Políticas del Programa para Desarrolladores (vigentes a partir del 5 de mayo de 2021)

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

Su innovación impulsa nuestro éxito compartido, pero conlleva cierta responsabilidad. Las Políticas del Programa para Desarrolladores y el Acuerdo de Distribución para Desarrolladores nos permiten asegurarnos de seguir brindando juntos las apps más innovadoras y confiables del mundo a más de mil millones de personas mediante Google Play. Lo invitamos a explorar nuestras políticas a continuación.

Contenido Restringido

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

Menores en Situación de Riesgo

Las aplicaciones que incluyen contenido que sexualiza a menores de edad se quitan inmediatamente de Store. Este tipo de aplicaciones incluye, sin limitaciones, las que promocionen la pedofilia o las interacciones inapropiadas con menores de edad (p. ej., caricias inapropiadas o manoseo).

Tampoco se permiten las aplicaciones atractivas para niños que tengan temas de adultos, lo que incluye, sin limitaciones, violencia excesiva y derramamiento de sangre, ni las aplicaciones que representen o fomenten actividades dañinas y peligrosas. Tampoco permitimos las apps que promocionen imágenes corporales o personales negativas, incluidas aquellas que representen, con fines de entretenimiento, pérdida de peso y otros ajustes estéticos de la apariencia física de una persona.

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

Contenido Inapropiado

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

Contenido Sexual y Lenguaje Obsceno

No permitimos apps que incluyan o promuevan contenido sexual o lenguaje obsceno, como pornografía o cualquier contenido o servicio destinado a brindar placer de carácter sexual. Se permite la publicación de contenido que incluya imágenes de desnudos si su objetivo principal es educativo, documental, científico o artístico, y no injustificado.

Los siguientes son ejemplos comunes de incumplimiento:

- Representaciones de desnudos sexuales o posturas provocativas en las que el sujeto está desnudo, desenfocado o con poca ropa, o en las que la ropa que viste no sería aceptable en un contexto público adecuado

- Representaciones, animaciones o ilustraciones de actos sexuales, posturas provocativas o representaciones sexuales de partes del cuerpo
- Contenido que represente o sirva de ayuda sexual, guías sexuales, temas sexuales ilegales y fetichismo
- Contenido obsceno o lascivo, lo que incluye, sin limitaciones, lenguaje obsceno, insultos, texto explícito, palabras clave de contenido sexual para adultos en la ficha de Play Store o en la app
- Contenido que represente, describa o promueva la zoofilia
- Aplicaciones que promuevan entretenimiento de tipo sexual, servicios de acompañantes o servicios de otro tipo sobre los que se pueda interpretar que proporcionan actos sexuales a cambio de una compensación
- Aplicaciones que degraden o deshumanicen a las personas

Incitación al Odio o a la Violencia

No permitimos apps que promuevan la violencia o fomenten el odio hacia una persona o hacia grupos de individuos en función de su origen étnico o raza, religión, discapacidad, edad, nacionalidad, condición de veterano de guerra, orientación sexual, género, identidad de género o alguna otra característica que esté asociada con la marginación o la discriminación sistémicas.

Es posible que, en ciertos países, se bloqueen las apps que incluyan contenido educativo, documental, científico o artístico relacionado con los nazis, de conformidad con las leyes y normativas locales.

Estos son ejemplos comunes de incumplimiento:

- Contenido o discursos que afirmen que un grupo protegido es inhumano, inferior o digno de ser odiado
- Apps que contengan insultos, estereotipos o teorías que indiquen que un grupo protegido posee características negativas (p. ej., que son malintencionados, corruptos, malvados, etc.) o afirmen de manera explícita o implícita que ese grupo es una amenaza
- Contenido o discursos que pretendan alentar a otros a creer que se debe odiar o discriminar a las personas porque pertenecen a un grupo protegido
- Contenido que promocione símbolos de odio, como banderas, símbolos, insignias, parafernalia o comportamientos asociados con grupos de odio

Violencia

No permitimos apps que representen o muestren violencia gratuita y otras actividades peligrosas. Por lo general, se permiten las apps que representan violencia ficticia en el contexto de un juego, como dibujos animados, o representaciones de caza o pesca.

Los siguientes son ejemplos comunes de incumplimiento:

- Representaciones gráficas o descripciones de violencia realista, o amenazas violentas hacia personas o animales
- Apps que promuevan acciones como autolesiones, suicidio, bullying, acoso, trastornos de alimentación, juegos de asfixia y otras conductas que puedan provocar lesiones graves o la muerte

Contenido Relacionado con el Terrorismo

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

No permitimos apps que incluyan contenido relacionado con el terrorismo, como el que fomente actos terroristas, incite a la violencia o celebre ataques terroristas. Si publica contenido relacionado con el terrorismo con fines educativos, documentales, científicos o artísticos, tenga presente que debe brindar información suficiente para que los usuarios entiendan el contexto.

Acontecimientos de Carácter Delicado

No permitimos apps que carezcan de sensibilidad razonable hacia desastres naturales, atrocidades, conflictos, la muerte y otros acontecimientos trágicos, o que se aprovechen de ellos. Por lo general, se permiten las apps cuyo contenido esté relacionado con un evento delicado si ese contenido tiene valor educativo, documental, científico o artístico, o tiene la intención de alertar a los usuarios sobre el evento delicado.

Estos son ejemplos comunes de incumplimiento:

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

Bullying y Acoso

No permitimos apps que contengan o faciliten el bullying, el acoso o las amenazas.

Estos son ejemplos comunes de incumplimiento:

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

Productos Peligrosos

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

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

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

Marihuana

No permitimos apps que faciliten la venta de marihuana ni productos de la marihuana, independientemente de su legalidad.

Los siguientes son ejemplos comunes de incumplimiento:

- Permitir que las personas pidan marihuana mediante una función de carrito de compra en la app
- Brindar asistencia a los usuarios para que organicen el retiro o la entrega de marihuana
- Facilitar la venta de productos que contengan THC (tetrahidrocannabinol), entre los que se incluyen productos como aceites de CBD, que contienen THC

Tabaco y Alcohol

No permitimos apps que faciliten la venta de tabaco (incluidos cigarrillos electrónicos y vaporizadores bolígrafo, o vapeadores) ni que fomenten el consumo ilegal o inadecuado de alcohol o tabaco.

Estos son ejemplos comunes de incumplimiento:

- Representar o promover el uso o la venta de alcohol o tabaco a menores
- Insinuar que el consumo de tabaco puede mejorar la condición social, sexual, profesional o atlética
- Mostrar el consumo excesivo de alcohol como algo positivo, incluida la representación positiva del consumo excesivo, sostenido o competitivo

Servicios Financieros

No permitimos apps que expongan a los usuarios a productos y servicios financieros engañosos o dañinos.

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

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

Opciones Binarias

No permitimos apps que brinden a los usuarios la posibilidad de comercializar opciones binarias.

Criptomonedas

No permitimos apps que minen criptomonedas en los dispositivos. Permitimos las apps que administren la minería de criptomonedas de manera remota.

Préstamos Personales

Definimos los préstamos personales como aquellos préstamos de dinero que un individuo, una organización o una entidad otorga a un consumidor individual de manera no recurrente y que no tienen como objetivo financiar la compra de un activo fijo ni educación. Los consumidores de préstamos personales requieren información sobre la calidad, las características, las tarifas, el cronograma de pagos, los riesgos y los beneficios de los productos de préstamos para poder tomar decisiones fundamentadas en cuanto a solicitar o no el préstamo.

- Ejemplos: Préstamos personales, préstamos de nómina, préstamos entre pares, préstamos de título
- Productos no incluidos: Hipotecas, préstamos para la compra de vehículos, préstamos para estudiantes, líneas de crédito rotativo (como tarjetas de crédito, líneas de crédito personales)

Las apps que proporcionan préstamos personales, incluidas, sin limitaciones, las que ofrecen préstamos directamente, las generadoras de clientes potenciales y aquellas que conectan a los consumidores con prestamistas externos, deben divulgar la siguiente información en los metadatos de la app:

- Período mínimo y máximo para el pago
- Tasa anual efectiva (TAE) máxima, que por lo general incluye la tasa de interés más las tarifas y otros cargos por un año, o alguna otra tasa similar que se calcule en concordancia con la legislación local
- Un ejemplo representativo del costo total del préstamo, incluidas todas las tarifas aplicables

- Una política de privacidad que divulgue de manera exhaustiva qué acceso se tendrá a los datos personales y sensibles de los usuarios, cómo se los recopilará y utilizará, y a quiénes se los divulgará

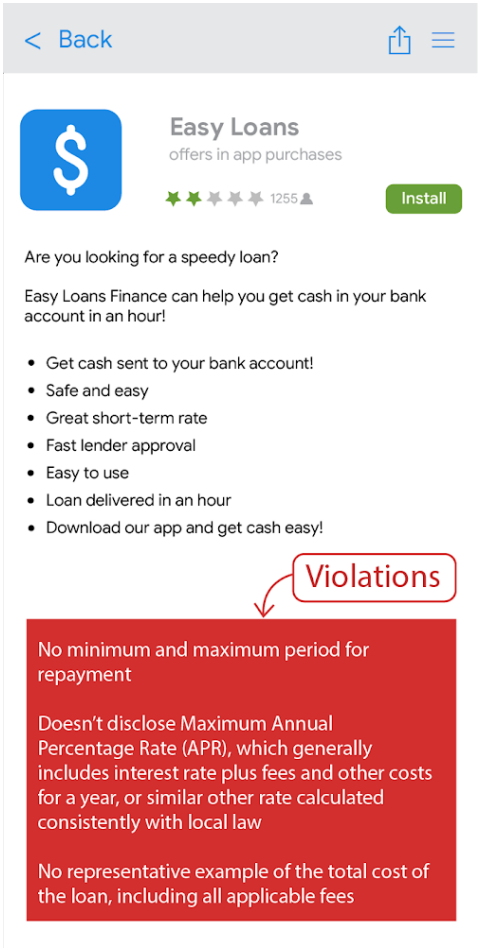
No permitimos apps que promuevan préstamos personales que requieran el pago íntegro en 60 días o menos desde la fecha de emisión del préstamo (nos referimos a estos como "préstamos personales a corto plazo").

Préstamos personales con TAE alta

En los Estados Unidos, no permitimos apps de préstamos personales en las que la tasa anual efectiva (TAE) sea del 36% o más alta. Las apps de préstamos personales publicadas en los Estados Unidos deben mostrar la TAE máxima, calculada en concordancia con la Ley Federal de Veracidad en Préstamos (Truth in Lending Act, TILA).

Esta política se aplica a las apps que ofrecen préstamos de forma directa, las que generan clientes potenciales y las que conectan a los consumidores con terceros prestamistas.

Este es un ejemplo de incumplimientos comunes:



Juegos de Apuestas, Concursos y Juegos con Dinero Real

Se permiten aplicaciones de juegos de apuestas con dinero real, anuncios relacionados con ellas, programas de lealtad ludificados y aplicaciones de deportes de fantasía diarios, siempre y cuando cumplan con ciertos requisitos.

Aplicaciones de Juegos de Apuestas

Conforme a las restricciones y el cumplimiento de todas las políticas de Google Play, se permiten las apps que habiliten o faciliten los juegos de apuestas en línea en los países que se incluyen en la siguiente tabla, siempre y

cuando el desarrollador complete el proceso de solicitud para las apps de juegos de apuestas que se distribuyen en Play, sea un operador gubernamental aprobado o esté registrado como operador con licencia ante la autoridad gubernamental de juegos de apuestas correspondiente en el país especificado y proporcione una licencia de operación válida en el país especificado para el tipo de producto de juegos de apuestas en línea que quiera ofrecer.

