Políticas del Programa para Desarrolladores (vigentes a partir del 1 de marzo del 2021)

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, junto con el Acuerdo de Distribución para Desarrolladores, nos permiten seguir ofreciendo juntos las aplicaciones más fiables e innovadoras del mundo a más de mil millones de usuarios a través de Google Play. Te invitamos a conocer nuestras políticas 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 incluyan contenido que sexualice a menores están sujetas a la retirada inmediata de Play Store. Esto incluye, por ejemplo, aplicaciones que promocionen la pedofilia o interacciones inadecuadas (como tocamientos o caricias) dirigidas a menores de edad.

Además, no se admiten las aplicaciones dirigidas a niños que contengan temas para adultos, como aplicaciones con violencia excesiva, sangre o contenido macabro, ni aplicaciones que representen o fomenten actividades dañinas y peligrosas. Tampoco admitimos aplicaciones que promuevan una imagen negativa del cuerpo o de uno mismo, ni aplicaciones que, con el fin de entretener, muestren intervenciones de cirugía plástica, pérdida de peso u otros ajustes estéticos en la apariencia física de una persona.

Si detectamos contenido con imágenes de abuso sexual infantil, se informará a las autoridades pertinentes y se eliminarán las cuentas de Google de todos los usuarios implicados en la distribución de ese contenido.

Contenido inapropiado

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 inapropiado 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. Es posible que se permitan contenidos que incluyan desnudos si el objetivo principal es educativo, informativo, científico o artístico y si los desnudos no aparecen sin ninguna justificación.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 fomenten actividades de entretenimiento relacionadas con el sexo, servicios de compañía u otros servicios que consistan en proporcionar favores sexuales a cambio de algún tipo de compensación.
- Aplicaciones que degraden o cosifiquen a las personas.

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 u otras características asociadas a la discriminación o la marginación sistémicas.

Las aplicaciones que incluyan contenido pedagógico, documental, científico o artístico relacionado con el nazismo pueden ser bloqueadas en determinados países, de conformidad con lo estipulado en las leyes y normativas locales.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Representaciones gráficas o descripciones de violencia realista, así como amenazas violentas dirigidas hacia cualquier persona o animal
- Aplicaciones que fomenten la autolesión, el suicidio, el hostigamiento, el acoso, los trastornos de la conducta alimentaria, los 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, proporciona información suficiente para que los usuarios puedan entender el contexto.

Acontecimientos sensibles

No admitimos aplicaciones que saquen provecho de desastres naturales, atrocidades, conflictos, fallecimientos o cualquier otro acontecimiento trágico, o que traten estos asuntos sin la sensibilidad necesaria. Por lo general, se permiten aplicaciones con contenido relacionado con un acontecimiento sensible si dicho contenido tiene un propósito pedagógico, documental, científico o artístico, o sirve para advertir o concienciar a los usuarios sobre el hecho sensible del que trata.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Mostrar una falta de sensibilidad hacia la muerte de una o varias personas debida a una sobredosis, suicidio, causas naturales, etc.
- Negar que un suceso trágico importante haya ocurrido.
- Obtener beneficio económico de un suceso trágico y que este beneficio no sea para las víctimas.

Hostigamiento y acoso

No admitimos aplicaciones que contengan o faciliten las amenazas, el hostigamiento o el acoso.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 derivados, independientemente de que sean legales o no.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 de bolígrafo) ni que inciten al consumo ilegal o inadecuado de alcohol o tabaco.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 aquellas que gestionen de forma remota la minería de criptomonedas.

Préstamos personales

Definimos los préstamos personales como aquellos que hace una persona, una organización o una entidad a un consumidor de forma no recurrente 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.

- No se incluyen hipotecas, préstamos para comprar coches, préstamos para estudiantes ni líneas de crédito rotativas (como tarjetas de crédito o líneas personales de crédito).

Las aplicaciones que ofrecen préstamos personales, incluyendo las que ofrecen préstamos de forma directa, las que generan oportunidades de venta o las que ponen en contacto a consumidores con prestamistas externos, deben proporcionar la siguiente información en sus metadatos:

- El periodo mínimo y máximo para devolver el préstamo.
- La tasa anual efectiva (TAE), 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 todas las comisiones 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.

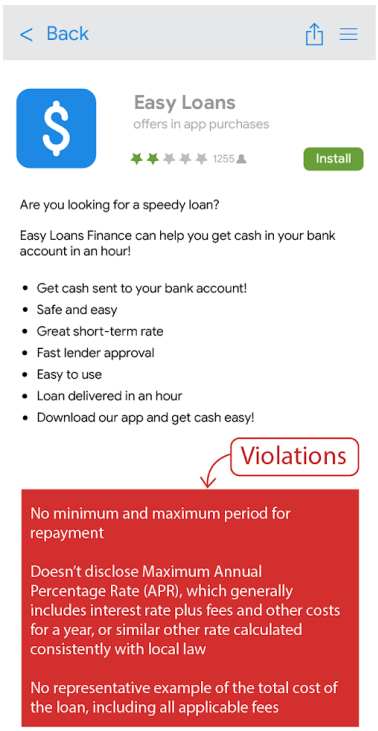
No admitimos aplicaciones que promocionen préstamos personales que se deban devolver en un plazo de 60 días o menos desde la fecha de emisión del préstamo (los consideramos préstamos personales a corto plazo).

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 TILA (ley estadounidense de veracidad en los préstamos).

Esta política afecta a las aplicaciones que ofrezcan préstamos de forma directa, a las que generen oportunidades de venta y a las que pongan en contacto a consumidores con prestamistas externos.

A continuación te mostramos un ejemplo de infracciones frecuentes:



Juegos de apuestas, juegos y concursos con dinero real

Permitimos aplicaciones de juegos de apuestas con dinero real, anuncios relacionados con juegos de apuestas con dinero real y aplicaciones de fantasy sport diarios que cumplan ciertos requisitos.

Aplicaciones de juegos de 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 apuestas online en los países de la tabla siguiente, siempre que el Desarrollador complete el proceso de solicitud para aplicaciones de juegos de apuestas que se distribuyen en Google Play. Además, debe ser un operador gubernamental autorizado y/o debe estar registrado como operador con licencia proporcionada por la autoridad gubernamental con potestad sobre los juegos de 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 apuestas online que quiera ofrecer.

Solo permitimos aplicaciones de juegos de apuestas con licencia o autorizadas que incluyan los siguientes tipos de productos relacionados con los juegos de apuestas online (consulta la tabla que aparece más abajo para ver los tipos específicos de productos de juegos de apuestas permitidos en cada país):

- Juegos de casino online
- Loterías
- Apuestas deportivas
- Fantasy sport diarios

Australia

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Apuestas deportivas • Loterías • Fantasy sport diarios

Bélgica

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Juegos de casino online • Apuestas deportivas • Loterías (solo operadores gubernamentales)

Brasil

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Loterías (limitado a aplicaciones aprobadas publicadas por Caixa Economica Federal) • Apuestas deportivas (solo carreras de caballos)

Canadá

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online (solo operadores gubernamentales) • Apuestas deportivas (solo operadores gubernamentales) • Loterías (solo operadores gubernamentales)

Colombia

Resumen	Detalles

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías (solo operadores gubernamentales)

Dinamarca

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías • Fantasy sport diarios

Finlandia

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online (solo operadores gubernamentales) • Apuestas deportivas (solo operadores gubernamentales) • Loterías (solo operadores gubernamentales)

Francia

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías (solo operadores gubernamentales)

Alemania

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Apuestas deportivas • Loterías (solo operadores gubernamentales)

Irlanda

Resumen	Detalles

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías (solo operadores gubernamentales u organizaciones benéficas)

Japón

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Apuestas deportivas (carreras de caballos, lanchas a motor, bicicletas y motocicletas, y apuestas de fútbol; solo operadores gubernamentales) • Loterías (solo operadores gubernamentales)

México

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías • Fantasy sport diarios

Nueva Zelanda

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Apuestas deportivas (solo operadores gubernamentales) • Loterías (solo operadores gubernamentales)

Noruega

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías

Rumanía

Resumen	Detalles

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Casinos online • Apuestas deportivas • Loterías (solo operadores gubernamentales)

España

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Juegos de casino online • Apuestas deportivas • Loterías (solo operadores gubernamentales) • Fantasy sport diarios

Suecia

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Juegos de casino online • Apuestas deportivas • Loterías (solo operadores gubernamentales)

Reino Unido

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Juegos de casino online • Apuestas deportivas • Loterías • Fantasy sport diarios

Estados Unidos

Resumen	Detalles

Resumen	Detalles
Se permiten con restricciones	De acuerdo con los requisitos de solicitud y licencia indicados más arriba, se permiten las aplicaciones que incluyan los siguientes tipos de productos de juegos de apuestas: • Juegos de casino online (permitidos en Delaware, Nevada [solo póker], Nueva Jersey y Pensilvania) • Apuestas deportivas (permitidas en Colorado, Distrito de Columbia [solo operadores gubernamentales], Illinois, Indiana, Iowa, Montana [solo operadores gubernamentales], Nevada, Nueva Jersey, Nuevo Hampshire, Oregón [solo operadores gubernamentales], Pensilvania, Rhode Island, Tennessee y Virginia Occidental) • Loterías (solo operadores estatales u operadores afiliados contratados por el estado en Carolina del Norte, Georgia, Illinois, Kentucky, Maine, Míchigan, Nueva York, Nuevo Hampshire, Pensilvania, Rhode Island y Virginia) • En función del estado, es posible que los fantasy sport diarios se consideren juegos de apuestas en EE. UU., y todas las aplicaciones de fantasy sport diarios que se publiquen en Estados Unidos están sujetas a los requisitos de las aplicaciones de fantasy sport diarios (DFS) que se indican más abajo.

Las aplicaciones deben cumplir los siguientes requisitos:

- El desarrollador debe completar el proceso de solicitud correctamente para distribuir la aplicación en 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;
- 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 claramente información sobre cómo participar en juegos de apuestas de forma responsable.

