programas

Las aplicaciones diseñadas para otras experiencias de Android y distribuidas a través de Google Play, además de estar sujetas a las políticas de contenido establecidas en este Centro de políticas, es

posible que deban cumplir requisitos de políticas específicas de otros programas. Revisa la lista que se incluye abajo para determinar si tu aplicación debe cumplir alguna de estas políticas.

Aplicaciones Instantáneas Android

Con las Aplicaciones Instantáneas Android pretendemos crear una experiencia de usuario atractiva y fluida, así como cumplir con los estándares más elevados de privacidad y seguridad. Hemos diseñado nuestras políticas para conseguir esos objetivos.

Los desarrolladores que decidan distribuir Aplicaciones Instantáneas Android a través de Google Play deben cumplir con las siguientes políticas, además del resto de Políticas del Programa para Desarrolladores de Google Play.

Identidad

Los desarrolladores deben integrar Smart Lock para contraseñas en las aplicaciones instantáneas que incluyan la función de inicio de sesión.

Enlaces compatibles

Los desarrolladores de Aplicaciones Instantáneas Android deben admitir los enlaces a otras aplicaciones. Si las aplicaciones instantáneas o instaladas del desarrollador contienen enlaces que puedan dirigir a una aplicación instantánea, el desarrollador debe dirigir a los usuarios a esa aplicación en lugar de, por ejemplo, capturar los enlaces en un WebView .

Especificaciones técnicas

Los desarrolladores deben cumplir las especificaciones técnicas de las Aplicaciones Instantáneas Android y los requisitos proporcionados por Google, incluidos los que aparecen en la documentación pública . Estos pueden sufrir modificaciones de forma ocasional.

Propuesta de instalación de la aplicación

La aplicación instantánea puede ofrecerle al usuario una que se puede instalar, pero este no debe ser su objetivo principal. Cuando ofrezcan instalar una aplicación, los desarrolladores:

- Deben utilizar el icono de "descargar aplicación" de Material Design y la etiqueta "instalar" en el botón de instalación.
- No pueden incluir más de dos o tres solicitudes implícitas de instalación en la aplicación instantánea.
- No deben utilizar un banner ni ningún tipo de técnica de anuncio para mostrar solicitudes de instalación a los usuarios.

Si quieres obtener más información sobre las aplicaciones instantáneas y las directrices de experiencia de usuario, consulta las prácticas recomendadas de experiencia de usuario .

Cambios en el estado del dispositivo

Las aplicaciones instantáneas no deben realizar cambios en el dispositivo del usuario que duren más que la sesión de la aplicación instantánea. Por ejemplo, no pueden cambiar el fondo de pantalla del usuario ni crear un widget en la pantalla de inicio.

Visibilidad de las aplicaciones

Los desarrolladores deben asegurarse de que el usuario pueda ver las aplicaciones instantáneas, de forma que sepa en todo momento que se están ejecutando en su dispositivo.

Identificadores de dispositivo

Las aplicaciones instantáneas no deben acceder a los identificadores de dispositivo que permanezcan después de que la aplicación instantánea haya dejado de ejecutarse y que el usuario no pueda restablecer. A continuación se indican algunos ejemplos:

- Build Serial
- Direcciones Mac de cualquier chip de red
- IMEI e IMSI

Las aplicaciones instantáneas pueden acceder al número de teléfono si lo obtienen con el permiso de tiempo de ejecución. El desarrollador no debe intentar identificar al usuario mediante estos identificadores ni de ninguna otra forma.

Tráfico de red

El tráfico de red de la aplicación instantánea debe cifrarse con un protocolo TLS, como HTTPS.

Política de emojis de Android

El objetivo de nuestra política de emojis es promocionar una experiencia de usuario inclusiva y coherente. Para lograr dicho objetivo, todas las aplicaciones que se ejecuten en Android 12 o versiones posteriores deben ser compatibles con la última versión de los emojis Unicode .

Las aplicaciones que usan los emojis predeterminados de Android sin implementaciones personalizadas ya usan la última versión de los emojis Unicode si se ejecutan en Android 12 o versiones posteriores.

Las aplicaciones con implementaciones de emojis personalizadas (por ejemplo, las incluidas como parte de bibliotecas de terceros), deben ser totalmente compatibles con la última versión de Unicode si se ejecutan en Android 12 o versiones posteriores en un plazo de 4 meses desde la publicación de la nueva versión de los emojis Unicode.

Consulta esta guía para descubrir cómo admitir los emojis más recientes.

Usa estos ejemplos de emojis para comprobar si tu aplicación es compatible con la versión más reciente de Unicode:

Ejemplos	Versión de Unicode
🫠 🫱🏽 🫰🏽	14.0
🫨 👩🏿 👩🏿‍❤️‍👩🏿	13.1
🥲 🫅🏿 🐻‍❄️	13.0
🧑‍🦰 🚶‍♀️ 👫	12.1
🦩 🫅🏿 👭	12.0

Familias

Google Play ofrece una avanzada plataforma para que los desarrolladores puedan mostrar contenido de alta calidad y adecuado según la edad para todos los miembros de la familia. Antes de enviar una aplicación al programa Diseñado para Familias o enviar a Google Play Store una aplicación dirigida a niños, debes asegurarte de que tu aplicación sea adecuada para niños y de que cumpla toda la legislación aplicable.

Consulta información sobre el proceso del contenido familiar y revisa la lista de comprobación interactiva en Academia de Aplicaciones.

Crear aplicaciones para niños y familias

Las familias usan cada vez más la tecnología y los padres buscan contenido seguro y de calidad para compartirlo con sus hijos. Puede que estés diseñando aplicaciones específicamente para niños o que solo quieras llamar su atención. En cualquier caso, Google Play te ayuda a asegurarte de que sean seguras para todos los usuarios, incluidas las familias.