Solo se permiten apps válidas de juegos de apuestas autorizadas o con licencia que tengan los siguientes tipos de productos de juegos de apuestas en línea (consulte la siguiente tabla para conocer los tipos específicos de productos de juegos de apuestas que se permiten en cada país):

- Juegos de casino en línea
- Loterías
- Apuestas deportivas
- Deportes de fantasía diarios

Australia
Bélgica
Brasil
Canadá
Colombia
Dinamarca
Finlandia
Francia
Alemania
Irlanda
Japón
México
Nueva Zelanda
Noruega

Rumania

España

Suecia

Reino Unido

Estados Unidos

Para que las aplicaciones sean aptas, se deben cumplir los siguientes requisitos:

- El desarrollador debe completar el proceso de solicitud correctamente para distribuir la app en Play.
- La app debe satisfacer todas las leyes aplicables y los estándares de la industria de cada país en el que se distribuye.
- El desarrollador debe tener una licencia de juegos de apuestas válida para cada país, estado o territorio en el que se distribuya la app.
- El desarrollador no debe ofrecer un tipo de producto de juegos de apuestas que exceda el alcance de su licencia de juegos de apuestas.
- La app debe impedir que los usuarios menores de edad la usen.
- La app debe impedir su uso y el acceso a ella en países, estados, territorios o áreas geográficas que no abarque la licencia de juegos de apuestas proporcionada por el desarrollador.
- La app NO debe poder comprarse como una aplicación pagada en Google Play ni usar la Facturación integrada en Google Play.
- La descarga y la instalación de la app desde Play Store deben ser gratuitas.
- La app debe estar clasificada como "Solo para adultos" (AO) o un equivalente de la IARC.
- La app y su ficha deben mostrar información clara sobre el uso responsable de los juegos de apuestas.

Otras Aplicaciones de Juegos, Concursos y Torneos con Dinero Real

Para todas las demás apps que no cumplan con los requisitos de elegibilidad de las apps de juegos de apuestas que se indicaron anteriormente, no se permite contenido ni servicios que permitan o faciliten a los usuarios realizar apuestas o participar con dinero real (incluidos elementos integrados en la app comprados con dinero) para obtener un premio de valor monetario real. Se incluyen, entre otros, los casinos en línea, las apuestas deportivas, las loterías y los juegos que aceptan dinero y ofrecen premios monetarios o de otro valor real (excepto los programas que se permiten en virtud de los requisitos de los programas de lealtad lúdicos que se describen a continuación).

Ejemplos de incumplimientos

- Juegos que aceptan dinero a cambio de una oportunidad de ganar un premio material o monetario
- Apps que tienen elementos o funciones de navegación (p. ej. elementos de menú, pestañas, botones webviews, etc.) y que proporcionan un "llamado a la acción" para realizar apuestas o participar en torneos, concursos o juegos con dinero real, como las apps que invitan a los usuarios a apostar, registrarse o competir en un torneo para tener la oportunidad de ganar un premio en efectivo, con frases como "APUESTA", "REGÍSTRATE" O "COMPITE"

- Apps que aceptan o administran apuestas, monedas de la app, ganancias o depósitos con el fin de jugar por un premio material o monetario

Programas de lealtad lúdicos

En los casos en los que lo permita la ley y cuando no estén sujetos a requisitos adicionales de licencias de juegos de apuestas o videojuegos, se permiten los programas de lealtad que recompensen a los usuarios con premios reales o con un valor monetario equivalente, de conformidad con los siguientes requisitos de elegibilidad de Play Store:

Para todas las apps (ya sean juegos o no):

- Los beneficios, las ventajas o las recompensas del programa de lealtad deben ser claramente complementarios y estar sujetos a cualquier transacción monetaria apta dentro de la app (donde la transacción monetaria apta debe ser una transacción genuina y aparte para proporcionar bienes o servicios independientemente del programa de lealtad) y no pueden estar sujetos a compras ni asociados a ningún modo de intercambio que infrinja las restricciones de la política de Juegos, Concursos y Juegos de Apuestas con Dinero Real.
  - Por ejemplo, ninguna parte de la transacción monetaria apta puede representar el pago de una tarifa o apuesta para participar en el programa de lealtad, y esta transacción no debe derivar en la compra de bienes o servicios por encima de su precio habitual.

En el caso de las aplicaciones de juegos , se aplica lo siguiente:

- Los puntos o recompensas de fidelidad con beneficios, ventajas o recompensas asociados con una transacción monetaria que cumpla con las condiciones necesarias solo se pueden otorgar y canjear en función de una proporción fija que se documente de forma visible en la aplicación y también en las reglas oficiales del programa disponibles para todo el público. Además, **no** se pueden apostar, entregar como recompensa ni aumentar los beneficios ni el valor de canje recibidos en función del rendimiento del juego o los resultados basados en probabilidades.

En las aplicaciones que no son juegos, se aplica lo siguiente:

- Los puntos o recompensas de fidelidad pueden asociarse con un concurso o con resultados basados en probabilidades si cumplen con los requisitos que se indican a continuación. Los programas de lealtad que tengan beneficios, ventajas o recompensas asociados con una transacción monetaria apta deben hacer lo siguiente:
  - Publicar las reglas oficiales del programa dentro de la aplicación
  - En el caso de los programas que incluyan sistemas de recompensas variables, basados en el azar o aleatorizados, deben divulgar dentro de las condiciones oficiales del programa 1) las probabilidades de todo programa de recompensas que use probabilidades fijas para determinar las recompensas y 2) el método de selección (p. ej., las variables que se usan a fin de determinar la recompensa) para todos esos programas
  - Especificar una cantidad fija de ganadores, una fecha límite de ingreso fija y la fecha de entrega del premio, según la promoción, dentro del marco de las condiciones oficiales de un programa que ofrece rifas, sorteos y otras promociones del mismo estilo
  - Documentar de forma visible en la aplicación y en las condiciones oficiales del programa cualquier proporción fija de recompensas por lealtad o puntos de fidelidad que se acumule o canjee

Tipo de aplicación con programa de lealtad	Programa de lealtad lúdico y recompensas variables	Recompensas de lealtad según un programa o una proporción fijos	Términos y Condiciones para el programa de lealtad obligatorios	Los Términos y Condiciones deben divulgar las probabilidades o el método de selección de cualquier programa de lealtad basado en probabilidades
Juego	No se permiten	Se permiten	Obligatorios	N/A (Las apps de juegos no pueden tener elementos basados en probabilidades en los programas de lealtad)
Que no son juegos	Se permiten	Se permiten	Obligatorios	Obligatorio

Anuncios de juegos de apuestas o con dinero real, concursos y torneos en apps que se distribuyen en Play

Se permiten las aplicaciones que tienen anuncios que promocionan juegos de apuestas o torneos, concursos y juegos con dinero real, siempre y cuando cumplan con los siguientes requisitos:

- La aplicación y el anuncio (incluidos los anunciantes) deben satisfacer todas las leyes y los estándares de la industria aplicables en cualquier ubicación donde se muestre el anuncio.
- El anuncio debe cumplir con los requisitos de licencias de anuncios locales aplicables a todos los productos y servicios relacionados con juegos de apuestas que se promocionen.
- La app no debe mostrar anuncios de juegos de apuestas a menores de 18 años.
- La aplicación no debe estar inscrita en el programa Designed for Families.
- La app no debe estar segmentada para menores de 18 años.
- Si se promociona una app de juegos de apuestas (como se definió anteriormente), el anuncio debe mostrar información clara sobre el uso responsable de los juegos de apuestas en la página de destino, la ficha de la app promocionada o dentro de la app.
- La aplicación no debe proporcionar contenido de juegos de apuestas simulado (p. ej., aplicaciones de casino sociales o aplicaciones con máquinas tragamonedas virtuales).
- La aplicación no debe proporcionar funciones de asistencia ni complementarias (p. ej., funciones que contribuyan a la realización de apuestas, pagos, el seguimiento de resultados, probabilidades o rendimiento deportivos, o la administración de fondos de juegos de apuestas) con relación a juegos de apuestas, lotería, torneos ni juegos con dinero real.
- El contenido de la aplicación no debe promocionar ni dirigir a los usuarios a juegos de apuestas o loterías, torneos ni juegos con dinero real.

Solo las aplicaciones que cumplan con todos los requisitos mencionados en el artículo correspondiente (más arriba) pueden incluir anuncios de juegos de apuestas o torneos, loterías y juegos con dinero real. Solo las Aplicaciones de Juegos de Apuestas (como se definió anteriormente) o las Aplicaciones de Deportes de Fantasía Diarios (como se definió anteriormente) aceptadas y que cumplan con los requisitos del 1 al 6 mencionados más arriba pueden incluir anuncios de juegos de apuestas o torneos, loterías y juegos con dinero real.

Ejemplos de incumplimientos

- Una app diseñada para usuarios menores de edad que muestra un anuncio que promociona servicios de juegos de apuestas
- Un juego de casino simulado que promociona casinos con dinero real o dirige a los usuarios hacia ellos
- Una app de seguimiento de probabilidades deportivas que contiene anuncios de juegos de apuestas integrados que se vinculan a un sitio de apuestas deportivas
- Apps que tienen anuncios de juegos de apuestas que no cumplen con nuestra política de Anuncios Engañosos, como anuncios que aparecen a los usuarios en forma de botones, íconos u otros elementos interactivos en la app

Apps de deportes de fantasía diarios (DFS)

Solo se permiten las apps de deportes de fantasía diarios (DFS), según se definan en las leyes locales aplicables, que cumplan con los siguientes requisitos:

- La app 1) solo se distribuye en los Estados Unidos o 2) cumple con el proceso de solicitud y los requisitos de la sección Apps de juegos de apuestas que se mencionaron anteriormente para países distintos a Estados Unidos.
- El desarrollador debe completar correctamente el proceso de solicitud de DFS y recibir la aceptación para poder distribuir la aplicación en Play.
- La app debe cumplir con todas las leyes aplicables y los estándares de la industria de los países en los que se distribuye.
- La app debe impedir que los usuarios menores de edad hagan apuestas o realicen transacciones monetarias dentro de ella.
- La app NO debe poder comprarse como una aplicación pagada en Google Play ni usar la Facturación integrada en Google Play.
- La descarga y la instalación de la app desde Play Store deben ser gratuitas.
- La app debe estar clasificada como "Solo para adultos" (AO) o un equivalente de la IARC.
- La app y su ficha deben mostrar información clara sobre el uso responsable de los juegos de apuestas.
- La aplicación debe satisfacer todas las leyes y los estándares de la industria aplicables en todos los estados o territorios de EE.UU. en los que se distribuya.
- El desarrollador debe tener una licencia válida para cada uno de los estados o territorios de los EE.UU. en los que se requiera una para las apps de deportes de fantasía diarios.
- La app debe impedir su uso en los estados o territorios de los EE.UU. en los que el desarrollador no posea la licencia requerida para las apps de deportes de fantasía diarios.
- La app debe impedir su uso en los estados o territorios de los EE.UU. donde no sean legales las apps de deportes de fantasía diarios.

Actividades ilegales

No permitimos apps que faciliten o promuevan actividades ilegales.