Otras aplicaciones de juegos, concursos y torneos con dinero real

En las aplicaciones que no cumplan los requisitos para las aplicaciones de juegos de apuestas indicados más arriba, no permitimos contenido o servicios que permitan a los usuarios apostar o participar con dinero real (incluidos elementos en la aplicación 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.

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) y 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 las políticas 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 solo se pueden otorgar y canjear con una proporción fija, la cual 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 premios 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 reglas 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 las reglas 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 las reglas 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 anuncios de juegos, concursos y torneos con dinero real en aplicaciones distribuidas en Play

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

1. 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.
2. 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.
3. La aplicación no debe mostrar anuncios de juegos de apuestas a usuarios menores de 18 años.
4. La aplicación no debe estar registrada en el programa Diseñado para Familias.
5. La aplicación no debe estar orientada a usuarios menores de 18 años.

6. 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.
7. La aplicación no debe ofrecer contenido de juegos de apuestas simulados (por ejemplo, aplicaciones de casino sociales o aplicaciones con máquinas tragaperras virtuales).
8. 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).
9. 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 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 que se indican 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 mencionados anteriormente.
- El desarrollador debe completar correctamente el proceso de solicitud de fantasy sport diario y dicha solicitud debe ser aceptada para poder 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 (International Age Ratings Coalition, IARC).
- La aplicación y su ficha deben mostrar información clara sobre cómo participar en juegos de apuestas de forma responsable.

Si se distribuye en Estados Unidos, deberán cumplirse los siguientes requisitos adicionales:

- 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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Facilitar o fomentar la compra o la venta no autorizada de drogas ilegales o de medicamentos que necesitan prescripción médica.
- Representar o fomentar el consumo o la venta de drogas, alcohol o tabaco en menores.
- Instrucciones para cultivar o elaborar drogas ilegales.

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 contengan o incluyan CGU deben:

- Hacer que los usuarios acepten los términos de uso o la política del usuario 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), y prohibirlos en los términos de uso o en las políticas de usuarios de la aplicación.
- Implementar medidas firmes, eficaces y continuas de moderación de contenido, siempre que sea razonable y de acuerdo con el tipo de CGU alojado por la aplicación.
  - En el caso de las aplicaciones de streaming en directo, el CGU inapropiado se debe retirar lo antes posible.
  - 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 realidad aumentada 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).
- Proporcionar en la aplicación un sistema fácil de usar que permita denunciar y actuar contra el CGU inadecuado cuando corresponda.
- Eliminar o bloquear usuarios con comportamiento inadecuado que infrinjan los términos de uso o la política de usuarios de la aplicación.
- Implementar medidas para evitar que se obtengan ingresos derivados de fomentar el comportamiento inadecuado de los usuarios.

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 resuelvan las reclamaciones de los usuarios sobre contenido inadecuado o cuestionable.

Sustancias no aprobadas

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

- 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 afirman 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 supervisamos, visita la página www.legitscript.com.

Propiedad intelectual

Cuando un desarrollador copia el trabajo de otra persona o lo utiliza sin el permiso necesario, puede dañar al propietario de ese trabajo. No utilices de forma desleal el trabajo de otros.

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 titular 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 (como 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.

A continuación te mostramos algunos ejemplos de contenido protegido por derechos de autor que se suelen utilizar sin autorización y sin ninguna razón legal válida:

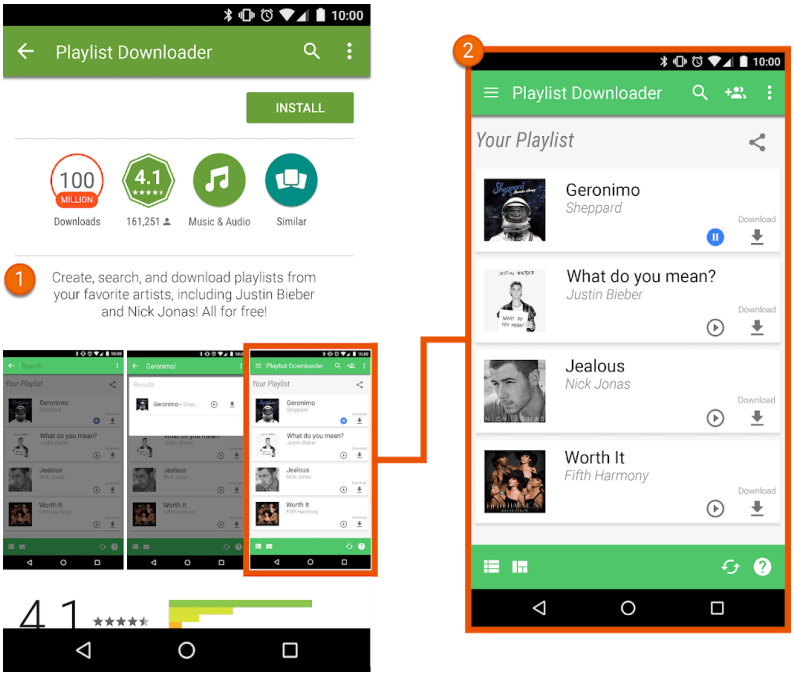
- Portadas de álbumes de música, videojuegos y libros
- Imágenes de marketing de películas, programas de TV y videojuegos
- Carátulas o imágenes de cómics, dibujos animados, películas, vídeos musicales o contenido de TV
- Logotipos de equipos deportivos profesionales y universitarios
- Fotos publicadas 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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 a 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. Cuando se adquiere una marca comercial, su propietario obtiene derechos exclusivos sobre su uso en lo que respecta a determinados productos o servicios.

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. Los productos falsificados imitan las características de marca de un producto auténtico para hacerse pasar por él.

Privacidad, elementos engañosos y uso inadecuado de dispositivos

Nos comprometemos a proteger la privacidad de los usuarios y a ofrecerles un entorno seguro. Las aplicaciones engañosas, maliciosas o que tengan como objetivo hacer un uso inadecuado de redes, dispositivos o 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 proporcionen o que se recoja sobre ellos, incluida la información de los dispositivos). Por eso, debes incluir un aviso en el que se comunique si tu aplicación va a acceder, usar o compartir sus datos, así como limitar el uso de dichos datos a los fines especificados. Además, si tu aplicación procesa datos sensibles o personales, debes cumplir los requisitos adicionales que se incluyen en la sección "Información personal y sensible". Estos requisitos de Google Play se suman a los requisitos prescritos en la legislación de protección de datos y privacidad aplicable.

Información personal y sensible

Los datos de usuario sensibles y personales son, entre otros, la información personal identificable, los datos de pago y financieros, la información de autenticación, la agenda, los contactos, la ubicación del dispositivo, los datos relacionados con los SMS y las llamadas, el micrófono, la cámara y otros datos confidenciales de uso o de los dispositivos. Si tu aplicación gestiona datos sensibles de los usuarios, debes hacer lo siguiente:

- Limitar tu forma de acceder, recoger, usar y compartir los datos sensibles o personales que se adquieren a través de la aplicación a los fines necesarios para proporcionar y mejorar las funciones de la aplicación (por ejemplo, funciones anunciadas a los usuarios que se mencionan y se promocionan en la descripción de la aplicación en Play Store). Las aplicaciones que amplíen el uso de estos datos para publicar anuncios deben cumplir nuestra Política de Anuncios.
- Publicar una política de privacidad en el campo adecuado de Play Console y en la propia aplicación. La política de privacidad, así como cualquier aviso que aparezca en la aplicación, debe explicar de forma exhaustiva cómo recoge, utiliza, comparte y accede tu aplicación a los datos de usuario. En la política de privacidad, debes especificar los tipos de datos sensibles y personales a los que tu aplicación accede y que recoge, utiliza y comparte, y el tipo de terceros con los que compartes los datos de usuario sensibles o personales.
- Procesar todos los datos de usuario sensibles o personales de forma segura y transmitirlos usando un sistema moderno de cifrado, como el protocolo HTTPS.
- Usar una solicitud de permisos de tiempo en ejecución siempre que sea posible antes de acceder a los datos que tengas disponibles mediante los permisos de Android.
- No vender datos de usuario sensibles ni personales.

Requisito de aviso destacado y consentimiento

En los casos en los que los usuarios no puedan esperar de forma razonable que sus datos de usuario sensibles o personales sean necesarios para ofrecer o mejorar funciones o características de tu aplicación que cumplan las políticas (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 en 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 sensibles o personales.

El aviso en 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 tiempo en ejecución asociado. No puedes recoger datos sensibles o personales ni 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 ignoren automáticamente o que caduquen para obtener el consentimiento del usuario.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Una aplicación que acceda al inventario de aplicaciones instaladas de un usuario y no trate estos datos como información sensible o personal sujeta a la política de privacidad, la gestión de datos y los requisitos de divulgación y consentimiento de forma visible.
- Una aplicación que acceda a los datos del teléfono o la agenda de un usuario y no los trate como información sensible o personal sujeta a los requisitos de la política de privacidad, del tratamiento de datos y de la visibilidad de los avisos de divulgación y consentimiento, todos ellos mencionados 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 ni 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 ni obtenga el consentimiento de acuerdo con los requisitos anteriores.

Restricciones específicas para el acceso a datos 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 sensibles o personales que contengan información financiera, datos de pago o números de identificación emitidos por el gobierno.
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.

EU-U.S. Privacy Shield (Escudo de la privacidad UE-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 Europa 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 mediante la dirección data-protection-office@google.com . Además, debes dejar de procesar la Información Personal de la UE o tomar de forma inmediata las medidas apropiadas para recuperar un nivel de protección adecuado.

Permisos

Las solicitudes de permisos deben resultar comprensibles para los usuarios. Solo puedes solicitar permisos que sean necesarios para implementar funciones o servicios actuales en tu aplicación que tengan una promoción en tu ficha de Play Store. No puedes utilizar permisos que 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 estos permisos.