La palabra "niños" hace referencia a distintos conceptos en diferentes idiomas y contextos. Es importante que te pongas en contacto con tu asesor legal para determinar las obligaciones o restricciones de edad que pueden afectar a tu aplicación. Eres quien mejor sabe cómo funciona tu aplicación, por lo que confiamos en que nos ayudes a que las aplicaciones que se ofrecen en Google Play sean seguras para las familias.

Las aplicaciones diseñadas específicamente para niños deben participar en el programa Diseñado para Familias. Si tu aplicación está dirigida tanto a niños como a adultos, puedes participar en el programa Diseñado para Familias. Todas las aplicaciones que participen en el programa Diseñado para Familias podrán clasificarse en el Programa Aprobada por profesores, pero no podemos garantizar que se incluyan en dicho programa. Aunque decidas no participar en el programa Diseñado para Familias, tendrás que cumplir los requisitos de la Política de Familias de Google Play que se indican más abajo, así como las Políticas del Programa para Desarrolladores de Google Play y el Acuerdo de Distribución para Desarrolladores.

Requisitos de Play Console

Contenido y audiencia objetivo

En la sección Contenido y audiencia objetivo de Google Play Console, debes indicar la audiencia objetivo de tu aplicación antes de publicarla. Para ello, selecciona uno de los grupos de edad disponibles en la lista. Independientemente de lo que especifiques en Google Play Console, si decides incluir en tu aplicación imágenes y terminología que puedan considerarse como dirigidas a niños, podría afectar en la evaluación que lleve a cabo Google Play sobre tu audiencia objetivo. Google Play se reserva el derecho de revisar la información de la aplicación para determinar si has elegido la audiencia objetivo adecuada.

Si seleccionas una audiencia objetivo que solo incluya adultos, pero Google determina que esta información no es precisa porque tu aplicación también va dirigida a niños, tendrás la opción de incluir una etiqueta de advertencia para dejar claro que tu aplicación no está dirigida a niños.

Solo debes seleccionar más de un grupo de edad como audiencia objetivo de tu aplicación si la has diseñado para usuarios de esos grupos y es adecuada para ellos. Por ejemplo, las aplicaciones diseñadas para bebés y niños en edad preescolar solo deben incluir el grupo de edad objetivo "Hasta 5 años". Si tu aplicación está diseñada para un nivel académico determinado, elige el grupo de edad que mejor lo represente. Solo debes seleccionar grupos de edad que incluyan tanto niños como adultos si tu aplicación va realmente dirigida a todas las edades.

Actualizaciones de la sección Contenido y audiencia objetivo

Puedes actualizar la información de tu aplicación en la sección Contenido y audiencia objetivo de Google Play Console en cualquier momento. Para que esta información se muestre en Google Play Store, primero debes actualizar la aplicación. No obstante, cualquier cambio que hagas en esta sección de Google Play Console se podrá revisar para comprobar si cumple las políticas incluso antes de que actualices la aplicación.

Te recomendamos encarecidamente que avises a tus usuarios si cambias el grupo de edad objetivo de tu aplicación o empiezas a usar anuncios o compras en la aplicación. Puedes hacerlo a través de la sección "Novedades" de tu ficha de Play Store o mediante notificaciones en la aplicación.

Información falsa en Play Console

Si incluyes información falsa sobre tu aplicación en Play Console, incluyendo en la sección Contenido y audiencia objetivo, es posible que se retire o se suspenda tu aplicación. Por eso, es importante que proporciones información veraz.

Requisitos de la Política de Familias

Si una de las audiencias objetivo de tu aplicación son los menores de edad, debes cumplir los siguientes requisitos. De lo contrario, tu aplicación se podrá retirar o suspender.

1. **Contenido de la aplicación:** el contenido de tu aplicación al que pueden acceder menores de edad debe ser adecuado para ellos. Si tu aplicación incluye contenido que no es adecuado en todo el mundo, pero ese contenido se considera adecuado para usuarios menores de edad en una región en concreto, es posible que la aplicación esté disponible en esa región (regiones limitadas), pero seguirá sin estar disponible en otras regiones.
2. **Funcionalidad de la aplicación:** tu aplicación no puede limitarse a proporcionar una vista web de un sitio ni tener como finalidad principal redirigir el tráfico de afiliados a un sitio web, independientemente de a quién pertenezca el sitio.
   - Trabajamos constantemente para encontrar otras maneras de ofrecer nuevas experiencias a los desarrolladores de aplicaciones para menores de edad. Si te interesa participar en nuestra prueba piloto de aplicaciones web educativas de confianza, háznoslo saber aquí .
3. **Respuestas de Play Console:** debes responder de forma precisa a las preguntas sobre tu aplicación en Play Console y actualizar las respuestas si haces algún cambio en tu aplicación. Esto incluye, entre otras cosas, especificar de forma precisa los elementos interactivos de tu aplicación en el cuestionario de clasificación del contenido. Por ejemplo:
   - Si los usuarios de tu aplicación pueden interactuar con el contenido o intercambiar información.
   - Si tu aplicación comparte con terceros información proporcionada por los usuarios.
   - Si tu aplicación comparte la ubicación física de los usuarios con otros usuarios.
4. **Anuncios:** si tu aplicación muestra anuncios a menores de edad o a usuarios de edad desconocida, debes:
   - Usar únicamente SDKs de anuncios certificados por Google Play para mostrar anuncios a esos usuarios.
   - Asegurarte de que los anuncios que se muestren a esos usuarios no estén basados en intereses (publicidad orientada a usuarios individuales que tienen determinadas características y en función de su comportamiento de navegación online) ni utilicen el remarketing (publicidad orientada a usuarios individuales en función de interacciones anteriores con una aplicación o un sitio web).
   - Asegurarte de que el contenido de los anuncios que se muestren a esos usuarios sea adecuado para menores de edad.
   - Asegurarte de que los anuncios que se muestren a esos usuarios sigan los requisitos de formato de anuncios para familias.
   - Cumplir con todas las obligaciones legales y normas del sector referentes a la publicidad dirigida a menores.
5. **Prácticas relacionadas con datos:** debes especificar si recoges en tu aplicación algún tipo de información personal y sensible de menores de edad, incluidos los datos recogidos a través de APIs y SDKs que se usen o a los que se llame desde tu aplicación. La información sensible de menores de edad incluye, entre otros datos, información de autenticación, datos de detección mediante cámaras y micrófonos, datos de dispositivos, el ID de Android y datos de uso de anuncios. Debes asegurarte también de que tu aplicación siga estas prácticas relacionadas con datos:
   - Las aplicaciones dirigidas únicamente a menores de edad no deben transmitir el identificador de publicidad de Android (AAID), el número de serie de la SIM, el número de serie de la compilación, el BSSID, la dirección MAC, el SSID, el IMEI ni el IMSI.