Los siguientes son ejemplos comunes de incumplimiento:

- Facilitar la compra o venta de drogas ilegales, o la compra o venta sin prescripción de medicamentos que deban venderse bajo prescripción médica

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

Contenido Generado por Usuarios

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

Las apps que incluyan CGU deben cumplir con lo siguiente:

- Deben requerir que los usuarios acepten las condiciones de uso o políticas del usuario de la app antes de crear o subir CGU.
- Deben definir el contenido y los comportamientos inaceptables (de una manera que cumpla con las Políticas del Programa para Desarrolladores de Play) y prohibirlos en las condiciones de uso o las políticas del usuario de la app.
- Deben implementar la moderación del CGU de manera rigurosa, efectiva y continua, y de forma razonable y coherente con los tipos de CGU que aloja la app.
  - En el caso de las apps de transmisión en vivo, el CGU inaceptable debe quitarse prácticamente en tiempo real.
  - En el caso de las apps de realidad aumentada (RA), la moderación de CGU (incluido el sistema de informes en la app) debe tener en cuenta tanto el CGU inaceptable de RA (p. ej., una imagen de RA sexualmente explícita) como la ubicación de anclaje de RA sensible (p. ej., contenido de RA anclado a un área restringida, como una base militar, o a una propiedad privada donde el anclaje de RA podría causar problemas al propietario).
- Deben proporcionar un sistema de fácil acceso integrado en la app para denunciar el CGU inaceptable, y tomar medidas contra ese CGU cuando corresponda.
- Deben quitar o bloquear a los usuarios con comportamiento inadecuado que infrinjan las condiciones de uso o la política del usuario de la app.
- Deben brindar protecciones para evitar que la monetización dentro de la app promueva un comportamiento reprochable por parte del usuario

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

Los siguientes son ejemplos comunes de incumplimiento:

- Promoción de contenido sexual explícito generado por el usuario, incluida la implementación de funciones pagas (o la posibilidad de incluirlas) cuyo principal objetivo sea fomentar que los usuarios compartan contenido inaceptable
- Apps que incluyan contenido generado por usuarios (CGU), pero que no contengan suficiente protección contra amenazas, bullying o acoso, en especial hacia menores
- Publicaciones, comentarios o fotos dentro de una app cuyo objetivo principal sea acosar o someter a una persona al abuso, a ataques malintencionados o al ridículo.
- Apps que con mucha frecuencia no resuelvan las denuncias de los usuarios acerca del contenido inaceptable

Sustancias No Aprobadas

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

- Todos los artículos de esta lista no exhaustiva de productos farmacéuticos y suplementos prohibidos
- Productos que contienen efedra
- Productos que contienen gonadotropina coriónica humana (hCG) en relación con la pérdida o el control del peso, o si se promocionan junto con esteroides anabólicos
- Suplementos herbales y dietéticos con ingredientes farmacéuticos activos o peligrosos
- Declaraciones falsas o engañosas de beneficios terapéuticos, incluidas las afirmaciones que insinúen que un producto es tan eficaz como los medicamentos de venta con receta o las sustancias controladas
- Productos sin aprobación gubernamental que se comercialicen de una manera que insinúe que su uso es seguro o que son eficaces para prevenir, curar o tratar determinadas enfermedades o problemas de salud
- Productos que hayan estado sujetos a acciones o advertencias reguladoras o gubernamentales
- Productos con nombres que pueden confundirse con productos farmacéuticos, sustancias controladas o suplementos no aprobados

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

Propiedad Intelectual

Cuando los desarrolladores copian el trabajo de otra persona o lo usan sin el permiso necesario, el propietario de ese trabajo podría verse perjudicado. No confíe en el uso desleal del trabajo de otras personas.

Propiedad Intelectual

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

Responderemos a las notificaciones claras de presuntos incumplimientos de los derechos de autor. Para obtener más información o enviar una solicitud de DMCA, consulte nuestros procedimientos relacionados con los derechos de autor.

Para enviar un reclamo sobre la venta o promoción para la venta de productos falsificados dentro de una app, envíe un aviso de falsificación.

Si usted es propietario de una marca y cree que hay una app en Google Play que incumple los derechos de su marca, comuníquese directamente con el desarrollador para resolver el problema. Si no puede llegar a un acuerdo con el desarrollador, use este formulario para enviar un reclamo por uso de marca.

Si cuenta con documentación escrita que demuestre que usted tiene permiso para usar la propiedad intelectual de un tercero en su app o ficha de Play Store (como nombres de marcas, logotipos y recursos gráficos), comuníquese con el equipo de Google Play antes de realizar el envío a fin de asegurarse de que no se rechace la app debido a un incumplimiento de la propiedad intelectual.

Uso No Autorizado de Contenido Protegido por Derechos de Autor

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

Tenga cuidado cuando use contenido protegido por derechos de autor para demostrar la funcionalidad de su app. En general, el enfoque más seguro es crear algo que sea original.

Estos son algunos ejemplos de contenido protegido por derechos de autor que se usa con frecuencia sin autorización o razón legal válida:

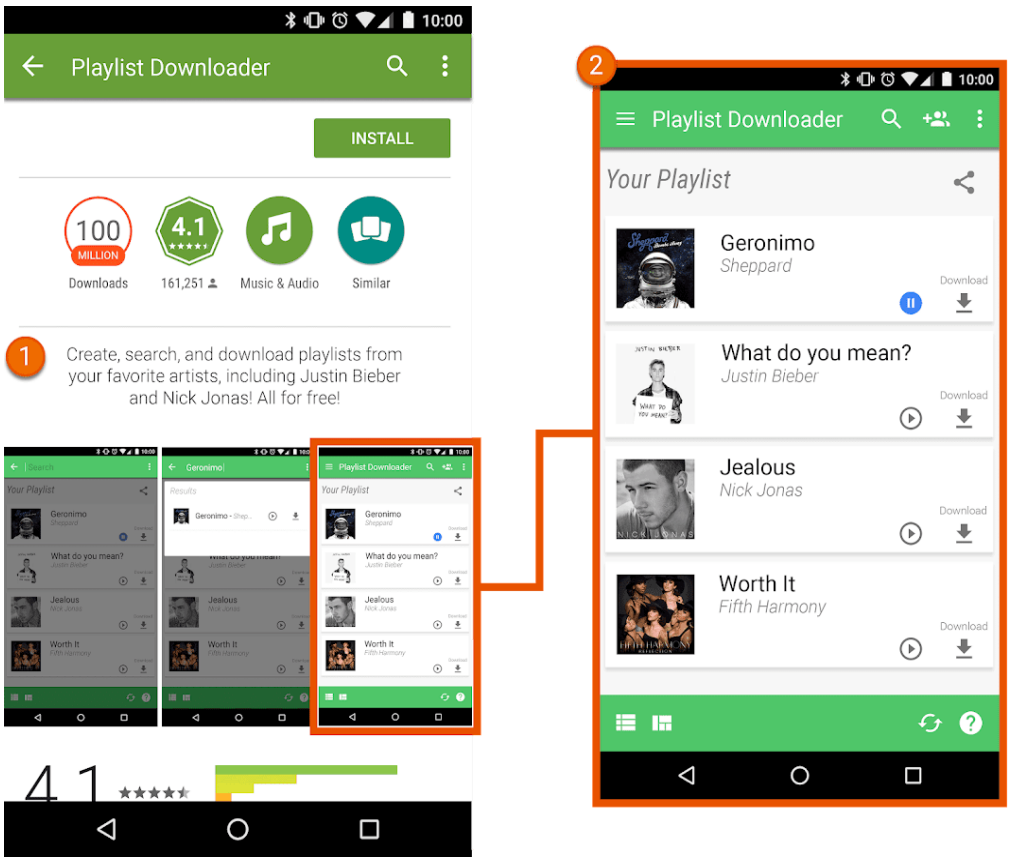
- Material gráfico para álbumes de música, videojuegos y libros
- Imágenes de comercialización de películas, televisión o videojuegos
- Material gráfico o imágenes de libros de cómics, dibujos animados, películas, videos de música o televisión
- Logotipos de equipos deportivos profesionales y universitarios
- Fotos tomadas de la cuenta de redes sociales de una persona pública
- Imágenes profesionales de personas públicas
- Reproducciones o "fan art" que no puedan distinguirse de la obra original protegida por derechos de autor
- Apps que tengan consolas que reproduzcan clips de audio de contenido protegido por derechos de autor
- Reproducciones completas o traducciones de libros que no sean de dominio público

Acciones que fomenten el incumplimiento de los derechos de autor

No permitimos apps que induzcan o fomenten el incumplimiento de los derechos de autor. Antes de publicar la app, busque posibles formas en las que esta pueda fomentar el incumplimiento de los derechos de autor, y pida asesoramiento legal si fuera necesario.

Los siguientes son ejemplos comunes de incumplimiento:

- Apps de streaming que permitan que los usuarios descarguen copias locales de contenido protegido por derechos de autor sin autorización
- Apps que alienten a los usuarios a transmitir y descargar obras protegidas por derechos de autor, incluidos videos y música, en incumplimiento de la legislación de derechos de autor aplicable



① La descripción en la ficha de la aplicación alienta a los usuarios a descargar contenido protegido por derechos

de autor sin autorización.
② La captura de pantalla de la ficha de la aplicación alienta a los usuarios a descargar contenido protegido por derechos de autor sin autorización.

Incumplimiento de Marca

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

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

Falsificación

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

Privacidad, Engaño y Abuso de Dispositivos

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

Datos del Usuario

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

Información Personal y Sensible

Los datos sensibles y personales de los usuarios incluyen, sin limitarse a ello, información de identificación personal, financiera, de pago y de autenticación; datos relacionados con la agenda telefónica, contactos, ubicación del dispositivo, SMS y llamadas; información del micrófono y la cámara, y otros datos sensibles relacionados con el uso o el dispositivo. Si su app administra datos sensibles de los usuarios, usted debe realizar lo siguiente:

- Limite su acceso a los datos personales o sensibles adquiridos a través de la app, así como la recopilación, el uso y el uso compartido de esa información, para fines directamente relacionados con la provisión y mejora de las funciones de la app (p. ej., una función que espera el usuario y que se documenta y anuncia en la descripción de la app en Play Store). Las aplicaciones que extienden el uso de estos datos para publicar anuncios deben cumplir con nuestra Política de Anuncios.
- Publique una política de privacidad, tanto en el campo designado en Play Console como en la app. La política de privacidad, junto con cualquier otro aviso de divulgación integrado en la aplicación, debe explicar

detalladamente cómo accede la aplicación a los datos del usuario, además de cómo los recopila, usa y comparte. Su política de privacidad debe revelar a qué tipos de datos personales y sensibles tiene acceso su aplicación, qué tipos de datos recopila, usa y comparte, y también con qué clases de terceros se comparten los datos personales o sensibles de los usuarios.
- Maneje todos los datos personales o confidenciales de los usuarios de forma segura, lo que incluye transmitirlos con criptografía moderna (por ejemplo, por HTTPS).
- Cuando esté disponible, use una solicitud de permisos de tiempo de ejecución antes de acceder a los datos mediante permisos de Android.
- No venda los datos sensibles ni personales de los usuarios.

Requisito de Divulgación Destacada y Consentimiento

En los casos en que tal vez los usuarios no tengan una expectativa razonable de que sus datos personales o sensibles sean necesarios para proporcionar o mejorar las características o las funciones que cumplan con las políticas dentro de tu app (p. ej., cuando la recopilación de datos se produce en segundo plano en la app), usted deberá cumplir con los siguientes requisitos:

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

- Debe estar dentro de la app, no solo en su descripción o en un sitio web.
- Se debe mostrar durante el uso normal de la app sin que el usuario tenga que ir al menú o la configuración.
- Debe describir los datos a los que se accede o que se recopilan.
- Debe explicar cómo se usarán o compartirán los datos.
- **No se puede** colocar únicamente en la política de privacidad o en las condiciones del servicio.
- **No se puede** incluir con otras divulgaciones que no estén relacionadas con la recopilación de datos personales o sensibles.