Solicita permisos y acceso a datos en contexto (mediante autenticación incremental) para que los usuarios comprendan por qué lo haces. 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 los anteriores, los permisos restringidos son permisos clasificados con los tipos Dangerous, Special o Signature en la documentación para desarrolladores y 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).

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 en función de los potenciales efectos sobre la privacidad o la 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 sobre Información Personal y Sensible y a los siguientes requisitos:

Permiso restringido	Requisito
El archivo de manifiesto de tu aplicación solicita el grupo de permisos de registro de llamadas (por ejemplo, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS).	Tu aplicación debe estar registrada de forma activa como controlador predeterminado del teléfono o del asistente en el dispositivo.
El archivo de manifiesto de tu aplicación solicita el grupo de permisos de SMS (por ejemplo, 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 la función principal, 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 (por ejemplo, mejorar otros servicios o aplicaciones o mostrar publicidad). 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 sensible y personal sujeto a la política sobre Información Personal y Sensible y 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 implementar funciones o servicios en tu aplicación.
- Nunca debes solicitar permisos de ubicación de los usuarios con fines de publicidad o análisis únicamente. Las aplicaciones que amplíen el uso permitido de estos datos para publicar anuncios deben cumplir nuestra Política de Anuncios.
- Las aplicaciones deben solicitar el nivel mínimo de acceso a la ubicación necesario, 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, rechazamos aplicaciones que solicitan o acceden a la ubicación en segundo plano sin justificación aparente.
- La ubicación en segundo plano solo se puede utilizar para proporcionar funciones beneficiosas al 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 ha iniciado como una continuación de una acción que ha iniciado el usuario en la aplicación.
- Finaliza inmediatamente después de que la aplicación complete el caso práctico previsto de la acción que ha iniciado el usuario.

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

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 sobre 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 tengan la versión R (Android 11, nivel de API 30) o una 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 la versión R, consulta este artículo de ayuda.

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 (entre los que se incluyen 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 ellos 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 de las Aplicaciones Principales 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 y tiene acceso limitado a las API de Android (como JavaScript en WebView o en un navegador).

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Aplicaciones que bloqueen una aplicación o interfieran en ella publicando anuncios.
- Aplicaciones para hacer trampas en juegos que afecten a la jugabilidad de otras aplicaciones.
- Aplicaciones que faciliten o den 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.

Comportamiento engañoso

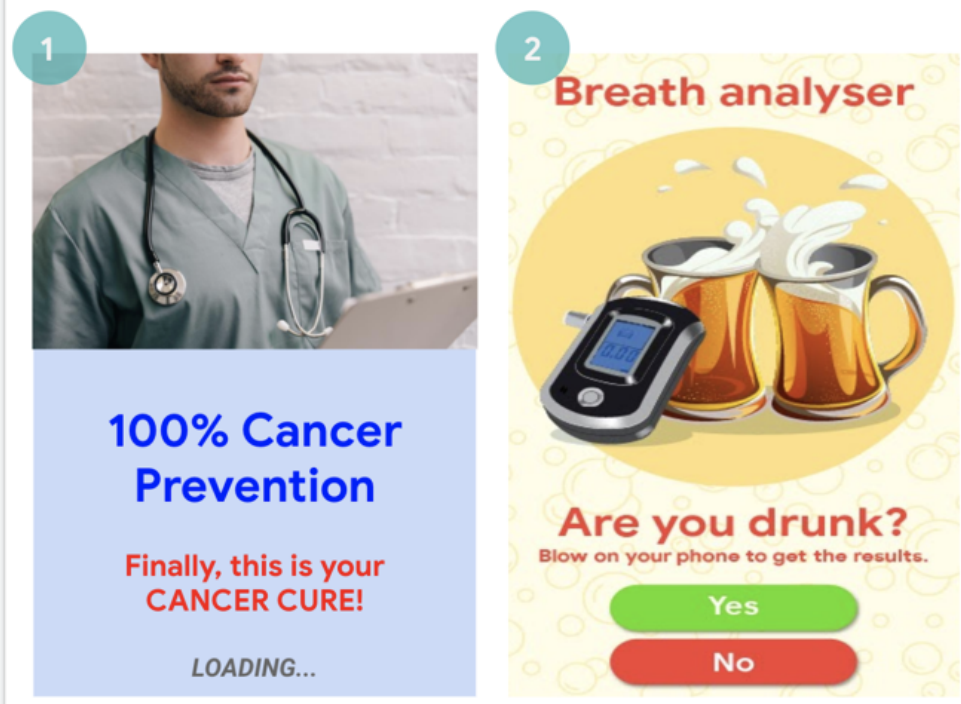
No admitimos aplicaciones que traten de engañar a los usuarios o facilitar conductas fraudulentas; esto incluye, por ejemplo, aplicaciones que estén diseñadas para no funcionar. Las aplicaciones deben proporcionar contenido informativo, descripciones, imágenes y vídeos precisos sobre sus funciones en 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 contengan información o afirmaciones falsas o engañosas (incluyendo las insertadas en los títulos, los iconos, las descripciones o las capturas de pantalla).

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 dice ser un antivirus, pero solo contiene una guía de texto explicando cómo eliminar virus.
- Nombres de aplicaciones o desarrolladores que no describen de forma fiel su clasificación o sus resultados en Google Play (por ejemplo, "Selección de los editores" "Aplicación número 1" o "Top ventas").
- Aplicaciones que incluyan funciones médicas o relacionadas con la salud que sean engañosas o potencialmente dañinas.
- Aplicaciones que afirmen disponer de funciones que son imposibles de llevar a cabo (por ejemplo, una aplicación repelente de insectos), incluso si se presentan como una broma, un chiste, etc.
- Aplicaciones que estén categorizadas de forma incorrecta (por ejemplo, en cuanto a la clasificación o la categoría de la aplicación).
- Contenido engañoso de manera demostrable que pueda interferir con procesos electorales.
- Aplicaciones que afirmen, sin ser cierto, estar asociadas a una entidad pública o promocionar servicios públicos de los que no tienen la autorización correspondiente.
- Aplicaciones que afirman ser falsamente 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) Estas aplicación afirma disponer de funciones que no se pueden implementar (usar el teléfono como alcoholímetro).

Cambios engañosos de los ajustes del dispositivo

No admitimos aplicaciones que realicen cambios en los ajustes o en las funciones del dispositivo del usuario fuera de la aplicación sin su conocimiento y 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; esto incluye, por ejemplo, aplicaciones que generen o que permitan generar carnés de identidad, números de la seguridad social, pasaportes, diplomas, tarjetas de crédito o carnés de conducir. Las aplicaciones deben proporcionar información, títulos, descripciones, imágenes y vídeos que reflejen de forma precisa 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 está exenta de la aplicación de nuestras políticas.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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.

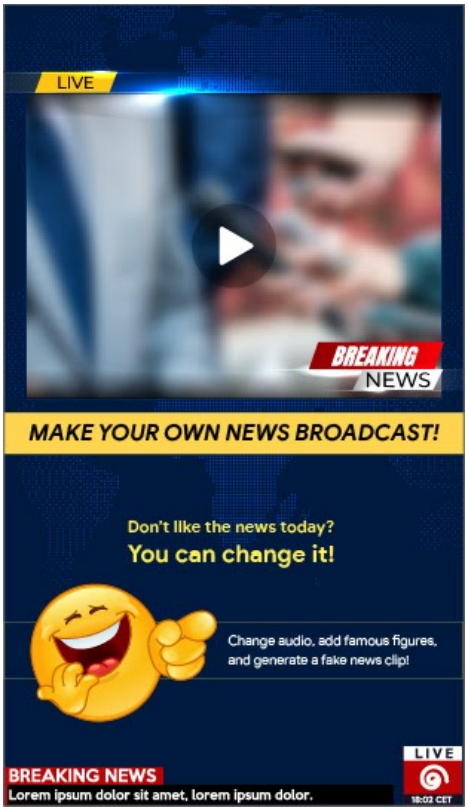
Manipulación de contenido

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Aplicaciones que añaden un personaje público 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, desarrolladores u otras cuentas para ocultar o proporcionar información falsa sobre la identidad de la aplicación o del desarrollador, o sobre otros detalles materiales, si el contenido de la aplicación está relacionado con temas políticos, problemas sociales o asuntos de interés público.

Software malicioso

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.

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. Basándonos en este principio fundamental, nos esforzamos por garantizar que el ecosistema de Android sea seguro para nuestros usuarios y sus dispositivos Android.

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. Por ello, 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: fraude de SMS, fraude de llamadas premium y fraude de servicios telefónicos.

Fraude de SMS

Código que cobra a los usuarios por enviar SMS premium sin su consentimiento, o que intenta encubrir sus actividades de SMS mediante la ocultación de los acuerdos de confidencialidad o la de los mensajes SMS del operador móvil que comunican cargos al usuario o confirman suscripciones.

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

Fraude de llamadas premium

Código que cobra a los usuarios por llamar a números de tarificación especial sin su consentimiento.

Fraude de servicios telefónicos

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

Los fraudes de servicios telefónicos incluyen cualquier tipo de facturación, excepto la de 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 periódica, y el SMS o el correo de confirmación se suele interceptar para impedir que los usuarios se den cuenta de la transacción financiera.

Stalkerware

Código que transmite información personal desde el dispositivo sin el consentimiento de los usuarios o sin avisarles adecuadamente, y sin mostrar una notificación permanente cuando esto ocurre.

Las aplicaciones de stalkerware normalmente transmiten datos a un tercero que no es el proveedor de la aplicación potencialmente dañina.

En su forma aceptable, estas aplicaciones se pueden usar para que los padres consulten la ubicación de sus hijos. Sin embargo, estas aplicaciones no se pueden utilizar para consultar la ubicación de una persona (la pareja del usuario, por ejemplo) sin su conocimiento o permiso a menos que se muestre una notificación permanente cuando se estén transmitiendo los datos.