- Las aplicaciones dirigidas tanto a menores de edad como a otros públicos no deben transmitir el AAID, el número de serie de la SIM, el número de serie de la compilación, el BSSID, la dirección MAC, el SSID, el IMEI, ni el IMSI de menores de edad o de usuarios de edad desconocida.
- El número de teléfono del dispositivo no se debe solicitar desde la clase TelephonyManager de la API de Android.
- Las aplicaciones orientadas únicamente a menores de edad no pueden solicitar permisos de ubicación, ni recoger, usar ni transmitir la ubicación precisa .
- Las aplicaciones deben usar Companion Device Manager (CDM) cuando soliciten acceso al Bluetooth, a menos que tu aplicación solo esté destinada a versiones del sistema operativo del dispositivo que no sean compatibles con CDM.

6. **APIs y SDKs:** tu aplicación debe implementar cualquier API o SDK correctamente.
   - Las aplicaciones dirigidas únicamente a menores de edad no deben contener APIs ni SDKs que no estén aprobados para su uso en servicios principalmente orientados a menores de edad. Entre ellos se incluyen el inicio de sesión de Google (o cualquier otro servicio de API de Google que acceda a datos asociados a una cuenta de Google), los Servicios de Juegos de Google Play y cualquier otro servicio de API que use tecnología OAuth para autenticar a los usuarios y obtener autorizaciones.
   - Las aplicaciones dirigidas tanto a menores de edad como a adultos no deben implementar APIs ni SDKs cuyo uso no se haya aprobado para servicios dirigidos a menores de edad, a menos que se utilicen con una pantalla de edad neutral o que se implementen de forma que no se recojan datos de menores de edad. Las aplicaciones dirigidas tanto a menores de edad como a adultos no deben requerir que los usuarios inicien sesión o accedan a contenido de aplicaciones a través de una API o un SDK que no esté aprobado para su uso en servicios dirigidos a menores de edad.
7. **Realidad aumentada:** si tu aplicación usa realidad aumentada, debes incluir una advertencia de seguridad que se muestre inmediatamente al abrir la sección de realidad aumentada. La advertencia debe contener lo siguiente:
   - Un mensaje adecuado sobre la importancia de la supervisión parental.
   - Un recordatorio sobre los riesgos físicos del mundo real (por ejemplo, la necesidad de prestar atención al entorno).
   - Tu aplicación no debe requerir el uso de un dispositivo no recomendado para menores de edad (por ejemplo, Daydream u Oculus).
8. **Aplicaciones y funciones sociales:** si tus aplicaciones permiten que los usuarios compartan o intercambien información, debes describir con exactitud estas funciones en el cuestionario de clasificación del contenido de Play Console.
   - Aplicaciones sociales: son las aplicaciones que se centran en permitir que los usuarios compartan contenido libremente o que se comuniquen con grupos grandes de personas. Todas las aplicaciones sociales que incluyan a menores de edad en su audiencia objetivo deben mostrar un recordatorio en la aplicación para indicarles que tomen medidas destinadas a proteger su seguridad en Internet, y también para recordarles los riesgos del mundo real asociados a las interacciones online antes de permitir que usuarios menores de edad intercambien contenido multimedia o información libremente. Además, la aplicación también debe requerir la intervención de un adulto para permitir que usuarios menores de edad intercambien información personal.
   - Funciones sociales: es la funcionalidad adicional de una aplicación que permite que los usuarios compartan contenido libremente o que se comuniquen con grupos grandes de personas. Todas las aplicaciones que incluyan menores de edad en su audiencia objetivo y tengan funciones sociales deben mostrar un recordatorio en la aplicación para indicarles que tomen medidas destinadas a proteger su seguridad en Internet, y también para recordarles los riesgos del mundo real asociados a las interacciones online antes de permitir que usuarios menores de edad intercambien contenido multimedia o información libremente. Además, la aplicación también debe proporcionar un método que permita a los adultos gestionar las funciones sociales de los

usuarios menores de edad, incluidos, entre otros, un método para habilitar o inhabilitar las funciones sociales o un método para seleccionar distintos niveles de funcionalidad. Por último, la aplicación debe requerir la intervención de un adulto para habilitar funciones que permitan a los menores de edad intercambiar información personal.

- La intervención de un adulto hace referencia a un mecanismo para verificar que el usuario no sea menor de edad y que no se anime a los menores de edad a que falsifiquen su edad para acceder a partes de la aplicación que estén diseñadas para adultos (es decir, secciones de la aplicación que requieran un PIN de adulto, una contraseña, una fecha de nacimiento, una verificación por correo electrónico, un documento de identidad con foto, una tarjeta de crédito o un número de la seguridad social).
- Las aplicaciones sociales que se centren en chatear con personas desconocidas no deben estar orientadas a menores de edad. Entre los ejemplos de este tipo de aplicaciones cabe citar aquellas que sean similares a Chatroulette, las aplicaciones de citas, las salas de chat abiertas orientadas a menores de edad, etc.