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

- Debe presentar el cuadro de diálogo de consentimiento de manera clara y sin ambigüedades.
- Debe exigir acciones afirmativas del usuario (p. ej., presionar para aceptar o marcar una casilla de verificación).
- **No debe** interpretar como consentimiento la acción de salir de la divulgación (incluidos presionar para salir o presionar el botón de inicio o atrás).
- **No debe** usar mensajes que caduquen o se descarten automáticamente como medio para obtener el consentimiento del usuario.

Los siguientes son ejemplos comunes de incumplimiento:

- Una app que accede al inventario de apps instaladas de un usuario y no trata estos datos como datos personales o sensibles sujetos a los requisitos de la Política de Privacidad, del manejo de datos y de Divulgación Destacada y Consentimiento
- Una app que accede a los datos del teléfono o de la agenda de contactos de un usuario y no los trata como datos personales o sensibles sujetos a los requisitos de la Política de Privacidad, del manejo de datos y de Divulgación Importante y Consentimiento
- Una app que graba la pantalla del usuario y no trata esta información como datos personales ni sensibles sujetos a esta política

- Una app que recopila la ubicación del dispositivo y no divulga su uso de forma exhaustiva ni obtiene el consentimiento de acuerdo con los requisitos anteriores
- Una app que recopila permisos restringidos en segundo plano, por ejemplo, para fines de seguimiento, investigación o marketing, y no divulga su uso de manera exhaustiva ni obtiene el consentimiento de acuerdo con los requisitos mencionados anteriormente

Restricciones Específicas para el Acceso a Datos Sensibles

Además de los requisitos anteriores, en la siguiente tabla, se describen los requisitos para actividades específicas.

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

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

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

- Debes cumplir con todas las leyes, directivas, regulaciones y reglas de privacidad, protección y seguridad de los datos aplicables.
- Debe procesar o usar la Información Personal de la UE, o acceder a estos datos, únicamente para fines acordes con el consentimiento otorgado por el individuo al cual se refiere dicha información.
- Debes implementar medidas organizativas y técnicas apropiadas para proteger la Información Personal de la UE contra cualquier pérdida, uso inadecuado y acceso, divulgación, alteración o destrucción no autorizada o ilícita.
- Debes proporcionar el mismo nivel de protección que requieren los Principios de Privacy Shield (Escudo de Privacidad) .

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

Permisos

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

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

Permisos Restringidos

Además de los anteriores, los permisos restringidos son aquellos que se designan como Riesgosos, Especiales o de Firma y están sujetos a los siguientes requisitos y restricciones adicionales:

- Los datos sensibles de los dispositivos o los usuarios a los que se acceda mediante Permisos Restringidos solo se pueden transferir a terceros si son necesarios para proporcionar o mejorar funciones o servicios existentes en la app que recopiló esos datos. También puede transferir datos cuando sea necesario para cumplir con la legislación aplicable o como parte de una fusión, adquisición o venta de activos, habiendo proporcionado una notificación legal adecuada a los usuarios. Se prohíben todas las demás transferencias o ventas de los datos de los usuarios.
- Se debe respetar la decisión de los usuarios si rechazan una solicitud de permisos restringidos; no se debe manipular ni forzar a los usuarios para que den su consentimiento a cualquier permiso que no sea crítico. Se deben realizar todos los esfuerzos razonables para ajustar el contenido a los usuarios que no otorguen acceso a permisos sensibles (p. ej., permitir que un usuario ingrese un número de teléfono de forma manual si restringió el acceso a los Registros de Llamadas).

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

Permisos de SMS y Registro de Llamadas

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

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

Las apps que no posean la función de controlador predeterminado de Asistente, Teléfono o SMS no pueden declarar el uso de los permisos anteriores en el manifiesto. Esto también se aplica al texto de marcador de

posición en el manifiesto. Además, las apps deben estar registradas de forma activa como controladores predeterminados de Asistente, Teléfono o SMS antes de solicitar a los usuarios que acepten cualquiera de los permisos anteriores. Asimismo, deben finalizar de inmediato el uso del permiso cuando dejen de ser controladores predeterminados. En esta página del Centro de ayuda, se pueden consultar los usos permitidos y las excepciones.

Las apps solo pueden usar el permiso (y cualquier dato derivado de este) para brindar su funcionalidad principal aprobada. La funcionalidad principal se define como el objetivo más importante de la app. Esto puede incluir una serie de funciones principales, las cuales deben estar claramente documentadas y promocionadas en la descripción de la app. Sin la función principal, la app se considerada "dañada" o inutilizable. Solo se deben transferir, compartir o usar con licencia estos datos a fin de brindar funciones o servicios principales dentro de la app, y no se puede extender su uso para ningún otro propósito (p. ej., mejorar otras apps o servicios, publicidad o marketing). No se pueden usar métodos alternativos (incluidos otros permisos, API o fuentes de terceros) para obtener datos atribuidos a los permisos de Registro de Llamadas o SMS relacionados.

Permisos de Ubicación

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

- Las apps no pueden acceder a los datos protegidos por permisos de ubicación (p. ej., ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) luego de que estos dejen de ser necesarios para implementar funciones o servicios existentes dentro de la app.
- Nunca debe solicitar permisos de ubicación a los usuarios únicamente con fines de publicidad o análisis. Las apps que extienden el uso permitido de este dato para publicar anuncios deben cumplir con nuestra Política de Anuncios.
- Las apps deben solicitar el alcance mínimo necesario (es decir, ubicación aproximada en lugar de precisa y uso en primer plano en vez de en segundo plano) para proporcionar el servicio o la función en curso que requiere la ubicación, y los usuarios deben tener una expectativa razonable de que el servicio o la función necesita el nivel de ubicación solicitado. Por ejemplo, es posible que rechacemos las aplicaciones que soliciten acceso o que accedan a la ubicación en segundo plano sin una justificación convincente.
- La ubicación en segundo plano solo se puede usar con el fin de proporcionar funciones beneficiosas para el usuario y relevantes para la funcionalidad principal de la aplicación.

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

- Se inició como una continuación de una acción iniciada por el usuario dentro de la aplicación.
- Finaliza inmediatamente después de que la app completa el caso de uso previsto de la acción iniciada por el usuario.

Las apps diseñadas específicamente para niños deben cumplir con la política de Designed for Families.

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 de Información Personal y Sensible y a los siguientes requisitos:

- Las apps solo deben solicitar acceso al almacenamiento del dispositivo que resulte fundamental para su funcionamiento y no pueden solicitar acceso al almacenamiento del dispositivo en nombre de ningún tercero que no esté relacionado con la funcionalidad crítica de la app.
- Los dispositivos Android que ejecuten R (Android 11, nivel de API 30) o versiones posteriores requerirán el permiso MANAGE_EXTERNAL_STORAGE para administrar el acceso en el almacenamiento compartido. Todas las apps que se orientan a R y solicitan acceso amplio al almacenamiento compartido ("Acceso a todos los

archivos") deben realizar y aprobar una revisión de acceso adecuada antes de su publicación. Las aplicaciones que pueden usar este permiso deben solicitar a los usuarios que habiliten el "Acceso a todos los archivos" en la configuración de "Acceso especial de apps". Para obtener más información sobre los requisitos de Android R, consulte este artículo de ayuda.

Abuso de Redes y Dispositivo

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

Las apps que se publiquen en Google Play deben cumplir con los requisitos de optimización del sistema Android predeterminado documentados en los Principales Lineamientos de Calidad para Apps en Google Play.

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

No permitimos código que introduzca ni explote vulnerabilidades de seguridad. Consulte el Programa de Mejora de la Seguridad de las Apps a fin de obtener información sobre los problemas de seguridad más recientes que se marcaron para los desarrolladores.

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que bloquean a otras o interfieren con ellas debido a la exhibición de anuncios
- Apps de trucos de juegos que afectan la experiencia de juego en otras apps
- Apps que facilitan o proporcionan instrucciones para piratear servicios, software, hardware o evadir las protecciones de seguridad
- Apps que acceden o usan un servicio o una API de forma tal que infrinjan las condiciones del servicio
- Apps que no son aptas para incluirse en la lista blanca y que intentan omitir la administración de energía del sistema
- Apps que facilitan servicios de proxy a terceros (solo deben hacerlo las apps que tengan esa finalidad como principal para el usuario)
- Apps o código de terceros (p. ej., SDK) que descargan código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play
- Apps que instalan otras apps en un dispositivo sin el consentimiento previo del usuario
- Apps que se vinculan a la distribución o instalación de software malicioso o facilitan estas prácticas

Comportamiento Engañoso

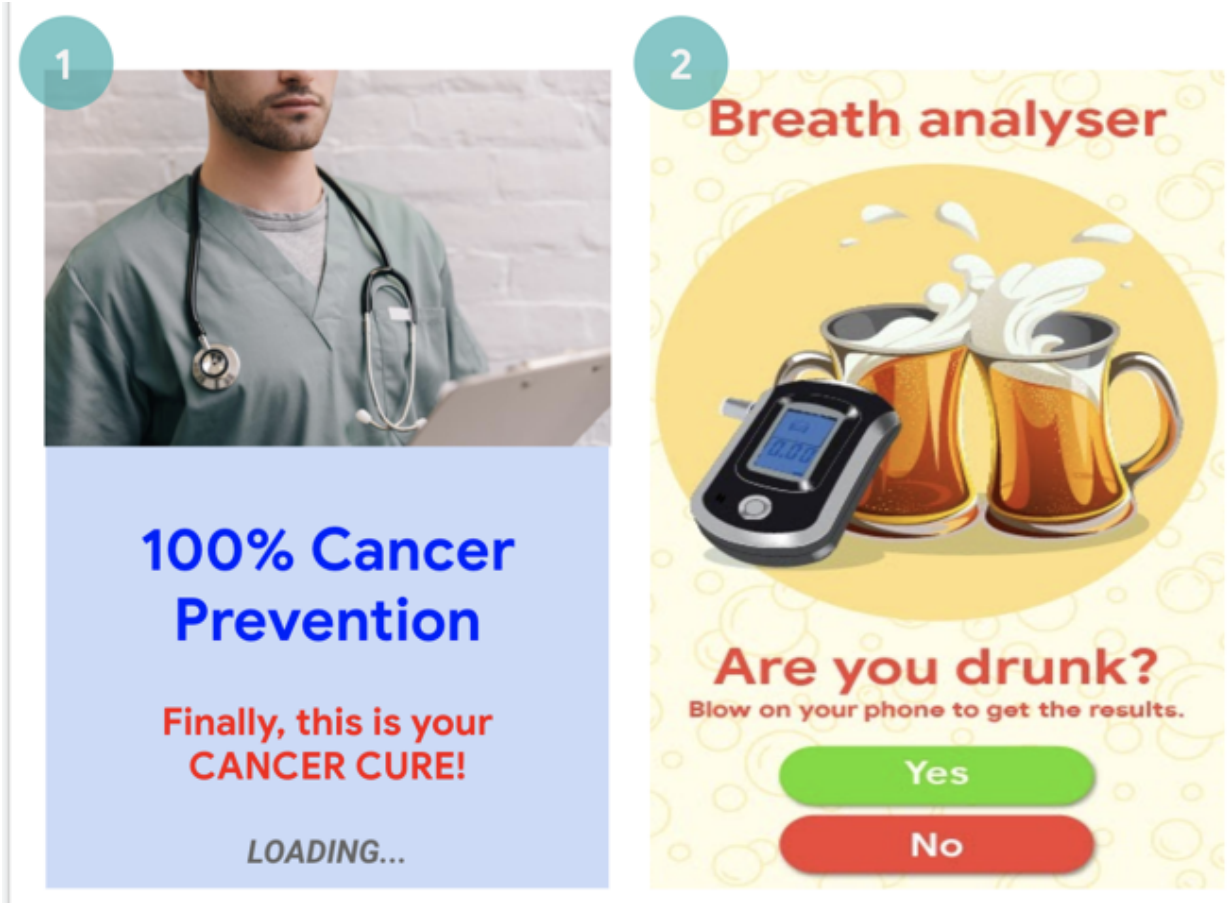
No permitimos apps que intenten engañar a los usuarios ni que den lugar a comportamientos deshonestos, lo que incluye, entre otras, aquellas diseñadas para ser funcionalmente imposibles. Las apps deben proporcionar divulgaciones, descripciones, imágenes y videos precisos sobre su funcionalidad en todas las partes de los metadatos. No deben intentar imitar las funciones ni las advertencias del sistema operativo ni de otras apps. Cualquier cambio en la configuración del dispositivo debe realizarse con el conocimiento y el consentimiento del usuario, y este debe poder revertirlo.