Solo las aplicaciones que cumplan nuestras políticas y estén diseñadas y promocionadas exclusivamente con fines de supervisión parental (o familiar) o de gestión de empresas se pueden distribuir a través de Play Store con funciones de seguimiento e informes, siempre que cumplan todos los requisitos que se detallan a continuación.

Las aplicaciones distribuidas en Play Store que no sean de stalkerware y estén destinadas a supervisar o registrar el comportamiento de los usuarios en un dispositivo deben cumplir estos 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 ofrecer una notificación permanente a los usuarios y mostrar un icono único que permita identificarlas con claridad.
- 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.
- Eres el único responsable de determinar la legalidad de tu aplicación en el mercado de destino. Retiraremos las aplicaciones que se consideren ilegales en los lugares en los que se publiquen.

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 diseñó 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 de descarga 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 parece 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 avanzados

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 engloban en la categoría de aplicaciones de rooteo.

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 un 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.

En cambio, las aplicaciones de rooteo maliciosas no informan al usuario de que van a rootear el dispositivo, o le informan del rooteo con antelación, pero ejecutan otras acciones propias de 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 o sin obtener su consentimiento.

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 recibidas en el 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 un componente dañino oculto. Por ejemplo, un juego que envía mensajes SMS premium desde el dispositivo del usuario en segundo plano y sin el conocimiento del usuario.

Nota sobre las 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. Esto no implica que la aplicación sea dañina, pero, sin una revisión más exhaustiva, tampoco podemos garantizar que sea segura.

Nota sobre la categoría de puerta trasera

Incluir una aplicación en 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 software malicioso de puerta trasera, sino como una aplicación que tiene una vulnerabilidad, y se pedirá al desarrollador que le aplique un parche.

Software no deseado para móviles

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.

Software no deseado para móviles

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
- Suplantación de identidad

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 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

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

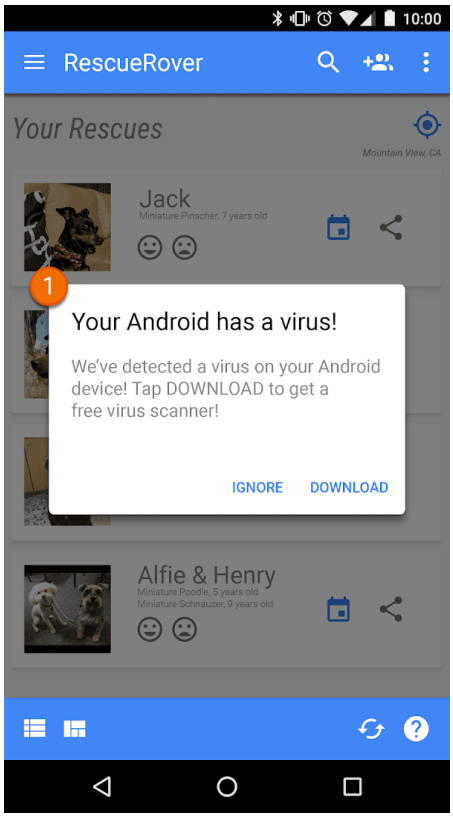
- Una aplicación que muestra anuncios que los usuarios no pueden ver.
- Una aplicación que genera automáticamente clics en anuncios sin la intervención del usuario, o que genera tráfico de red equivalente para ofrecer créditos de clics de forma fraudulenta.
- Una aplicación que envía clics de atribución 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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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.

Suplantación de identidad

Cuando los desarrolladores suplantan la identidad de otras personas o de sus aplicaciones, confunden a los usuarios y perjudican a la comunidad de desarrolladores. Las aplicaciones que confundan a los usuarios suplantando la identidad de otra persona están prohibidas.

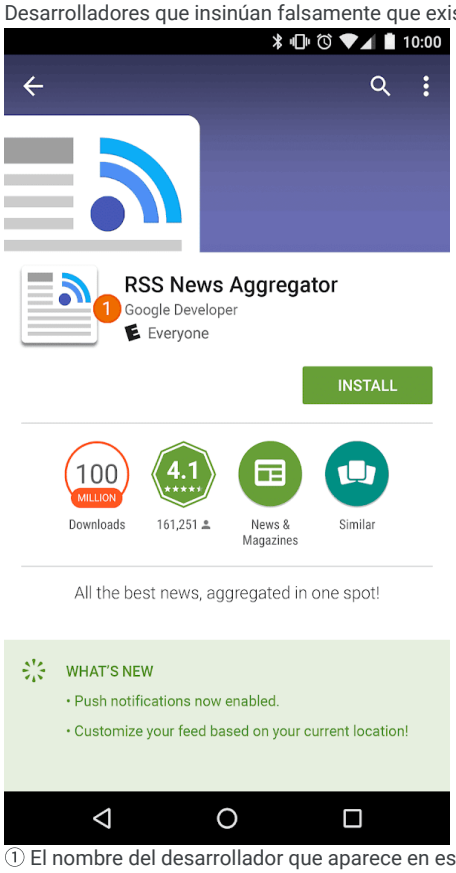
Suplantación de identidad

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Desarrolladores que insinúan falsamente que existe una relación con otra empresa o con otro desarrollador:



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

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

Monetización y anuncios

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. Para garantizar la mejor experiencia de usuario, necesitamos que cumplas estas políticas.

Pagos

1. Los desarrolladores que apliquen cargos por las aplicaciones y por las descargas de Google Play deben utilizar el sistema de facturación de Google Play como método de pago.
2. Las aplicaciones distribuidas por Play deben utilizar el sistema de facturación de Google Play como método de pago si requieren o aceptan pagos para acceder a funciones o servicios, incluidos los productos o contenidos digitales y las funciones de la aplicación.

a. Algunos ejemplos de funciones de aplicaciones o servicios que requieren el uso del sistema de facturación de Google Play son las compras en la aplicación de:
   - Elementos (como monedas virtuales, vidas extra, tiempo de juego adicional, complementos, personajes y avatares).
   - Servicios de suscripción (como aplicaciones de fitness, juegos, citas, educación, música, vídeo u otros servicios de suscripción de contenido).
   - Contenido o funciones de aplicaciones (como, por ejemplo, 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 o software de gestión financiera).

b. El sistema de facturación de Google Play no debe utilizarse en los siguientes casos:
   - Si el pago es principalmente:

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

     - 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.
   - Si se incluyen pagos de punto a punto, subastas online y donaciones exentas de impuestos.
   - 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..
   - Si el pago se realiza por un producto cuya categoría se considera inaceptable según las Políticas de Contenido del Centro de Pagos de Google.

3. Las aplicaciones que no estén descritas en 2 (b) no pueden dirigir a los usuarios a ningún 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 dirigen a los usuarios desde una aplicación a un método de pago distinto al sistema de facturación de Google Play.
4. Las monedas virtuales en aplicaciones solo se deben utilizar en la aplicación o el juego para el que se hayan comprado.
5. 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. 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.
6. Los juegos y aplicaciones 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.

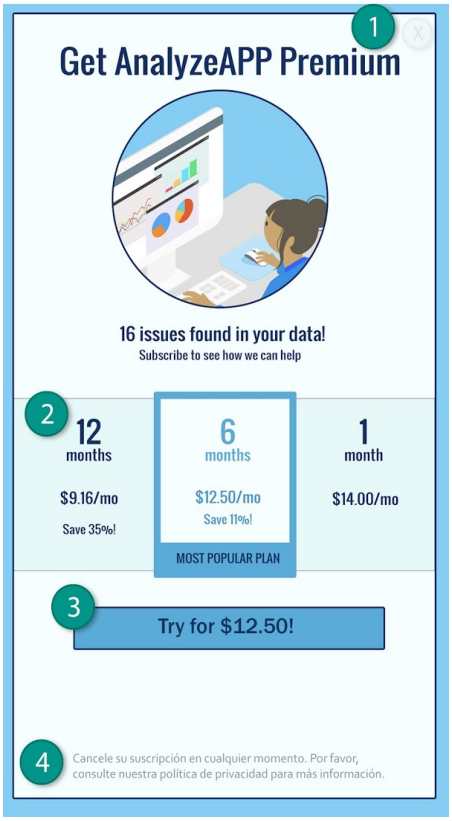
Suscripciones

Como desarrollador, no puedes confundir a los usuarios sobre el contenido o los servicios de suscripción que ofreces en tu aplicación. Es fundamental comunicar lo que ofreces de forma clara en pantallas de inicio o promociones en la aplicación.

En tu aplicación: debes indicar de forma transparente qué es lo que ofreces. Esto incluye, por ejemplo, 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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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" en una suscripción que se cobra periódicamente.



① El botón 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.

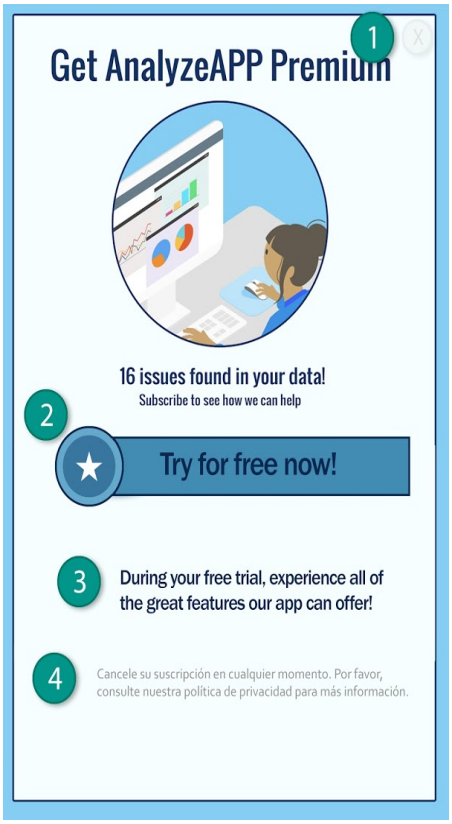
④ La oferta debe estar localizada en el mismo idioma que los términos y condiciones para que los usuarios puedan entenderla por completo.