9. **Cumplimiento legal:** tu aplicación, así como cualquier API o SDK que utilice, debe cumplir la ley de protección de la privacidad infantil online de EE. UU. (COPPA) , el Reglamento General de Protección de Datos de la UE (RGPD) y cualquier otra ley o normativa aplicable.

Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Aplicaciones que promocionan juegos para niños en la ficha de Play Store, pero cuyo contenido solo es adecuado para adultos.
- Aplicaciones que implementan APIs con términos del servicio que prohíben su uso en aplicaciones dirigidas a niños.
- Aplicaciones que hacen parecer atractivo el consumo de alcohol, tabaco o sustancias controladas.
- Aplicaciones que incluyen juegos de apuestas reales o simulados.
- Aplicaciones que incluyen contenido violento, sangriento o desagradable, o no adecuado para niños.
- Aplicaciones que proporcionan servicios de citas u ofrecen consejos maritales o sexuales.
- Aplicaciones que contienen enlaces a sitios web que muestran contenido que infringe las Políticas del Programa para Desarrolladores de Google Play.
- Aplicaciones que muestran anuncios para adultos (por ejemplo, contenido violento o contenido sexual o de juegos de apuestas) a niños. Para obtener más información sobre las políticas de Google Play sobre publicidad, compras en la aplicación y contenido comercial para niños, consulta las políticas sobre Anuncios y Monetización para Familias.

Programa Diseñado para Familias

Las aplicaciones diseñadas específicamente para niños deben participar en el programa Diseñado para Familias. Si tu aplicación está diseñada para todos los públicos, incluidos niños y familias, también puedes solicitar que se incluya en el programa.

Antes de que se acepte tu participación en el programa, tu aplicación debe cumplir todos los requisitos de la Política de Familias y del programa Diseñado para Familias, además de los que se indican en las Políticas del Programa para Desarrolladores de Google Play y el Acuerdo de Distribución para Desarrolladores .

Más información sobre el proceso de envío de aplicaciones para incluirlas en el programa

Participación en el programa

Todas las aplicaciones que participan en el programa Diseñado para Familias y los anuncios que contengan deben ser relevantes y adecuados para niños (las aplicaciones deben tener la clasificación "Todos" o "Todos +10" según el sistema de ESRB u otro equivalente) y solo deben usar SDKs de

anuncios certificados de Google Play . Las aplicaciones que se aceptan en el programa deben cumplir estos requisitos en todo momento. Google Play puede rechazar, retirar o suspender cualquier aplicación que se considere inadecuada para el programa Diseñado para Familias.

A continuación se incluyen algunos ejemplos de aplicaciones comunes que no pueden participar en el programa:

- Aplicaciones con la clasificación "Para todos" de la ESRB que contienen anuncios de juegos de apuestas.
- Aplicaciones para padres o cuidadores (por ejemplo, monitores de lactancia o guías de desarrollo).
- Guías para padres o aplicaciones de gestión de dispositivos que solo están dirigidas a padres o cuidadores.

Categorías

Si se acepta tu participación en el programa Diseñado para Familias, puedes elegir una segunda categoría específica para familias que describa tu aplicación. Estas son las categorías disponibles:

Acción y aventura: juegos y aplicaciones de acción, desde sencillos juegos de carreras a aventuras de fantasía y otros juegos y aplicaciones diseñados para resultar emocionantes.

Juegos de agilidad mental: juegos que hagan pensar a los usuarios, como puzles, juegos de unir piezas, juegos de preguntas y otros juegos que pongan a prueba la memoria, la inteligencia o la lógica.

Creatividad: aplicaciones y juegos que fomenten la creatividad, como aplicaciones de dibujo, pintura, programación y otros juegos y aplicaciones en los que puedes construir y crear cosas.

Educación: aplicaciones y juegos diseñados con la colaboración de expertos del ámbito académico (por ejemplo, educadores, especialistas e investigadores) para promocionar el aprendizaje académico, socioemocional, físico y creativo, así como el aprendizaje relacionado con habilidades básicas, pensamiento crítico y resolución de problemas.

Música y vídeo: aplicaciones y juegos con un componente musical o de vídeo, desde aplicaciones de simulación de instrumentos hasta aplicaciones con contenido de audio y vídeo.

Juegos simulados: aplicaciones y juegos en los que el usuario puede asumir un rol ficticio, como el de cocinero, cuidador, príncipe o princesa, bombero, policía o personaje de ficción.

Anuncios y monetización

Si vas a monetizar una aplicación dirigida a niños en Google Play, es importante que tu aplicación cumpla los requisitos de la Política sobre Anuncios y Monetización para Familias que se indican a continuación.

Las políticas que se incluyen más abajo se aplican a todos los elementos de monetización y publicidad de tu aplicación, incluidos los anuncios, las promociones cruzadas (las de tus aplicaciones y las de aplicaciones de terceros), las ofertas de compras en aplicaciones o cualquier otro contenido comercial (como colocación de productos pagada). Todos los elementos de monetización y publicidad de estas aplicaciones deben cumplir la legislación aplicable (como las directrices de autorregulación o del sector correspondientes).

Google Play se reserva el derecho de rechazar, retirar o suspender aplicaciones en las que se empleen tácticas comerciales demasiado agresivas.