Afirmaciones Engañosas

No permitimos apps que contengan información o afirmaciones falsas o engañosas en la descripción, el título, el ícono o la captura de pantalla.

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que tergiversen o no describan de forma precisa y clara su funcionalidad:
  - Una app que afirma ser un juego de carreras en la descripción y en las capturas de pantalla, pero que en realidad es un juego de estrategia que usa la imagen de un automóvil
  - Una app que afirma ser un antivirus, pero solo tiene texto que explica cómo quitar virus.
- Nombres de apps o desarrolladores que tergiversen su estado o rendimiento actual en Google Play (p. ej., "Selección del editor", "App número 1", "Top ventas")
- Apps que incluyan funciones o contenido de medicina o relacionados con la salud que sean engañosos o potencialmente perjudiciales
- Apps que afirmen tener funciones que no se pueden implementar (p. ej., apps repelentes de insectos), incluso si se representan como bromas, falsificaciones, chistes, etcétera
- Apps que se categoricen de forma incorrecta, por ejemplo, que tengan una clasificación o una categoría de la app errónea
- Contenido engañoso comprobable que pueda interferir con los procesos de votación
- Apps que afirmen falsamente mantener algún vínculo con una entidad gubernamental o proporcionar o facilitar servicios gubernamentales para los cuales no están debidamente autorizadas
- Apps que afirmen falsamente ser la app oficial de una entidad establecida (no se permite el uso de títulos como "Oficial de Justin Bieber" sin los permisos o derechos necesarios)



(1) Esta aplicación presenta afirmaciones relacionadas con la salud o la medicina (cura del cáncer) que son engañosas.

(2) Esta aplicación afirma tener funciones que no se pueden implementar (usar el teléfono como alcoholímetro).

Cambios Engañosos en la Configuración del Dispositivo

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

Tampoco permitimos lo siguiente:

- Apps que modifiquen la configuración o las funciones con el consentimiento del usuario, pero que lo hagan de forma tal que no sea sencillo revertir la acción
- Apps o anuncios que modifiquen la configuración o las funciones del dispositivo como un servicio a terceros o con fines publicitarios
- Apps que engañen a los usuarios para que quiten o inhabiliten apps de terceros, o modifiquen la configuración o las funciones del dispositivo
- Apps que fomenten o incentiven a los usuarios a que quiten o inhabiliten apps de terceros o modifiquen la configuración o las funciones del dispositivo, a menos que sean parte de un servicio de seguridad comprobable

Prácticas que Fomentan un Comportamiento Fraudulento

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

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

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

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que imiten a otras apps o sitios web para engañar a los usuarios a fin de que divulguen información personal o de autenticación
- Apps que representen o muestren números de teléfono, contactos, direcciones o información de identificación personal no verificados o reales de personas o entidades que no hayan brindado su consentimiento para ello
- Apps con diferentes funciones principales según la ubicación geográfica del usuario, los parámetros del dispositivo y otros datos que dependen de los usuarios, cuando esas diferencias no se promocionen de forma destacada en la ficha de Play Store
- Apps que cambien significativamente entre versiones sin alertar al usuario (p. ej., en la sección "Novedades") y sin actualizar la ficha de Play Store
- Apps que intenten modificar u ocultar el comportamiento durante la revisión
- Apps con descargas facilitadas por la red de distribución de contenidos (CDN) que no guían al usuario ni indican el tamaño de la descarga antes de que se inicie el proceso

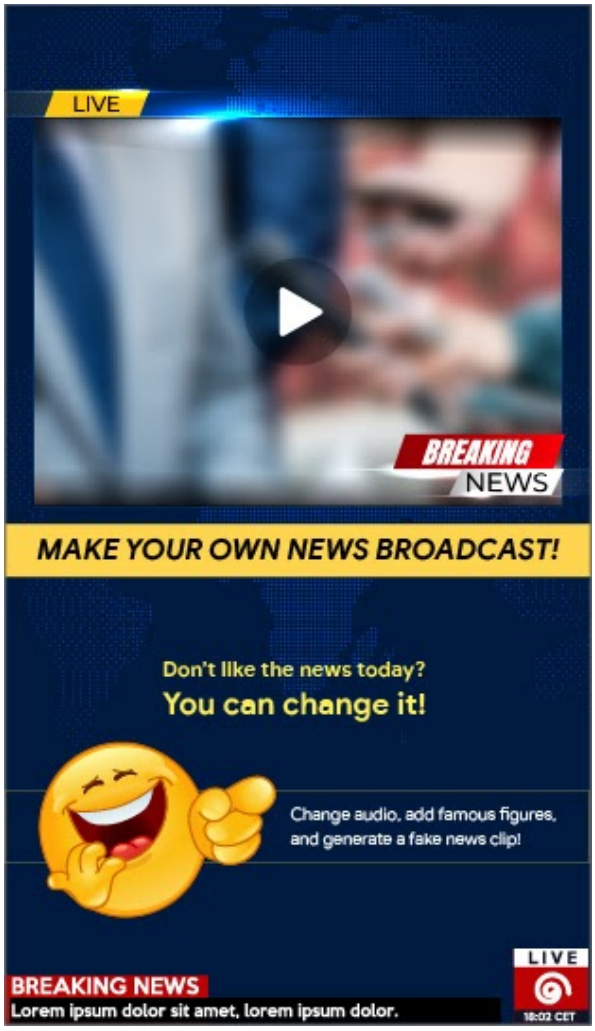
Manipulación de Contenido Multimedia

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

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

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que agreguen una figura pública a una protesta durante un evento políticamente sensible
- Apps que usen figuras públicas o contenido multimedia a partir de un evento sensible para publicitar sus capacidades de alteración del contenido multimedia dentro de la ficha de Play Store de una app
- Apps que alteren clips con contenido multimedia para imitar transmisiones de noticias



(1) Esta app permite modificar clips con contenido multimedia para imitar una transmisión de noticias y agregar figuras famosas o públicas al clip sin una marca de agua.

Tergiversación

No se permiten apps ni cuentas de desarrolladores que hagan lo siguiente:

- roben la identidad de otra organización o persona, o que oculten o tergiversen su objetivo principal o propiedad
- participen en actividades coordinadas para engañar a los usuarios (incluidas, sin limitaciones, las que ocultan o tergiversan su país de origen y dirigen su contenido a usuarios de otro país)
- coordinen con otras apps, sitios, desarrolladores u otras cuentas para ocultar o tergiversar la identidad de los desarrolladores o las apps y demás detalles importantes cuando el contenido se relacione con política, asuntos sociales o cuestiones de interés público

Software Malicioso

El Software Malicioso es cualquier código que pudiera poner en riesgo a un usuario, a sus datos o a un dispositivo. Se incluyen, entre otros, apps potencialmente dañinas (APD), objetos binarios o modificaciones de framework, que a su vez se organizan en categorías como troyanos, suplantación de identidad (phishing) y apps de software espía. Nota: Actualizamos esta lista de manera continua con nuevas categorías.

Software Malicioso

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

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

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

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

Una aplicación, un objeto binario o una modificación del framework pueden ser potencialmente dañinos y, por lo tanto, generar un comportamiento malicioso, aunque no estén diseñados para causar daño. Esto sucede porque es posible que las aplicaciones, los objetos binarios o las modificaciones del framework funcionen de manera diferente según diversas variables. Por lo tanto, lo que es perjudicial para un dispositivo Android podría no plantear ningún riesgo para otro dispositivo Android. Por ejemplo, un dispositivo que ejecuta la última versión de Android no se ve afectado por apps dañinas que usan API obsoletas para provocar un comportamiento malicioso, pero sí podría estar en riesgo un dispositivo que ejecuta una versión de Android mucho más antigua. Las apps, los objetos binarios y las modificaciones de framework se marcan como software malicioso o APD si claramente plantean un riesgo para todos los dispositivos y usuarios de Android.

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

Para obtener más información, visite Google Play Protect .

Puertas Traseras

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

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

Fraude de Facturación

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

Los fraudes de facturación de telefonía celular se dividen en Fraude de SMS, Fraude telefónico y Fraude de cargos telefónicos.

Fraude de SMS

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

Parte de este código, si bien técnicamente divulga el comportamiento de envío de SMS, incorpora comportamiento adicional que da lugar al Fraude de SMS. Algunos ejemplos incluyen ocultarle al usuario partes de un acuerdo de divulgación, dificultar su lectura y suprimir de forma condicional mensajes SMS del operador de telefonía móvil en los que se le informa al usuario sobre los cargos o se confirma una suscripción.

Fraude telefónico

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

Fraude de cargos telefónicos

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

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

Stalkerware

Se trata de código que recopila o transmite datos personales o sensibles del usuario desde un dispositivo sin el aviso o consentimiento adecuados, y no muestra una notificación persistente al respecto.

Las aplicaciones de stalkerware toman como blanco de sus ataques a los usuarios de los dispositivos, supervisan sus datos personales o sensibles y los transmiten o divulgan a terceros.

Las aplicaciones diseñadas y comercializadas exclusivamente para que los padres sigan a sus hijos o de administración empresarial son las únicas de vigilancia aceptables, siempre que satisfagan por completo los requisitos que se describen más abajo. Estas aplicaciones no se pueden usar para seguir a nadie más (por ejemplo, un cónyuge) incluso con el conocimiento y permiso de la persona, más allá de si se muestra una notificación persistente.

Las aplicaciones distribuidas en Play Store que no son de stalkerware y que supervisan el comportamiento de un usuario en un dispositivo deben satisfacer los siguientes requisitos mínimos:

- No deben presentarse como una solución de espionaje ni vigilancia secreta.
- Las aplicaciones no deben ocultar ni encubrir el seguimiento del comportamiento, ni intentar engañar a los usuarios sobre esa función.
- Las aplicaciones deben presentarse ante los usuarios con una notificación persistente en todo momento mientras estén en ejecución y deben tener un ícono único que las identifique claramente.
- Las aplicaciones y fichas que se muestran en Google Play no deben proporcionar ningún medio para activar o acceder a funcionalidades que infrinjan estos términos y condiciones, como vínculos a archivos APK alojados fuera de Google Play que no cumplan con dichos términos.
- La responsabilidad de determinar la legalidad de la app en el mercado de destino recae exclusivamente sobre usted. Se quitarán las aplicaciones que se consideren ilegales en los lugares donde estén publicadas.

Denegación del Servicio (DoS)

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

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

Apps de Descarga Hostil

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

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

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

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

- No activan descargas sin la interacción del usuario.
- Todas las descargas de APD son iniciadas por un usuario que prestó su consentimiento.

Amenaza No Relacionada con Android

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

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

Suplantación de Identidad (Phishing)

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

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

Abuso de Privilegios Elevados

Se trata de código que compromete la integridad del sistema, ya que trasciende la zona de pruebas de la app, obtiene privilegios elevados o cambia o inhabilita el acceso a funciones básicas relacionadas con la seguridad.