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 saben cómo y cuándo la prueba gratuita se convertirá en una suscripción de pago, cuánto cuesta la suscripción de pago, y que pueden cancelar la prueba si no quieren que se convierta en una suscripción de pago.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 y cancelación de suscripciones

Como desarrollador, debes asegurarte de que tu aplicación incluya un aviso claro sobre cómo puede gestionar o cancelar su suscripción el usuario.

Eres responsable de notificar a los usuarios los cambios que hagas en tu suscripción y en las políticas de reembolsos y cancelación, así como de garantizar que estas cumplan la legislación aplicable.

Anuncios

No admitimos aplicaciones que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los publica. Consideramos que los anuncios publicados son parte de tu aplicación, así que deben cumplir todas nuestras políticas. Consulta las políticas sobre anuncios de juegos de apuestas.

Uso de los datos de ubicación para anuncios

Existen aplicaciones que, para publicar anuncios, amplían el uso de los datos de ubicación del dispositivo que están basados en permisos. Estas aplicaciones están sujetas a la política sobre Información Personal y Sensible y deben cumplir los siguientes requisitos:

- Los usuarios deben poder identificar con claridad el uso o la recogida con fines publicitarios de los datos de ubicación del dispositivo que están basados en permisos. Además, este proceso debe estar documentado en la política de privacidad obligatoria de la aplicación, incluyendo el enlace a cualquier política de privacidad pertinente de la red publicitaria donde se aborde el uso de los datos de ubicación.

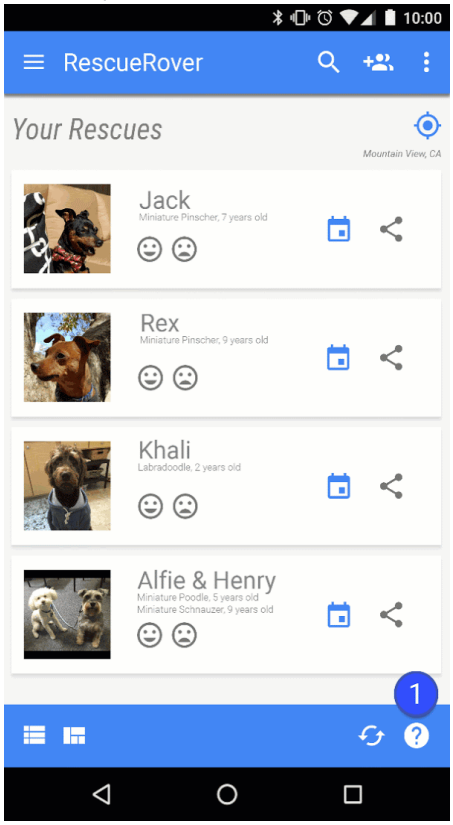
- De acuerdo con los requisitos de los permisos de ubicación, este tipo de permisos solo se puede solicitar para implementar los servicios o las funciones actuales en la aplicación. No se pueden solicitar permisos de ubicación del dispositivo solo para usar anuncios.

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.

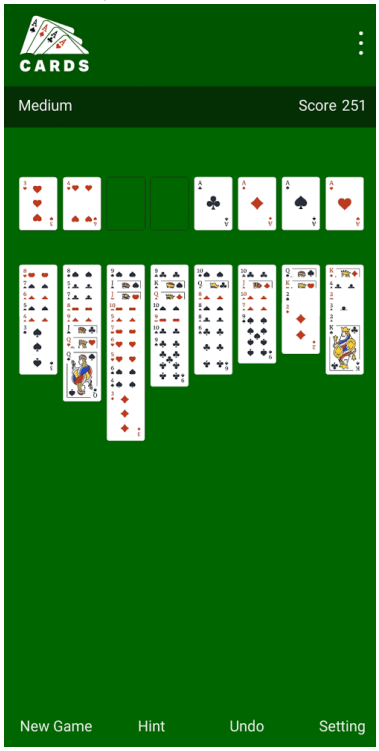
A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

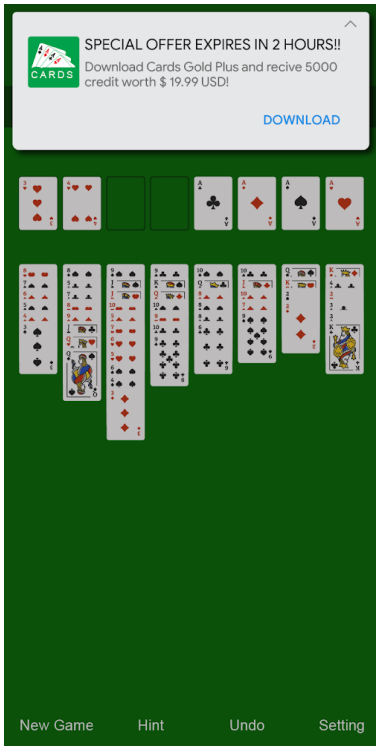
- Anuncios que imitan la interfaz de usuario de una aplicación:



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

- Anuncios que imitan una notificación del sistema:





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 ni 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

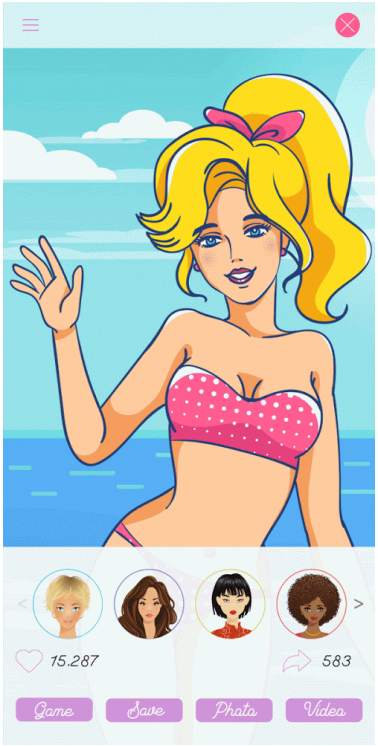
dentro de la aplicación que los publique. Si tu aplicación muestra anuncios intersticiales u otros anuncios que interfieran con el uso normal, el usuario debe poder cerrarlos fácilmente sin ninguna penalización.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

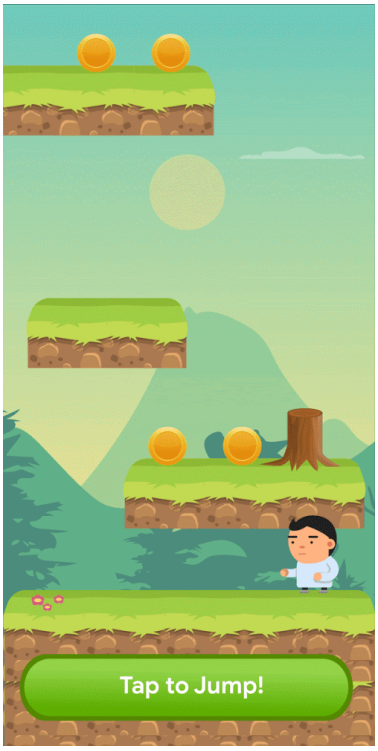
- Anuncios que ocupan toda la pantalla o interfieren con el uso normal y no ofrecen ningún método claro para cerrarlos:

① Este anuncio no tiene ningún botón para cerrarlo.

- 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.



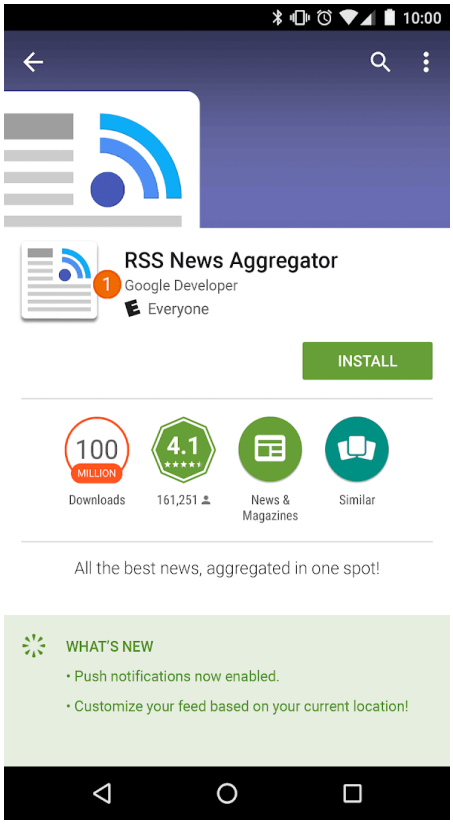
Un anuncio que aparece de repente en una zona en la que el usuario está acostumbrado a tocar para usar funciones en la aplicación.

Interferir con 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.

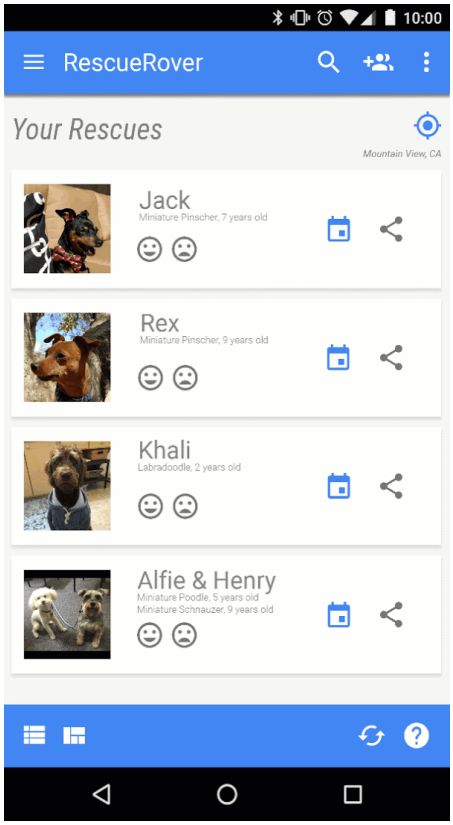
A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 esta pantalla.