Requisitos de formato

Los elementos de monetización y publicidad de tu aplicación no deben incluir contenido engañoso ni estar diseñados de forma que den lugar a clics involuntarios por parte de usuarios menores de edad. No se permite lo siguiente:

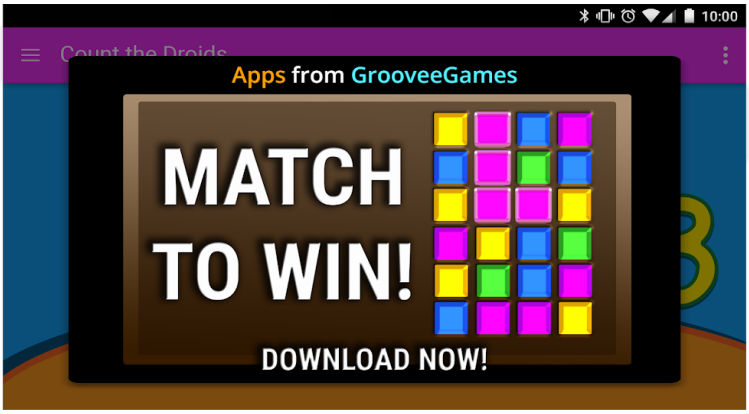
- Mostrar elementos de monetización o publicidad invasivos, incluidos los elementos de monetización y publicidad que ocupen toda la pantalla o interfieran en el uso normal y no ofrezcan ningún medio claro para cerrarlos (por ejemplo, ad walls).
- Mostrar elementos de monetización o publicidad que interfieran en el uso normal de la aplicación o el juego y que no se puedan cerrar después de 5 segundos.
- Los elementos de monetización o publicidad que no interfieran en el uso normal de la aplicación o el juego pueden durar más de 5 segundos (por ejemplo, contenido de vídeo con anuncios integrados).

- Mostrar elementos de monetización o publicidad intersticiales de forma inmediata al abrir la aplicación.
- Incluir varios emplazamientos publicitarios en una página. Por ejemplo, no se permiten anuncios de banner que muestren varias ofertas en un emplazamiento o que muestren más de un banner o anuncio de vídeo.
- Mostrar elementos de monetización o publicidad que no se puedan distinguir fácilmente del contenido de la aplicación.
- Usar tácticas impactantes o emocionalmente manipulativas que promuevan la visualización de los anuncios o las compras en la aplicación.
- No distinguir entre el uso de monedas virtuales de un juego y el dinero real para hacer compras en la aplicación.

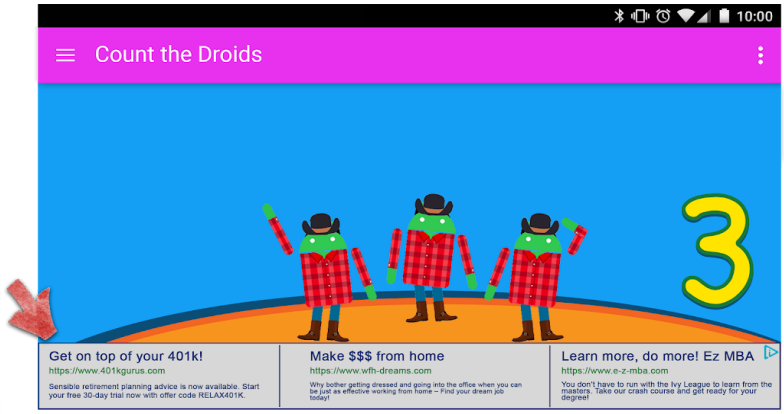
Para asegurarnos de que Google Play siga siendo una plataforma segura y respetuosa, hemos creado estándares que definen y prohíben el contenido que se considere dañino o inadecuado para nuestros usuarios.

- Elementos de monetización y publicidad que se muevan cuando el usuario intente tocarlos para cerrarlos
- Elementos de monetización y publicidad que no proporcionen al usuario una manera de salir de la oferta tras cinco (5) segundos, como se muestra en el siguiente ejemplo:

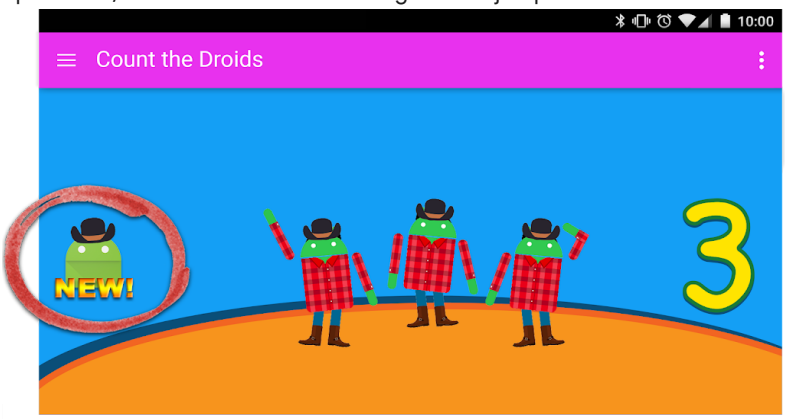
- Elementos de monetización y publicidad que ocupen la mayor parte de la pantalla del dispositivo sin que el usuario pueda cerrarlos fácilmente, como se muestra en el siguiente ejemplo:



- Anuncios de banner que muestren varias ofertas, como se ilustra en el siguiente ejemplo:

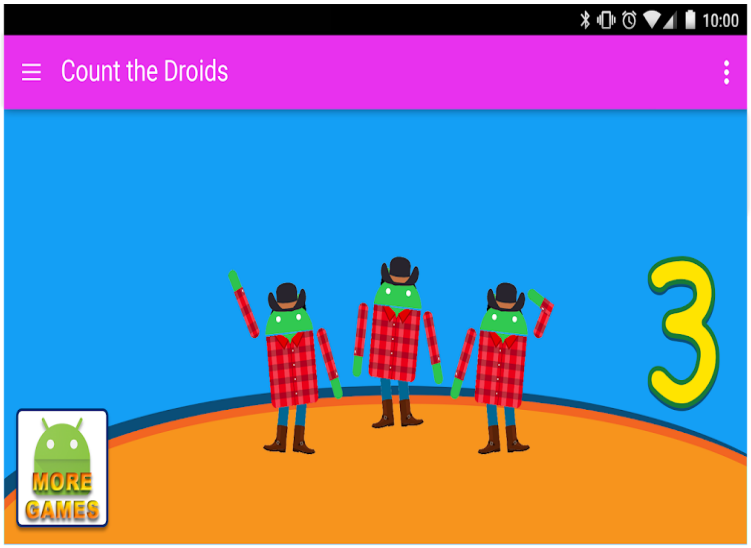


- Elementos de monetización y publicidad que el usuario podría confundir con contenido de la aplicación, como se muestra en el siguiente ejemplo:



- Botones, anuncios u otros elementos de monetización que promocionen otras de tus fichas de Google Play Store y que no se puedan distinguir del contenido de la aplicación, como se muestra en

el siguiente ejemplo:



A continuación se incluyen algunos ejemplos de contenido publicitario inadecuado que no se debe mostrar a niños.

- **Contenido multimedia inadecuado:** anuncios de programas, series, películas, álbumes de música o cualquier otro contenido multimedia que no sea adecuado para niños.
- **Software descargable y videojuegos no adecuados:** anuncios sobre videojuegos o aplicaciones descargables que no sean adecuadas para niños.
- **Sustancias controladas o perjudiciales:** anuncios de alcohol, tabaco, sustancias controladas o cualquier otra sustancia perjudicial.
- **Juegos de apuestas:** anuncios que promocionen simulaciones de juegos de apuestas, concursos o sorteos, aunque la participación sea gratuita.
- **Contenido de carácter sexual y para adultos:** anuncios con contenido sexual, sugerente y no apto para menores.
- **Citas o relaciones:** anuncios de sitios web de citas o relaciones entre adultos.
- **Contenido violento:** anuncios con contenido explícito y violento que no sea adecuado para niños.

En vigor desde el 1 de noviembre del 2022

SDKs de anuncios

Si publicas anuncios en tu aplicación y tu audiencia objetivo solo incluye menores de edad, entonces solo debes usar SDKs de anuncios autocertificados para familias . Si la audiencia objetivo de tu aplicación incluye tanto a menores de edad como a adultos debes implementar filtros de edad, como una pantalla de edad neutral , y asegurarte de que los anuncios que se muestran a los menores de edad procedan exclusivamente de los SDKs de anuncios autocertificados para familias. Las aplicaciones del programa Diseñado para Familias solo deben usar SDK de publicidad autocertificados.

Consulta en la página de la política del Programa de SDKs de anuncios autocertificados para familias para ver todos los detalles de estos requisitos y consultar la lista actual de SDKs de anuncios autocertificados.

Si utilizas AdMob, accede al Centro de Ayuda de AdMob para consultar más información sobre sus productos.

Es tu responsabilidad asegurarte de que tu aplicación cumpla todos los requisitos relativos a los anuncios, compras en la aplicación y contenido comercial. Ponte en contacto con los responsables de tus SDKs de anuncios para obtener más información sobre sus políticas de contenido y sus prácticas publicitarias.

Compras en aplicaciones

Google Play volverá a solicitar la autenticación de todos los usuarios antes de que hagan compras en aplicaciones que participen en el programa Diseñado para Familias. Esta medida está pensada para que quienes aprueben una compra sean los responsables del pago, y no los menores de edad.

Medidas de cumplimiento

Es recomendable evitar las infracciones de las políticas en lugar de tener que corregirlas. No obstante, si se produce una infracción, nos comprometemos a ayudar a los desarrolladores para que comprendan cómo pueden mejorar sus aplicaciones y cumplir las directrices. Si detectas una infracción o tienes alguna pregunta sobre cómo corregirla, ponte en contacto con nosotros.

Cobertura de la política

Nuestras políticas se aplican a cualquier contenido que aparezca en tu aplicación o al que se acceda a través de esta, incluidos los anuncios que muestre y el contenido generado por usuarios que esté alojado en esa aplicación o al que se acceda a través de ella. Asimismo, se aplican a cualquier contenido de tu cuenta de desarrollador que se muestre públicamente en Google Play, incluido tu nombre de desarrollador y la página de destino del sitio web de desarrollador que hayas indicado.

No admitimos aplicaciones que permitan que los usuarios instalen otras aplicaciones en sus dispositivos. Las aplicaciones que proporcionan acceso a otros juegos, aplicaciones o software sin instalarlos, como funciones y experiencias proporcionadas por terceros, deben asegurarse de que todo el contenido al que dan acceso cumple todas las políticas de Google Play. Además, es posible que ese contenido esté sujeto a revisiones adicionales de cumplimiento de políticas.

Los términos definidos que se usan en estas políticas tienen el mismo significado que en el Acuerdo de Distribución para Desarrolladores (ADD). Además de cumplir estas políticas y el ADD, el contenido de tu aplicación se debe clasificar de acuerdo con las Directrices de Clasificación del Contenido.

No admitimos las aplicaciones o el contenido que pueda menoscabar la confianza de los usuarios en el ecosistema de Google Play. Tenemos en cuenta una serie de factores para evaluar si se deben incluir o retirar aplicaciones de Google Play, como un patrón de comportamiento dañino o un alto riesgo de abuso. Entre otros, identificamos los riesgos de uso inadecuado en función de elementos como las reclamaciones dirigidas específicamente a la aplicación o al desarrollador, la cobertura informativa, el historial de infracciones, los comentarios de los usuarios y el uso de marcas, personajes y otros recursos populares.