Los siguientes son algunos ejemplos:

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

Las apps de elevación de privilegios que otorgan a los dispositivos derechos de administrador sin que el usuario conceda el permiso se clasifican como apps de rooting, a apps que modifican los dispositivos para obtener permisos de administrador.

Ransomware

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

El ransomware puede encriptar los datos dentro del dispositivo y exige que se efectúe un pago para desencriptarlos, o bien aprovecha las funciones administrativas del dispositivo de modo que un usuario común no pueda quitar la restricción. Los siguientes son algunos ejemplos:

- Bloquear a un usuario para que no pueda acceder al dispositivo y exigirle dinero para restablecer su control
- Encriptar datos en el dispositivo y exigir un pago, ostensiblemente, para desencriptarlos
- Implementar las funciones del Administrador de políticas del dispositivo y bloquear la acción del usuario para quitar la restricción

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

Modificación de Dispositivos para Obtener Permisos de Administrador (Rooting)

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

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

Las apps que modifican el dispositivo para obtener permisos de administrador con fines maliciosos no le notifican al usuario sobre el proceso, o bien lo hacen con anticipación, pero además ejecutan otras acciones que se aplican a otras categorías de APD.

Spam

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

Software Espía

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

Por ejemplo, la transmisión de la siguiente información sin divulgación previa o de manera inesperada para el usuario es suficiente para que la app se considere como software espía:

- Lista de contactos
- Fotos y otros archivos que se guardan en la tarjeta SD, o que no pertenecen a la app
- Contenido del correo electrónico del usuario
- Registro de llamadas
- Registro de SMS
- Historial web o favoritos del navegador predeterminado
- Información de los directorios de /datos/ de otras apps

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

Troyano

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

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

Nota sobre Apps Poco Comunes

Las apps nuevas o exóticas podrían clasificarse como poco comunes si Google Play Protect no tiene suficiente información para considerarlas seguras. Esto no significa que la app sea necesariamente dañina, pero tampoco

se puede considerar segura sin un análisis más profundo.

Nota sobre la Categoría de Puerta Trasera

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

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

Software No Deseado para Dispositivos Móviles

Esta política complementa la Política de Software No Deseado de Google y describe los principios del ecosistema de Android y Google Play Store. Todo software que infringe estos principios se considera potencialmente perjudicial para la experiencia de los usuarios, y tomaremos medidas para protegerlos.

Software No Deseado de Dispositivos Móviles

En Google, creemos que, si nos centramos en el usuario, el resto viene solo. En nuestros Principios de Software y en la Política de Software No Deseado, proporcionamos recomendaciones generales para el software que ofrece una excelente experiencia del usuario. Esta política complementa la Política de Software No Deseado de Google y describe los principios del ecosistema de Android y Google Play Store. Todo software que infringe estos principios se considera potencialmente perjudicial para la experiencia de los usuarios, y tomaremos medidas para protegerlos.

Como se mencionó en la Política de Software No Deseado, descubrimos que la mayoría de este tipo de software muestra una o más de las mismas características básicas:

- Es engañoso, ya que promete una propuesta de valor que no cumple.
- Intenta engañar a los usuarios para que lo instalen, o viene incorporado en la instalación de otro programa.
- No informa al usuario acerca de todas sus funciones principales e importantes.
- Afecta al sistema del usuario de forma inesperada.
- Recopila o transmite información privada sin que los usuarios lo sepan.
- Recopila o transmite información privada sin un manejo seguro (p. ej., no transmite mediante HTTPS).
- Está incluido en otro software y su presencia no se divulga.

En los dispositivos móviles, el software es código en forma de una aplicación, un objeto binario, una modificación del framework, etc. A fin de evitar la existencia de software dañino para el ecosistema de software o que interrumpa la experiencia del usuario, tomaremos medidas con respecto al código que no cumpla con esos principios.

A continuación, nos basamos en la Política de Software No Deseado para extender su aplicabilidad al software para dispositivos móviles. Al igual que con esa política, seguiremos definiendo mejor esta Política de Software no Deseado para Dispositivos Móviles a fin de abordar nuevos tipos de abuso.

Comportamiento transparente y divulgaciones claras

Todo el código debe cumplir con las promesas hechas al usuario. Las aplicaciones deben proporcionar toda la funcionalidad comunicada Las apps no deben confundir a los usuarios.

- Las aplicaciones deben ser claras acerca de su funcionalidad y objetivos.
- Explique de manera explícita y clara al usuario qué cambios realizará la aplicación en el sistema. Permita que los usuarios revisen y aprueben todos los cambios y las opciones de instalación importantes.
- El software no debe tergiversar el estado del dispositivo del usuario, por ejemplo, afirmando que el sistema se encuentra en un estado crítico de seguridad o está infectado con virus.
- No utilice actividades no válidas diseñadas para aumentar el tráfico de anuncios o las conversiones.
- No permitimos aplicaciones que confundan a los usuarios mediante el robo de identidad de otra persona (p. ej., otro desarrollador, empresa o entidad). No insinúe que su aplicación está relacionada con otra persona o autorizada por ella.

Ejemplos de incumplimiento:

- Fraude publicitario
- Robo de identidad

Protege los datos del usuario

Sé claro y transparente sobre el acceso, el uso, la recopilación y el uso compartido de datos personales y sensibles del usuario. Los usos de los datos del usuario deben cumplir con todas las políticas de datos del usuario pertinentes, cuando corresponda, y tomar todas las precauciones necesarias para protegerlos.

- Permita que los usuarios acepten que se recopilen sus datos antes de comenzar a recopilarlos y enviarlos desde el dispositivo, incluidos los datos sobre cuentas de terceros, correo electrónico, número de teléfono, aplicaciones instaladas, archivos, ubicación y cualquier otro dato personal y confidencial que el usuario no esperaría que se recopilara.
- Los datos personales y sensibles del usuario que se recopilen deben manejarse de forma segura, lo que incluye transmitirlos mediante criptografía moderna (por ejemplo, por HTTPS).
- El software, incluidas las aplicaciones para dispositivos móviles, solo debe transmitir datos personales y sensibles de los usuarios a los servidores que estén relacionados con la funcionalidad de la app.

Ejemplos de incumplimiento:

- Recopilación de datos (consulta Software espía)
- Abuso de permisos restringidos

Ejemplo de Políticas de Datos del Usuario:

- *Política de Datos del Usuario de Google Play*
- *Política de Datos del Usuario de los Requisitos de GMS*
- *Política de Datos del Usuario del Servicio de las API de Google*

Cuida la experiencia en los dispositivos móviles

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

- No muestre anuncios a los usuarios de formas inesperadas, entre las que se incluyen afectar o interferir con la usabilidad de las funciones del dispositivo, o mostrarlos fuera del entorno de la aplicación que los activa y que no se puedan descartar fácilmente, y con la atribución y el consentimiento adecuados.
- Las aplicaciones no deben interferir con otras aplicaciones ni con la usabilidad del dispositivo.

- La desinstalación, si corresponde, debe ser clara.
- El software para dispositivos móviles no debe intentar imitar los mensajes del SO del dispositivo ni de otras aplicaciones. No suprima las alertas al usuario desde otras aplicaciones ni desde el sistema operativo, en especial aquellas que informan al usuario sobre los cambios en su SO.

Ejemplos de incumplimiento:

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

Fraude publicitario

El fraude publicitario está estrictamente prohibido. Las interacciones con anuncios generadas con el fin de engañar a una red de publicidad para que crea que el tráfico es de interés auténtico del usuario es un fraude publicitario, que es una forma de tráfico no válido. El fraude publicitario puede ser el resultado de que los desarrolladores implementen anuncios de maneras no permitidas, como mostrar anuncios ocultos, hacer clic automáticamente en los anuncios, alterar o modificar la información, o aprovechar de alguna otra manera las acciones no manuales (arañas, bots, etc.) o la actividad humana diseñada 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 generan una pérdida de confianza a largo plazo en el ecosistema de anuncios para dispositivos móviles.

Los siguientes son ejemplos comunes de incumplimiento:

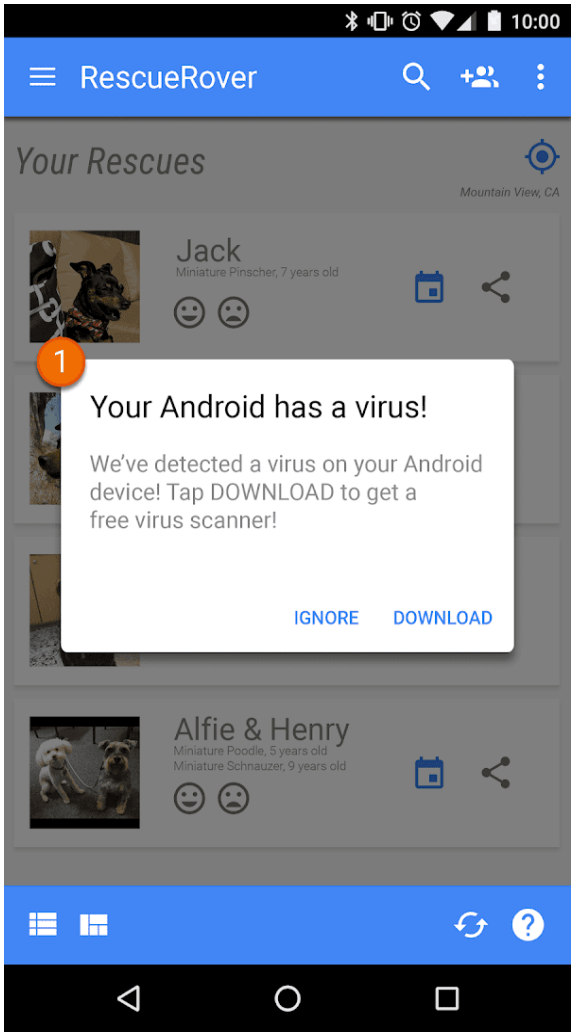
- Una app que procesa anuncios que no son visibles para el usuario
- Una app que genera clics automáticamente en anuncios sin la intención del usuario o que produce tráfico de red equivalente para otorgar créditos de clics de manera fraudulenta
- Una app que envía clics de atribución de instalación falsos para recibir pagos por instalaciones que no se originaron en la red del remitente
- Una app que muestra anuncios cuando el usuario no está en la interfaz de la app
- Declaraciones falsas del inventario de anuncios de una app, p. ej., una app que comunica a las redes de publicidad que se ejecuta en un dispositivo iOS cuando se está ejecutando en un dispositivo Android o una app que tergiversa el nombre del paquete que se está monetizando

Uso no autorizado o imitación de las funciones del sistema

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

Los siguientes son ejemplos comunes de incumplimiento:

- Apps o anuncios que se envían por medio de una notificación o alerta del sistema:



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

Para ver ejemplos adicionales que incluyan anuncios, consulte la política de Anuncios.