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

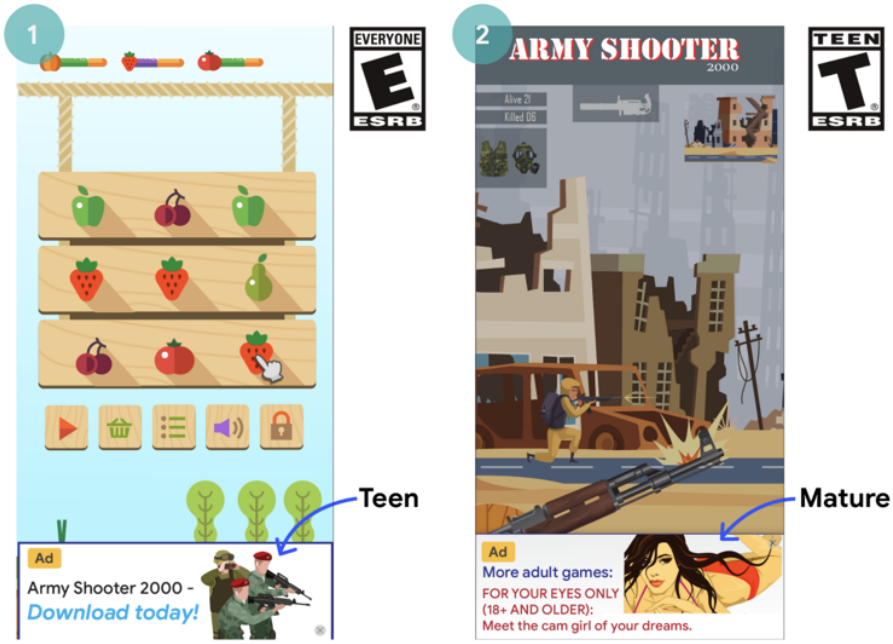


Descripción: el usuario intenta salir de la aplicación y acceder a la pantalla de inicio, pero el proceso se interrumpe con un anuncio.

Anuncios inadecuados

Los anuncios que se muestran en las aplicaciones deben ser adecuados para la audiencia a la que están dirigidos, aunque el contenido en sí mismo cumpla nuestras políticas.

A continuación te mostramos un ejemplo de una infracción frecuente:



① Este anuncio es inadecuado (Adolescente) para la audiencia a la que va dirigida esta aplicación (mayores de 7 años).
② Este anuncio es inadecuado (Adulto) para la audiencia a la que va dirigida esta aplicación (mayores de 12 años)

Uso del ID de publicidad de Android

La versión 4.0 de los Servicios de Google Play ha introducido nuevas API y un ID que pueden utilizar los proveedores de análisis y de publicidad. A continuación se indican los términos de uso de este ID.

- **Uso.** El identificador de publicidad de Android 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 de identificación personal 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 Analytics: El identificador de publicidad solo debe vincularse a información personal identificable o asociada a cualquier identificador de dispositivo persistente (por ejemplo, SSAID, dirección MAC, IMEI, etc.) con el consentimiento explícito del usuario.
- **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. Asimismo, se debe respetar la opción del usuario para inhabilitar la publicidad basada en intereses o los anuncios personalizados. Si un usuario ha habilitado esta opción, no puedes utilizar el identificador de publicidad para crear perfiles de usuario con fines publicitarios o 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.
- **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 estos términos, 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 Usuario.
- **Cumplimiento de los términos de uso**. El identificador de publicidad solo podrá utilizarse de acuerdo con estos términos, incluyendo el uso que haga de él cualquier parte con la que puedas compartirlo 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.

Programa de Anuncios para Familias

Si publicas anuncios en tu aplicación y tu audiencia objetivo solo incluye niños, según lo descrito en la Política de Familias, debes usar los SDK de publicidad que cumplan los requisitos de autocertificación de las políticas de Google Play, incluidos los requisitos que se indican más abajo sobre certificación de SDKs de publicidad. Si la audiencia objetivo de tu aplicación incluye tanto niños como adultos, debes implementar filtros de edad y asegurarte de que los anuncios que se muestran a los niños proceden exclusivamente de uno de los SDK de publicidad autocertificados. Las aplicaciones del programa Diseñado para Familias solo deben usar SDK de publicidad autocertificados.

El uso de SDK de publicidad certificados por Google Play solo es necesario si utilizas SDKs para mostrar publicidad a niños. Sin una autocertificación de Google Play de los SDK de publicidad, 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. Se permite lo siguiente:

- Publicar anuncios propios mediante los cuales utilices 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 gestionar el inventario.

Requisitos de certificación de los SDK de publicidad

- Define el contenido de los anuncios y los comportamientos potencialmente inadecuados y prohíbelos en los términos o las políticas de los SDK de publicidad. Las definiciones deben cumplir las Políticas del Programa para Desarrolladores de 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 que Google proporciona a los SDK 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 niños a la hora de publicar anuncios. Este tratamiento debe cumplir las leyes y normativas aplicables, 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 SDK de anuncios inhabiliten los anuncios personalizados, la publicidad basada en intereses y el remarketing para obtener la clasificación de contenido dirigido a niños.
- Permitir que los editores seleccionen formatos de anuncio que cumplan la política sobre Anuncios y Monetización para Familias de Play y los requisitos del Programa Aprobada por profesores.
- Cuando se utilicen las pujas en tiempo real para mostrar anuncios a niños, las creatividades deben haberse revisado y los indicadores de privacidad deben haberse propagado a los postores.
- Proporciona a Google suficiente información, como la que se indica en el formulario de interés, para verificar que el SDK de publicidad cumple todos los requisitos de la certificación y responde lo antes posible a cualquier solicitud de información posterior.

Nota: Los SDK de publicidad deben admitir tecnologías de servicio de anuncios que cumplan todas las normativas que puedan aplicarse a los editores en relación con el contenido dirigido a niños.

Requisitos de mediación para plataformas que muestran anuncios a niños:

- Solo se deben usar SDKs de publicidad certificados de Play o implementar las medidas de protección necesarias para que los anuncios publicados por los SDK 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 niños.

Los desarrolladores pueden consultar la lista de SDK de publicidad certificados.

También pueden compartir un formulario de interés con los SDK de publicidad que quieran autocertificarse.

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 actividades promocionales engañosas o dañinas para los usuarios o para el ecosistema de desarrolladores. Entre estas, se incluyen las aplicaciones con este comportamiento:

- Uso de publicidad engañosa en sitios web, aplicaciones u otras propiedades, como las notificaciones que son similares a las del sistema y las alertas
- Promoción o instalación de sistemas que provocan redireccionamientos a Google Play o la descarga de aplicaciones sin informar al usuario
- Promoción no solicitada a través de servicios SMS

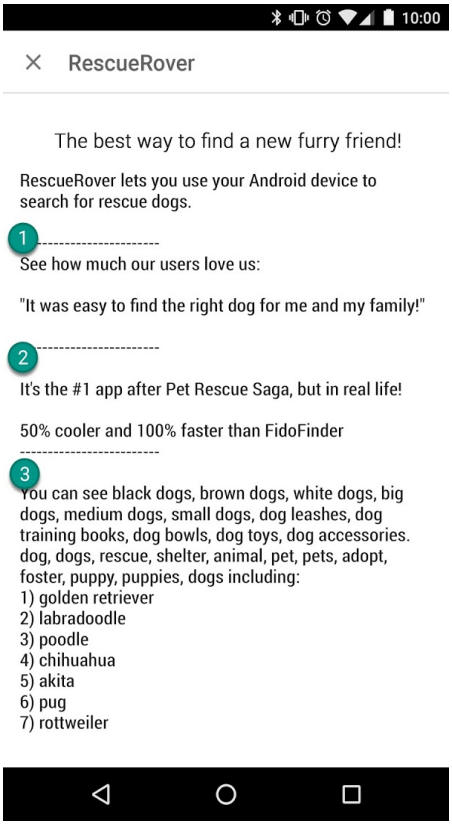
Eres responsable de garantizar que las redes publicitarias o las entidades asociadas con tu aplicación cumplan estas políticas y no se lleven a cabo actividades promocionales prohibidas.

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.

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

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:



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

A continuación te indicamos algunos ejemplos de texto, imágenes o vídeos inapropiados para 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:

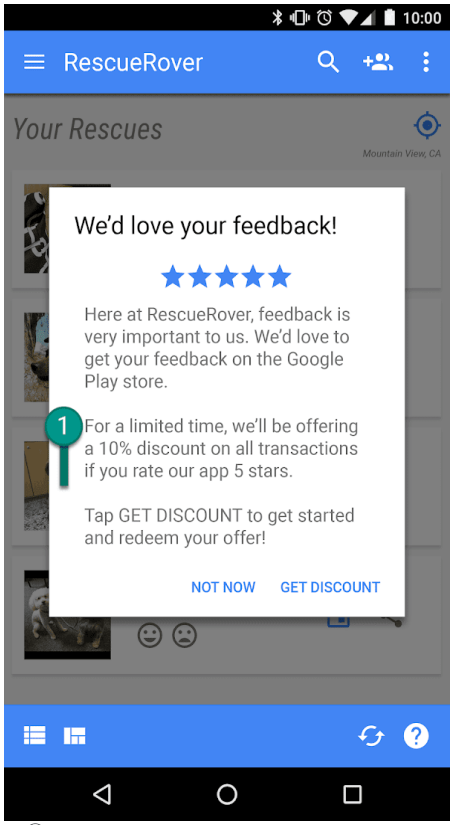
- Destaca las virtudes de tu aplicación. Comparte información interesante y atractiva sobre tu aplicación para que los usuarios comprendan por qué es especial.
- Comprueba que el título y la descripción de tu aplicación describan de forma precisa sus funciones.
- Evita el uso de palabras clave y referencias 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 inapropiados 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 opiniones ni los recuentos de instalaciones de productos (por ejemplo, mediante valoraciones, opiniones o instalaciones fraudulentas o incentivadas).