Cómo funciona Google Play Protect

Google Play Protect comprueba las aplicaciones cuando las instalas. También analiza periódicamente tu dispositivo. Si encuentra una aplicación potencialmente dañina, puede llevar a cabo una de estas acciones:

- Enviarte una notificación. Para eliminar la aplicación, toca la notificación y, a continuación, toca Desinstalar.
- Inhabilitar la aplicación hasta que la desinstales.
- Eliminar la aplicación de forma automática. En la mayoría de los casos, si se detecta una aplicación dañina, recibirás una notificación para informarte de que la aplicación se ha eliminado.

Cómo funciona la protección contra software malicioso

Para protegerte contra el software malicioso de terceros, URLs de esta índole y otros problemas de seguridad, Google podría recibir información sobre los siguientes aspectos:

- Las conexiones de red de tu dispositivo
- URL potencialmente dañinas

- El sistema operativo y las aplicaciones que se hayan descargado en tu dispositivo a través de Google Play o de otras fuentes

Es posible que recibas una advertencia de Google sobre una aplicación o URL que podrían no ser seguras. Google puede eliminar la aplicación o URL (o evitar su instalación) si se sabe que resulta dañina para los dispositivos, los datos o los usuarios.

Puedes inhabilitar algunas de estas opciones de protección en los ajustes del dispositivo. No obstante, es posible que Google siga recibiendo información de las aplicaciones que instales a través de Google Play y que, por motivos de seguridad y sin que se envíe información a Google, se sigan revisando las aplicaciones que se instalen en tu dispositivo y provengan de otras fuentes.

Cómo funcionan las alertas de privacidad

Google Play Protect te avisará si se retira una aplicación de Google Play Store porque puede acceder a tu información personal, y podrás desinstalarla.

Proceso de cumplimiento

Si tu aplicación infringe alguna de nuestras políticas, tomaremos las medidas oportunas tal como se indica a continuación. Además, te proporcionaremos información pertinente sobre la acción que hemos tomado por correo electrónico junto con instrucciones sobre cómo apelar si crees que hemos tomado medidas por error.

Es posible que la retirada o los avisos administrativos no indiquen todas las infracciones de las políticas presentes en tu aplicación o en tu catálogo de aplicaciones. Los desarrolladores son responsables de solucionar los problemas relacionados con el cumplimiento de las políticas y de llevar a cabo procedimientos adicionales de diligencia debida para garantizar que el resto de su aplicación cumple todas las directrices. Si no se solucionan las infracciones de las políticas en todas las aplicaciones, es posible que se apliquen medidas de cumplimiento adicionales.

En los casos en los que las infracciones de estas políticas o del Acuerdo de Distribución para Desarrolladores sean reiteradas o graves (como en el caso del software malicioso, el fraude y las aplicaciones que puedan causar daños a usuarios o dispositivos), se cancelará esa cuenta de desarrollador de Google Play o las cuentas relacionadas.

Medidas de cumplimiento

Las distintas medidas de cumplimiento pueden afectar a tu aplicación de diferentes formas. En la siguiente sección se describen las diferentes acciones que Google Play puede tomar y su impacto en tu aplicación o en tu cuenta de desarrollador de Google Play. Esta información también se explica en este vídeo.

Rechazo

- Las aplicaciones nuevas o las actualizaciones enviadas para su revisión no estarán disponibles en Google Play.
- Si se rechaza la actualización de una aplicación, la versión publicada antes de la actualización seguirá estando disponible en Google Play.
- Los rechazos no te impiden acceder a las descargas, estadísticas y valoraciones de usuarios de una aplicación rechazada.
- Los rechazos no influyen en el estado de tu cuenta de desarrollador de Google Play.

Nota: No intentes volver a enviar una aplicación rechazada hasta que hayas corregido todas las infracciones de las políticas.

Retirada

- La aplicación, junto con sus versiones anteriores, se retirará de Google Play y los usuarios ya no podrán descargarla.
- Como la aplicación se ha eliminado, los usuarios no podrán ver la ficha de Play Store, las descargas ni las estadísticas y valoraciones de la aplicación. Esta información se restaurará cuando envíes una actualización de la aplicación eliminada que cumpla las políticas.
- Es posible que los usuarios no puedan hacer compras en la aplicación ni usar ninguna función de facturación por compras en la aplicación hasta que Google Play apruebe una versión que cumpla las políticas.
- Las eliminaciones no influyen directamente en el estado de tu cuenta de desarrollador de Google Play, pero, si se producen de forma reiterada, es posible que se suspenda tu cuenta.

Nota: No intentes volver a publicar una aplicación retirada hasta que hayas corregido todas las infracciones de las políticas.

Suspensión

- La aplicación, junto con sus versiones anteriores, se retirará de Google Play y los usuarios ya no podrán descargarla.
- La suspensión puede deberse a infracciones graves o reiteradas de las políticas, al igual que las retiradas o los rechazos reiterados de una aplicación.
- Como la aplicación se ha suspendido, los usuarios no podrán ver la ficha de Play Store, las descargas, las estadísticas ni la puntuación de la aplicación. Esta información se restaurará cuando envíes una actualización que cumpla las políticas.
- No puedes seguir usando el APK o el app bundle de una aplicación suspendida.
- Los usuarios no podrán hacer compras en la aplicación ni usar ninguna función de facturación por compras en la aplicación hasta que Google Play apruebe una versión que cumpla las políticas.
- Las suspensiones repercuten negativamente en el estado de tu cuenta de desarrollador de Google Play. Si recibes varios avisos, podemos cancelar cuentas de desarrollador de Google Play individuales y cuentas relacionadas.

Nota: No intentes volver a publicar una aplicación suspendida a menos que Google Play te haya explicado que puedes hacerlo.