Robo de identidad

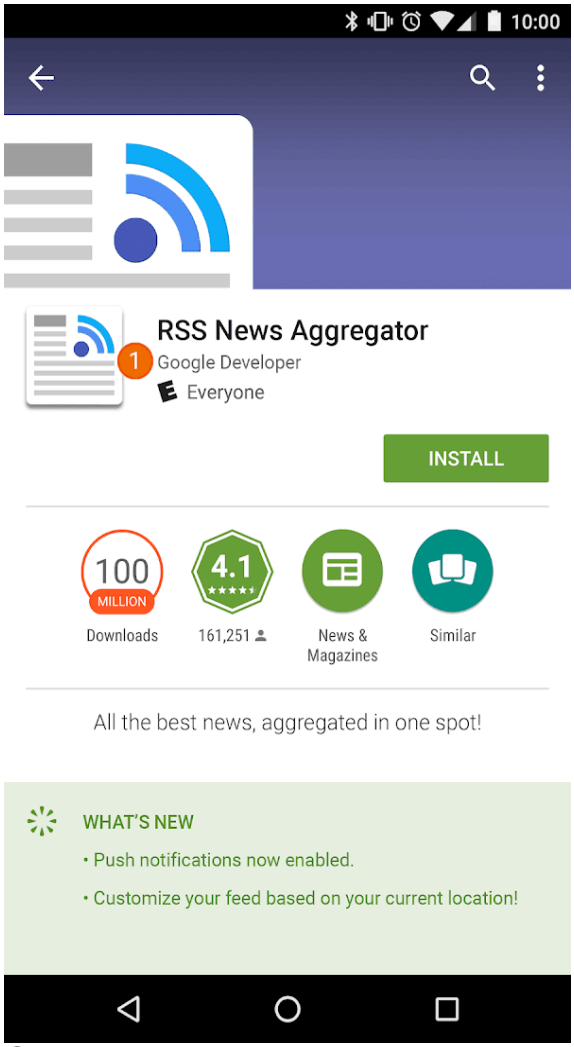
Cuando los desarrolladores roban la identidad de otras personas o sus apps, engañan a los usuarios y perjudican a la comunidad de desarrolladores. Prohibimos las apps que confunden a los usuarios mediante el robo de la identidad de otra persona.

Robo de identidad

No permitimos apps que confundan a los usuarios mediante el robo de la identidad de otra persona (p. ej., otro desarrollador, empresa o entidad) o de otra app. No insinúe que su app está relacionada o autorizada por otra persona. Tenga cuidado de no usar íconos, descripciones, títulos o elementos integrados en la app que puedan engañar a los usuarios sobre la relación de su app con otra persona o con otra app.

Los siguientes son ejemplos comunes de incumplimiento:

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



① El nombre del desarrollador de esta aplicación sugiere una relación oficial con Google, aunque esta no exista.

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

Monetización y anuncios

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

Pagos

1. Los desarrolladores que cobran por apps y descargas de Google Play deben usar el sistema de facturación de Google Play como forma de pago.
2. Las apps que se distribuyen en Play deben usar el sistema de facturación de Google Play como forma de pago si requieren o aceptan pagos para acceder a funciones o servicios, lo que incluye cualquier funcionalidad de la app, contenido digital o bienes.

    a. Entre los ejemplos de funciones o servicios de la app que requieren el uso del sistema de facturación de Google Play, se incluyen las compras directas desde la aplicación para adquirir lo siguiente:
        - artículos (como monedas virtuales, vidas adicionales, tiempo de juego adicional, elementos complementarios, personajes y avatares)
        - servicios de suscripción (como entrenamiento, juegos, citas, educación, música, videos y otros servicios de suscripción de contenido)
        - funcionalidad o contenido de la app (como una versión sin anuncios de una app o funciones nuevas que no estén disponibles en la versión gratuita)
        - software y servicios en la nube (como servicios de almacenamiento de datos, software de productividad empresarial y software de administración financiera)

    b. El sistema de facturación de Google Play no debe utilizarse en los siguientes casos:
        - el pago tiene principalmente uno de estos fines:

          Nota: En algunos mercados, ofrecemos Google Pay para apps que venden bienes físicos o servicios. Si quieres obtener más información, visita la página de Google Pay para desarrolladores.

            - la compra o el alquiler de bienes físicos (como comestibles, ropa, artículos para el hogar, artículos electrónicos)
            - la compra de servicios físicos (como servicios de transporte, servicios de limpieza, pasajes de avión, membresías de gimnasio, envío de comida, entradas para eventos en vivo)
            - el funcionamiento como remesa con respecto a una factura de tarjeta de crédito o de servicios públicos (como servicios de cable y telecomunicaciones)
        - pagos que incluyen transacciones entre pares, subastas en línea y donaciones exentas de impuestos
        - pagos por contenido o servicios que facilitan los juegos de apuestas en línea, como se describe en la sección Apps de juegos de apuestas de la política de Juegos, Concursos y Juegos de Apuestas con Dinero Real
        - pagos en relación a cualquier categoría de producto que se considere inaceptable según las Políticas de Contenido del Centro de Pago de Google

3. Las apps que no sean las que se describen en 2(b) no pueden dirigir a los usuarios a una forma de pago que no sea el sistema de facturación de Google Play. Esta restricción incluye, entre otras, la posibilidad de dirigir a los usuarios a otras formas de pago a través de lo siguiente:

    - Una ficha de la app en Google Play
    - Promociones dentro de la app relacionadas con el contenido que se puede comprar
    - Vistas web, botones, vínculos, mensajes, anuncios y otros llamados a la acción en la app
    - Flujos de la interfaz de usuario en la app, incluidos los flujos de creación de cuentas o de registro, que dirigen a los usuarios a una forma de pago que no es el sistema de facturación de Google Play como parte de esos flujos

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

5. Los desarrolladores deben informar a los usuarios de manera clara y precisa sobre las condiciones y los precios de sus apps o sobre cualquier función o suscripción integrada que se pueda comprar. Los precios integrados en la app deben coincidir con los que se muestran en la interfaz de Facturación Play para el usuario. Si la descripción de tu producto en Google Play hace referencia a funciones integradas en la app a las que se aplica un cargo específico o adicional, la ficha de la app debe notificar claramente a los usuarios que se requiere un pago para acceder a esas funciones.
6. Las apps y los juegos que ofrecen mecanismos para recibir elementos virtuales aleatorios de una compra, incluidos, entre otros, "cajas de botín", deben divulgar claramente las probabilidades de recibir esos elementos por adelantado y cerca del momento de la compra.

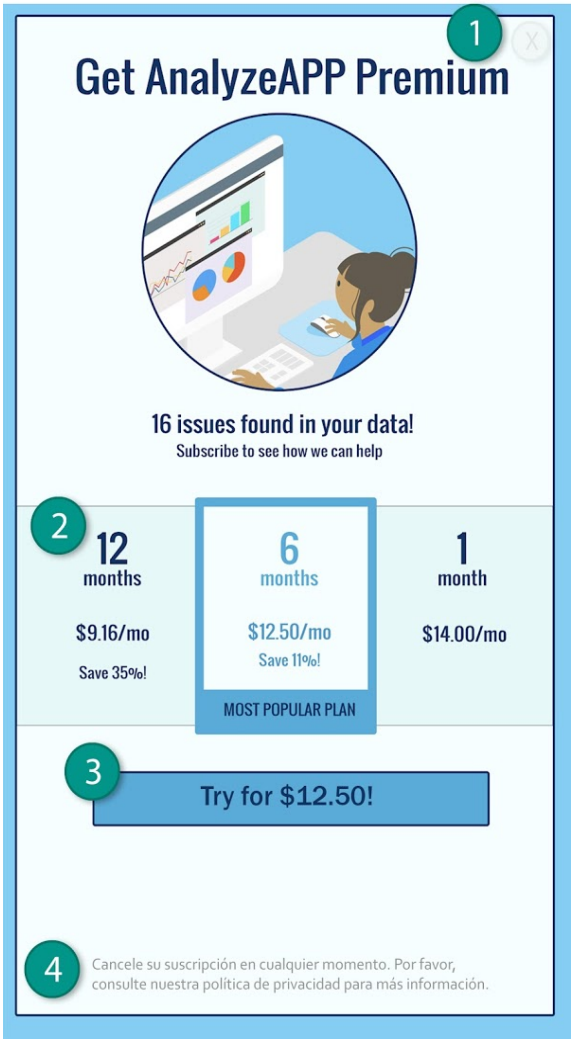
Suscripciones

Como desarrollador, no debe engañar a los usuarios acerca de ningún servicio de suscripción o contenido que ofrezca dentro de su app. Es fundamental que, en promociones dentro de la app o pantallas de presentación, la comunicación sea clara.

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

Los siguientes son ejemplos comunes de incumplimiento:

- Suscripciones mensuales que no informan a los usuarios que se les renovará el plan de forma automática y se les cobrará cada mes
- Suscripciones anuales que muestran sus precios de forma más prominente en términos del costo mensual
- Precios y condiciones de las suscripciones que no están totalmente localizados
- Promociones integradas en la aplicación que no demuestran con claridad que el usuario puede acceder al contenido sin una suscripción (cuando esté disponible)
- Nombres de SKU que no representan con precisión la naturaleza de la suscripción, como la etiqueta "Prueba gratuita" en una suscripción que tiene un cargo automático recurrente



① El botón para descartar no está claramente visible, por lo que es posible que los usuarios no comprendan que pueden acceder a la función sin aceptar la oferta de suscripción.

② La oferta solo muestra los precios en términos del costo mensual, por lo que es posible que los usuarios no comprendan que se les cobrarán seis meses en el momento de la suscripción.

③ La oferta solo muestra el precio de lanzamiento, por lo que es posible que los usuarios no comprendan cuánto se les cobrará automáticamente cuando finalice el período de lanzamiento.

④ La oferta se debe localizar al mismo idioma que los Términos y Condiciones, de manera que los usuarios puedan comprender la información completa.

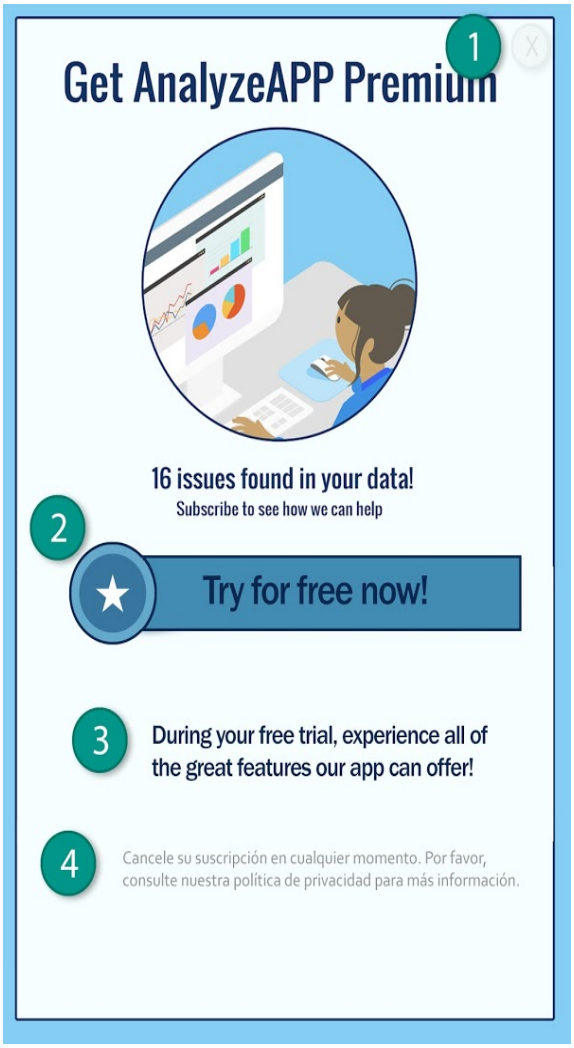
Pruebas gratuitas y ofertas de lanzamiento

Antes de que se inscriba un usuario en su suscripción: Debe describir de manera clara y precisa las condiciones de su oferta, incluidos el precio, la duración y la descripción de los servicios o el contenido a los que se dará acceso. Asegúrese de que los usuarios sepan cómo y cuándo la prueba gratuita se convierte en una suscripción pagada, el costo de esa suscripción y la posibilidad de cancelar si el usuario no desea realizar la conversión.