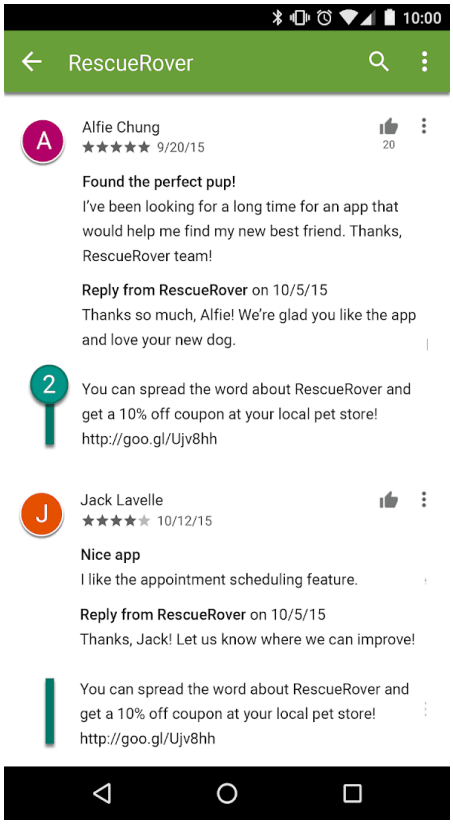
A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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), por ejemplo, afiliados, 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.

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 del contenido.

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

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 obtener 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 que se declare como aplicación de "Noticias" en Google Play debe cumplir todos los requisitos siguientes.

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

Las aplicaciones de noticias deben, en todos los casos:

- Proporcionar información sobre la propiedad del editor de prensa y sus colaboradores, incluidos, entre otros, el sitio web oficial de las noticias publicadas en tu aplicación, información de contacto válida y verificable y el editor original de cada artículo.
- Tener un sitio web o una página en la aplicación que proporcione información de contacto válida del editor de prensa.

Las aplicaciones de noticias no deben, en ningún caso:

- Contener errores ortográficos y gramaticales importantes.
- Incluir solamente contenido estático (por ejemplo, contenido con varios meses de antigüedad).
- Tener como objetivo principal el marketing de afiliación o los 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 de Google Noticias.

Spam y funcionalidad mínima

Como mínimo, las aplicaciones deben proporcionar a los usuarios un nivel básico de funcionalidad y una experiencia de usuario respetuosa. Las aplicaciones que fallan, que tienen un comportamiento que no ofrece una experiencia de usuario funcional o que solo sirven para enviar spam a los usuarios o a Google Play no aportan valor al catálogo.

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.

Mensajes de spam

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.

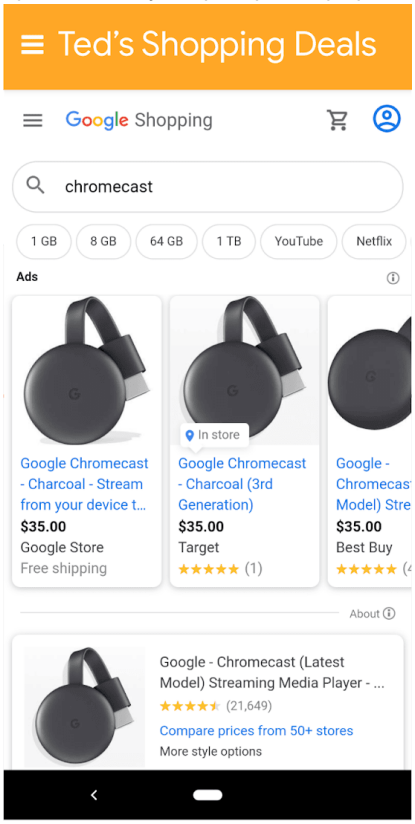
Spam de afiliados y de vistas web

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

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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:



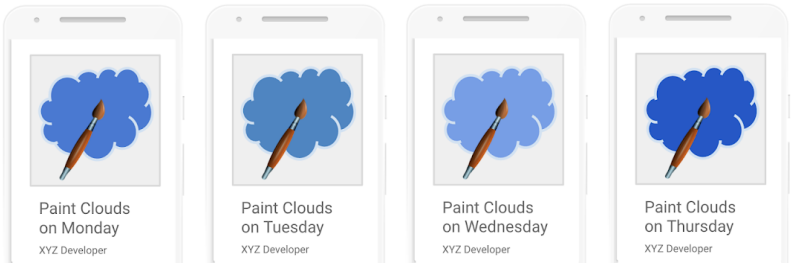
Esta aplicación se llama "Ted's Shopping Deals" y lo único que hace es proporcionar una WebView de Google Shopping.

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.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 cuyo objetivo principal sea publicar anuncios.

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Aplicaciones en las que se muestren anuncios intersticiales después de cada acción del usuario (por ejemplo, cuando hace clic o desliza el dedo).

Funcionalidad mínima

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

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- Aplicaciones que se han diseñado sin ningún objetivo o que no tienen ninguna función.

Funcionalidad defectuosa

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

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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. No olvides revisar la lista que se incluye a continuación 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 Google 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.

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.

Obtén más información sobre el proceso del contenido familiar y consulta la lista de comprobación interactiva en la Academia de Aplicaciones.

Crear aplicaciones para niños y familias

Cada vez se usa más la tecnología como parte de la vida familiar, y los padres buscan contenido seguro y de calidad que puedan compartir 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 indicar claramente que tu aplicación no está dirigida a niños, para lo que tendrás que aceptar incluir una etiqueta de advertencia.

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 te has cerciorado de que 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 niños, debes cumplir los siguientes requisitos. De lo contrario, tu aplicación se podrá suspender o retirar.

1. **Contenido de la aplicación:** el contenido de tu aplicación al que pueden acceder niños debe ser adecuado para ellos.
2. **Respuestas de Google Play Console:** debes responder de forma precisa a las preguntas sobre tu aplicación en Google Play Console y actualizar las respuestas si haces algún cambio en tu aplicación.
3. **Anuncios:** si tu aplicación muestra anuncios a niños o usuarios de edad desconocida, debes:
   - Usar únicamente SDKs de anuncios certificados de Google Play para mostrar anuncios a esos usuarios.
   - Asegurarte de que los anuncios que se muestren a esos usuarios no están basados en intereses (publicidad orientada a usuarios individuales que tienen determinadas características basadas en su comportamiento de navegación online) ni utilizan el remarketing (publicidad orientada a usuarios individuales basada en una interacción anterior con una aplicación o sitio web).
   - Asegurarte de que el contenido de los anuncios que se muestran a esos usuarios sea adecuado para niños.
   - Asegurarte de que los anuncios que se muestran a esos usuarios sigan los requisitos de formatos para familias.
   - Cumplir todas las obligaciones legales y normas del sector relativas a la publicidad dirigida a menores.
4. **Recogida de datos:** debes especificar si recoges en tu aplicación algún tipo de información personal y sensible de niños, incluidos los datos recogidos a través de APIs y SDKs. Entre la información sensible de niños cabe citar, entre otros datos, información de autenticación, datos de detección mediante cámaras y micrófonos, datos de dispositivos, ID de Android, datos de uso de anuncios e ID de publicidad.
5. **APIs y SDKs:** tu aplicación debe implementar cualquier API o SDK correctamente.
   - Las aplicaciones dirigidas únicamente a niños no pueden contener APIs ni SDKs cuyo uso no se haya aprobado en servicios para niños. Entre ellas 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 niños como a adultos no deben implementar APIs ni SDKs cuyo uso no se haya aprobado en servicios para niños, a menos que se utilicen con una pantalla de edad neutral o que se implementen de forma que no se recojan datos de niños (por ejemplo, ofreciendo el inicio de sesión de Google como función opcional). Las aplicaciones dirigidas tanto a niños 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 niños.
6. **Política de privacidad:** debes incluir un enlace a la política de privacidad de tu aplicación en la página de la ficha de Play Store. Este enlace se debe mantener mientras la aplicación esté disponible y debe dirigir a una política de privacidad que, entre otras cosas, describa de forma precisa el uso y la recogida de datos de tu aplicación.
7. **Restricciones especiales:**
   - Si tu aplicación usa realidad aumentada, debes incluir una advertencia de seguridad que se muestre inmediatamente al abrir la sección de RA. 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 conocer bien el entorno).

- Tu aplicación no debe requerir el uso de un dispositivo no recomendado para niños (por ejemplo, Daydream u Oculus).

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

A continuación, te mostramos algunos ejemplos de infracciones frecuentes:

- 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 presentan contenido que infringe las Políticas del Programa para Desarrolladores de Google Play.
- Aplicaciones que muestran anuncios para adultos (por ejemplo, contenido violento, contenido sexual o de juegos de apuestas) a niños. Consulta las políticas sobre Anuncios y Monetización para Familias para obtener más información sobre las políticas de Google Play sobre publicidad, compras en la aplicación y contenido comercial para niños.

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 en el Acuerdo de Distribución para Desarrolladores.

Consulta en este artículomás 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 su contenido deben ser relevantes y adecuados para niños, así como cumplir todos los requisitos que se especifican más abajo. 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.

Requisitos del programa Diseñado para Familias

1. Las aplicaciones deben estar clasificadas como "Para todos" o "Para mayores de 10 años" según el sistema de la ESRB (comisión de clasificación de software de entretenimiento de Estados Unidos), o tener una clasificación equivalente.
2. Debes especificar de forma precisa los elementos interactivos de la aplicación en el cuestionario sobre clasificación del contenido de Google Play Console. Entre otras cosas, debes indicar lo siguiente:
   - Si los usuarios pueden interactuar con el contenido o intercambiar información.
   - Si tu aplicación comparte con terceros información personal proporcionada por los usuarios.
   - Si tu aplicación comparte la ubicación física de los usuarios con otros usuarios.
3. Si tu aplicación utiliza la API Android Speech, se debe asignar el valor PackageName al parámetro RecognizerIntent.EXTRA_CALLING_PACKAGE.
4. Las aplicaciones solo deben usar SDKs de anuncios certificados de Google Play.
5. Las aplicaciones diseñadas específicamente para niños no pueden solicitar permisos de ubicación.
6. 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.