Visibilidad limitada

- La descubribilidad de tu aplicación en Google Play está restringida. Tu aplicación seguirá estando disponible en Google Play y los usuarios podrán acceder a ella con un enlace directo a la ficha de Play Store de la aplicación.
- Tener tu aplicación en un estado de visibilidad limitada no afecta al estado de tu cuenta de desarrollador de Google Play.
- El hecho de que tu aplicación tenga el estado de visibilidad limitada no afecta a la capacidad de los usuarios para ver la ficha de Play Store, las descargas, las estadísticas y la puntuación de la aplicación.

Regiones limitadas

- Tu aplicación solo deben poder descargarla a través de Google Play los usuarios de determinadas regiones.
- Los usuarios de otras regiones no deben poder encontrar la aplicación en Play Store.
- Los usuarios que hayan instalado la aplicación anteriormente podrán seguir usándola en su dispositivo, pero dejarán de recibir actualizaciones.
- La limitación regional no afecta al estado de tu cuenta de desarrollador de Google Play.

Cancelación de cuentas

- Si se cancela tu cuenta de desarrollador, todas las aplicaciones de tu catálogo se retirarán de Google Play y ya no podrás publicar nuevas aplicaciones. Esto también significa que las cuentas de desarrollador de Google Play relacionadas también se suspenderán de forma permanente.
- Las suspensiones reiteradas o por infracciones graves de las políticas pueden dar lugar también a la cancelación de tu cuenta de Play Console.
- Como las aplicaciones de la cuenta cancelada se eliminan, los usuarios no podrán ver sus fichas de Play Store, las descargas, las estadísticas ni las valoraciones.

Nota: Cualquier cuenta nueva que intentes abrir también se cancelará (y no se te reembolsará la cuota de registro de desarrollador), así que no intentes crear una nueva cuenta de Play Console si se ha cancelado una de tus otras cuentas.

Cuentas inactivas

Las cuentas inactivas son cuentas de desarrollador que no se usan o se han abandonado. Estas cuentas no están en regla, de acuerdo con los requisitos del Acuerdo de Distribución para Desarrolladores .

Las cuentas de desarrollador de Play están destinadas a desarrolladores activos que publican aplicaciones y las mantienen activamente. Para evitar abusos, cerramos las cuentas que están inactivas, no se usan o no tienen una actividad regular de cualquier otro tipo, por ejemplo, para publicar y actualizar aplicaciones, acceder a estadísticas o gestionar fichas de Play Store.

Al cerrar una cuenta inactiva, se eliminarán tanto tu cuenta como todos los datos asociados a ella. Tu cuota de registro no es reembolsable, la perderás. Antes de que cerremos tu cuenta inactiva, te enviaremos una notificación usando la información de contacto que proporcionaste para esa cuenta.

El cierre de una cuenta inactiva no limitará tu capacidad de crear otra cuenta en el futuro si decides publicar contenido en Google Play. No podrás reactivar tu cuenta, y los datos o aplicaciones anteriores no estarán disponibles en una cuenta nueva.

Gestionar y denunciar infracciones de las políticas

Apelar una acción obligatoria

Las aplicaciones se restaurarán si consideramos que se ha cometido un error y si se determina que la aplicación no infringe las Políticas del Programa para Desarrolladores de Google Play y el Acuerdo de Distribución para Desarrolladores. Si has revisado las políticas detenidamente y crees que nuestra decisión puede haber sido un error, sigue las instrucciones que se indican en la notificación que recibiste por correo electrónico para apelar la decisión.

Recursos adicionales

Si necesitas más información sobre una medida de cumplimiento o sobre la valoración o el comentario de un usuario, puedes consultar algunos de los recursos que aparecen a continuación o ponerte en contacto con nosotros a través del Centro de Ayuda de Google Play. No obstante, no podemos ofrecerte asesoramiento legal. Si lo necesitas, consulta a un abogado.

- Verificación de aplicaciones
- Denunciar infracciones de las políticas
- Contactar con Google Play para realizar una consulta sobre la cancelación de una cuenta o la retirada de una aplicación
- Advertencias
- Denunciar aplicaciones y reseñas inadecuadas
- Mi aplicación se ha retirado de Google Play
- Cancelación de cuentas de desarrollador de Google Play

Requisitos de Play Console

Google Play quiere ayudar a sus usuarios a disfrutar de una experiencia segura y satisfactoria con sus aplicaciones, y a los desarrolladores, a tener el mayor éxito posible. Trabajamos para lograr que el proceso de poner tu aplicación a disposición de los usuarios se desarrolle sin problemas.

Para evitar infracciones habituales que podrían alargar el proceso de revisión o dar lugar al rechazo de una aplicación, no te olvides de seguir los pasos que se describen a continuación cuando envíes información a través de Play Console.

Antes de enviar tu aplicación, debes hacer lo siguiente:

- Proporcionar de forma precisa todos los metadatos e información de la aplicación
- Asegurarte de que tu información de contacto esté actualizada
- Subir la política de privacidad de tu aplicación y rellenar los requisitos de la sección **Seguridad de los datos**
- Proporcionar una cuenta de prueba activa, información de inicio de sesión y todos los recursos necesarios para revisar tu aplicación (por ejemplo, credenciales de inicio de sesión, código QR, etc.)

Como siempre, debes asegurarte de que tu aplicación ofrezca una experiencia de usuario estable, atractiva y adaptable. Comprueba que todos los elementos de tu aplicación, incluidos los servicios de analíticas, las redes publicitarias y los SDKs de terceros, cumplan las Políticas del Programa para Desarrolladores de Google Play. Además, si la audiencia objetivo de tu aplicación incluye a niños, asegúrate de cumplir nuestra política de Familias .

Recuerda que eres responsable de revisar el Acuerdo de Distribución para Desarrolladores y todas las Políticas del Programa para Desarrolladores para asegurarte de que tu aplicación cumpla todos los requisitos.

Developer Distribution Agreement

¿Necesitas más ayuda?

Prueba estos pasos:

Ponte en contacto con nosotros

Danos más información para que podamos ayudarte