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.
- Aplicaciones que utilizan un icono de aplicación o un icono del launcher que es inadecuado para niños.

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 fomentan 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 chef, cuidador, príncipe o princesa, bombero, policía o personaje de ficción.

Anuncios y monetización

Las políticas que se incluyen más abajo se aplican a toda la publicidad de tu aplicación, incluida la de tus aplicaciones y la de aplicaciones de terceros, las ofertas de compras en aplicaciones o cualquier otro contenido comercial (como colocación de productos pagada) que se muestre a los usuarios de aplicaciones que estén sujetas a los requisitos de la Política de Familias o del programa Diseñado para Familias. Cualquier anuncio, oferta de compras en la aplicación y contenido comercial de estas aplicaciones debe cumplir la legislación y la normativa aplicables (como las directrices de autorregulación o del sector correspondientes).

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

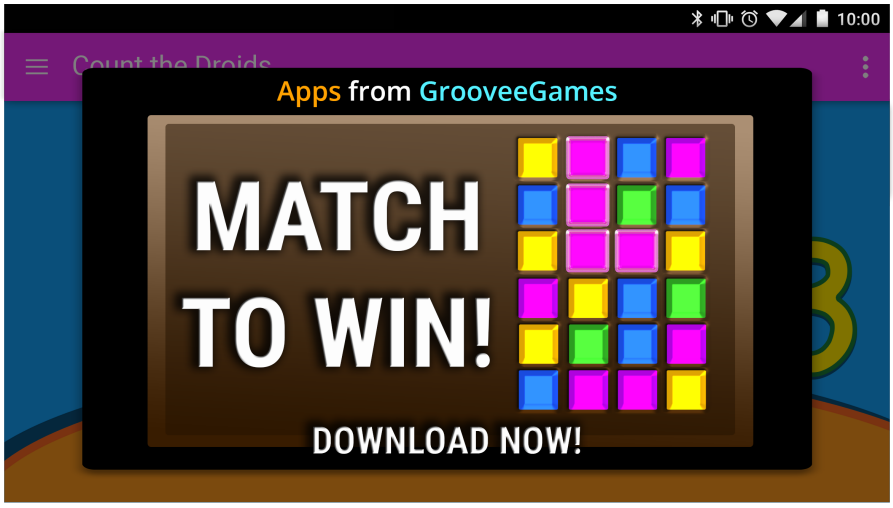
Requisitos de formato de los anuncios

Los anuncios y ofertas de compras en la aplicación no deben incluir contenido engañoso ni estar diseñados de forma que den lugar a clics involuntarios por parte de usuarios que sean niños. No se permite lo siguiente:

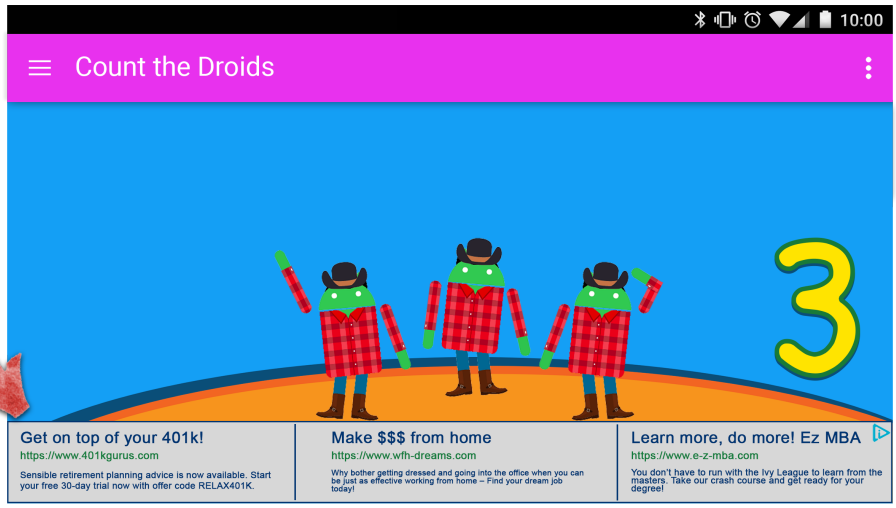
- Anuncios invasivos, incluidos los que ocupan toda la pantalla o interfieren con el uso normal y no ofrecen ningún medio claro para ignorarlos (por ejemplo, muros de anuncios)
- Mostrar anuncios que interfieran con el uso normal de la aplicación o el juego y que no se puedan cerrar después de 5 segundos. Los anuncios que no interfieran con el uso normal de la aplicación o juego pueden durar más de 5 segundos (por ejemplo, contenido de vídeo con anuncios integrados).
- Mostrar ofertas o anuncios intersticiales de compras en la aplicación 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.
- Publicar anuncios u ofertas de compras en la aplicación 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 y dinero real para hacer compras en la aplicación.

A continuación se incluyen algunos ejemplos de infracciones frecuentes por el formato de los anuncios:

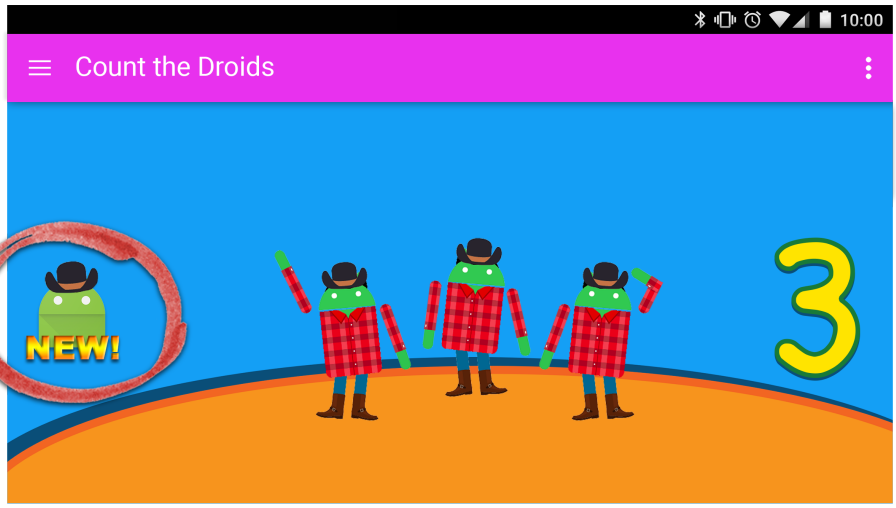
- Anuncios que se mueven cuando el usuario intenta tocarlos para cerrarlos
- Anuncios que ocupan la mayor parte de la pantalla del dispositivo o todo el espacio sin que el usuario pueda cerrarlos fácilmente, como se muestra en el siguiente ejemplo:



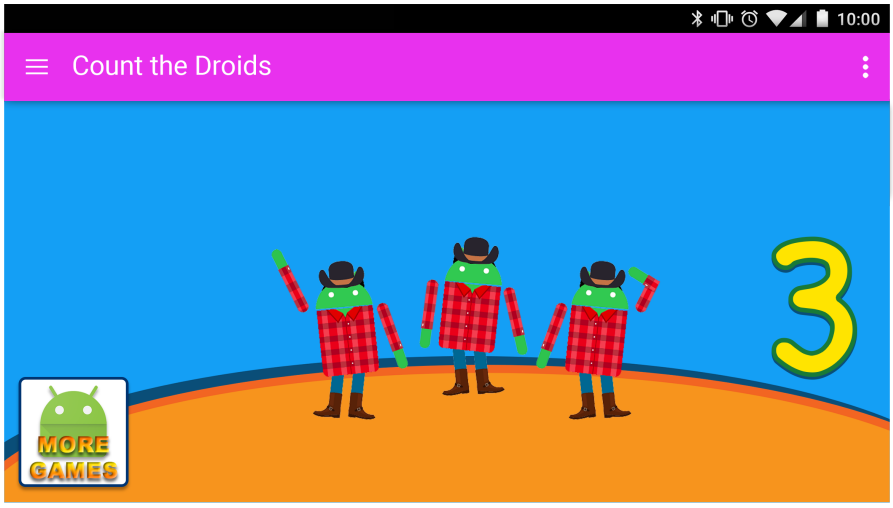
- Anuncios de banner que muestran varias ofertas, como se muestra en el siguiente ejemplo:



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



- Botones o anuncios que promocionan otras de tus aplicaciones de Google Play Store y que no se pueden 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.

SDKs de publicidad

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

En la página de la política del Programa de Anuncios para Familias puedes consultar más información sobre estos requisitos y ver la lista actual de SDK de publicidad aprobados.

Si utilizas AdMob, accede al Centro de Ayuda de AdMob para obtener 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 SDK de publicidad 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 niños.

Medidas de cumplimiento

Evitar las infracciones de las políticas siempre es mejor que tener que corregirlas. No obstante, si se produce una infracción, nos comprometemos a ayudar a que los desarrolladores comprendan cómo pueden mejorar sus aplicaciones y cumplir las directrices. Si detectas una infracción o tienes alguna pregunta sobre cómo corregir una, 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.

Eliminación

- La aplicación, junto con sus versiones anteriores, se eliminará 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 eliminada hasta que hayas corregido todas las infracciones de las políticas.

Suspensión

- La aplicación, junto con sus versiones anteriores, se eliminará 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 las valoraciones 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 visibilidad 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 las valoraciones de la aplicación.

Cancelación de cuentas

- Si se cancela tu cuenta de desarrollador, todas las aplicaciones de tu catálogo se eliminarán 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.

Gestionar y denunciar infracciones de las políticas

Apelar una medida de cumplimiento

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.

- Apelaciones y 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 comentarios y aplicaciones inapropiados
- Mi aplicación se ha retirado de Google Play
- Cancelación de cuentas de desarrollador de Google Play

Danos más información para que podamos ayudarte