Los siguientes son ejemplos comunes de incumplimiento:

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

- Ofertas que no explican de manera clara que se inscribirá de forma automática al usuario en una suscripción paga al final del período de oferta
- Ofertas que no demuestran de forma clara que los usuarios pueden acceder al contenido sin una prueba (cuando está disponible esa opción)
- Precios y condiciones de ofertas que no están completamente localizados



① El botón para descartar no está claramente visible, por lo que es posible que los usuarios no comprendan que pueden acceder a esta función sin registrarse para la prueba gratuita.

② La oferta hace hincapié en la prueba gratuita, por lo que es posible que los usuarios no comprendan que se les cobrará automáticamente un cargo al finalizar esa prueba.

③ La oferta no indica un período de prueba, por lo que es posible que los usuarios no comprendan cuánto tiempo durará el acceso gratuito a la suscripción.

④ La oferta se debe localizar al mismo idioma que los Términos y Condiciones, de manera que los usuarios puedan comprender la información completa.

Administración y cancelación de suscripciones

Como desarrollador, debe asegurarse de que su app divulgue de forma clara cómo los usuarios pueden administrar o cancelar su suscripción.

Es su responsabilidad notificarlos sobre los cambios implementados en las políticas de suscripción, la cancelación y el reembolso, y garantizar que las políticas cumplan con la legislación vigente.

Anuncios

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

Uso de datos de ubicación para los anuncios

Las apps que extienden el uso de datos de ubicación del dispositivo basados en permisos para publicar anuncios están sujetas a la Política de Información Personal y Sensible y también deben cumplir con los siguientes requisitos:

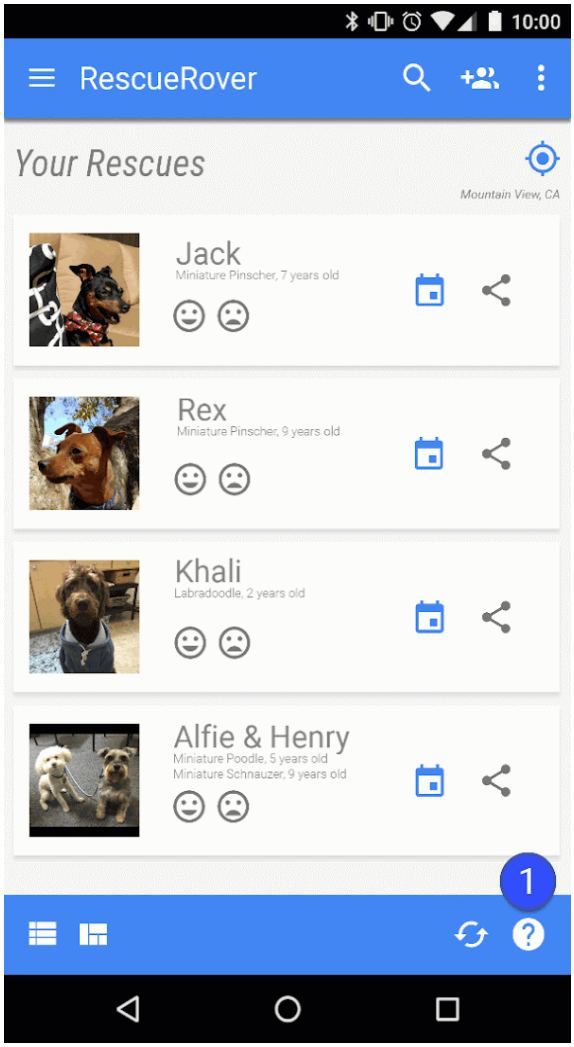
- El uso o la recopilación con fines publicitarios de los datos de ubicación del dispositivo basados en permisos deben estar claros para el usuario y documentados en la Política de Privacidad obligatoria de la app, incluidos los vínculos a cualquier Política de Privacidad de redes publicitarias relevantes que aborde el uso de datos de ubicación.
- De acuerdo con los requisitos de Permisos de Ubicación, solo pueden solicitarse permisos de ubicación para implementar servicios o funciones actuales dentro de su app y no pueden solicitarse permisos de ubicación del dispositivo exclusivamente para el uso de anuncios.

Anuncios engañosos

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

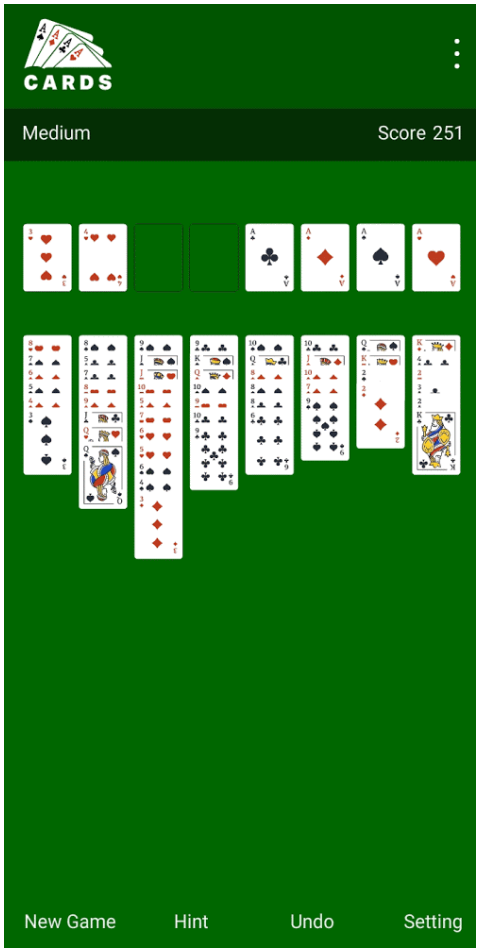
Los siguientes son ejemplos comunes de incumplimiento:

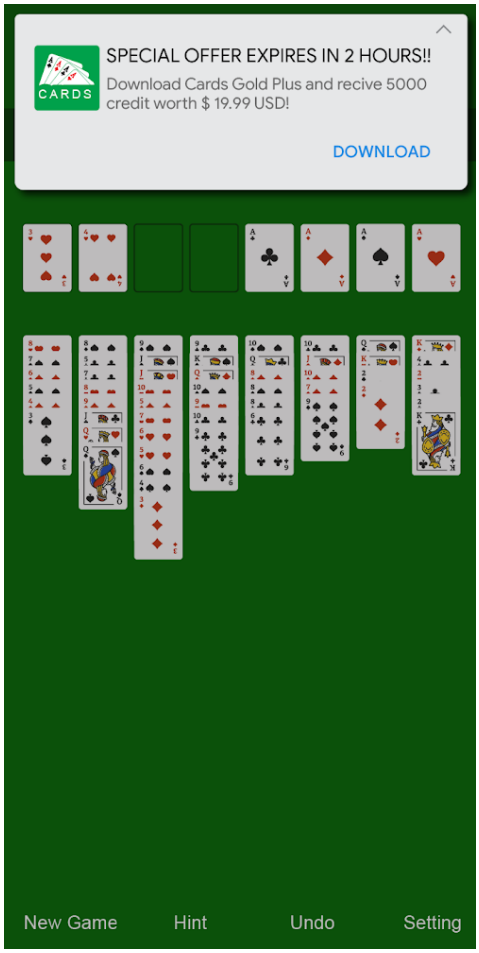
- Anuncios que imitan la IU de una aplicación:



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

- Anuncios que imitan una notificación del sistema:



- 

En los ejemplos anteriores, se muestra la forma en la que los anuncios imitan las notificaciones de varios sistemas.

Monetización de la pantalla bloqueada

A menos que funcionen exclusivamente como pantalla de bloqueo, las apps no pueden incluir anuncios o funciones que moneticen la pantalla de bloqueo de un dispositivo.

Anuncios invasivos

Los anuncios invasivos son aquellos que se muestran a los usuarios de formas inesperadas, que pueden generar clics involuntarios o que afectan la usabilidad de las funciones del dispositivo.

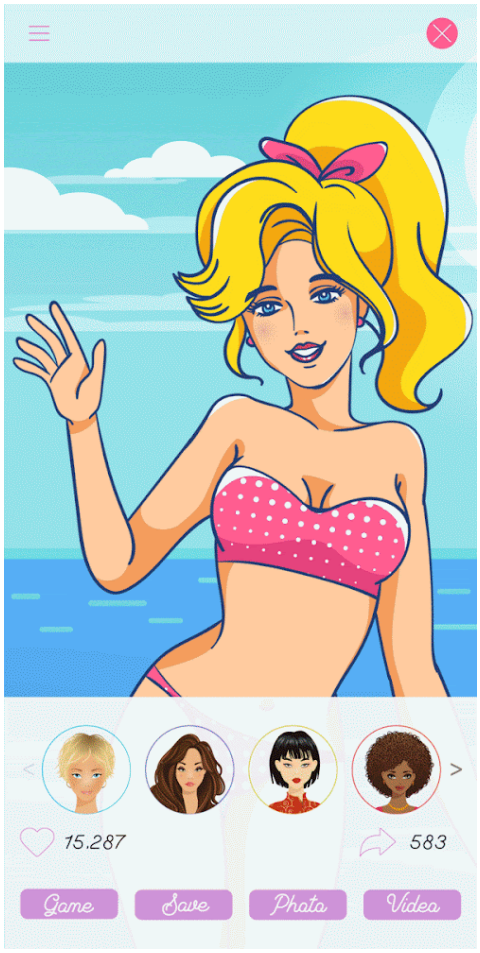
Su app no puede obligar al usuario a hacer clic en un anuncio ni a enviar información personal con fines publicitarios antes de que pueda usarla por completo. Los anuncios intersticiales solo se pueden mostrar dentro de la app que los publica. Si su app muestra anuncios intersticiales, o bien otros anuncios que interfieren con el uso normal, estos deben poder descartarse fácilmente sin penalización.

Los siguientes son ejemplos comunes de incumplimiento:

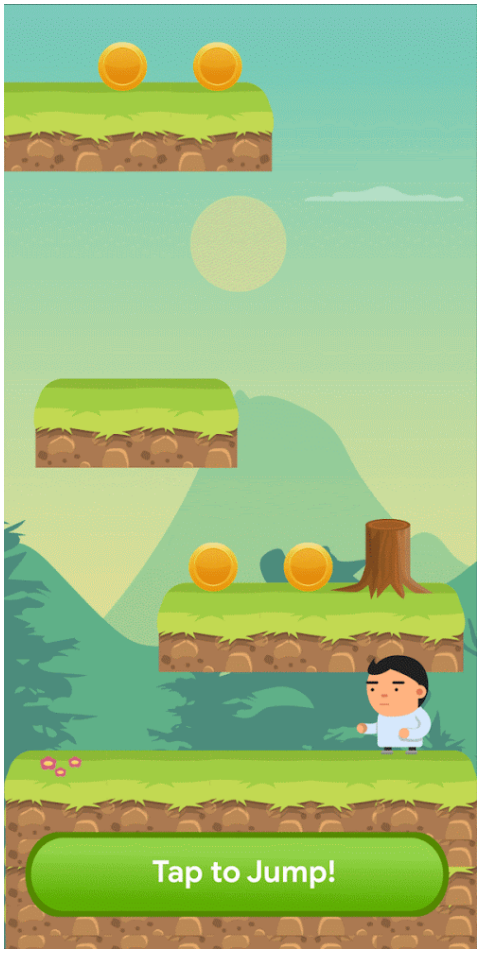
- Anuncios que ocupan toda la pantalla o interfieren con el uso normal y no proporcionan un medio claro para descartar el anuncio:

① Este anuncio no tiene un botón para descartar.

- Anuncios que obligan al usuario a hacer clic con un botón de descarte falso o que hacen que los anuncios aparezcan repentinamente en áreas de la app donde el usuario suele presionar otra función.



Un anuncio que utiliza un botón para descartarlo falso



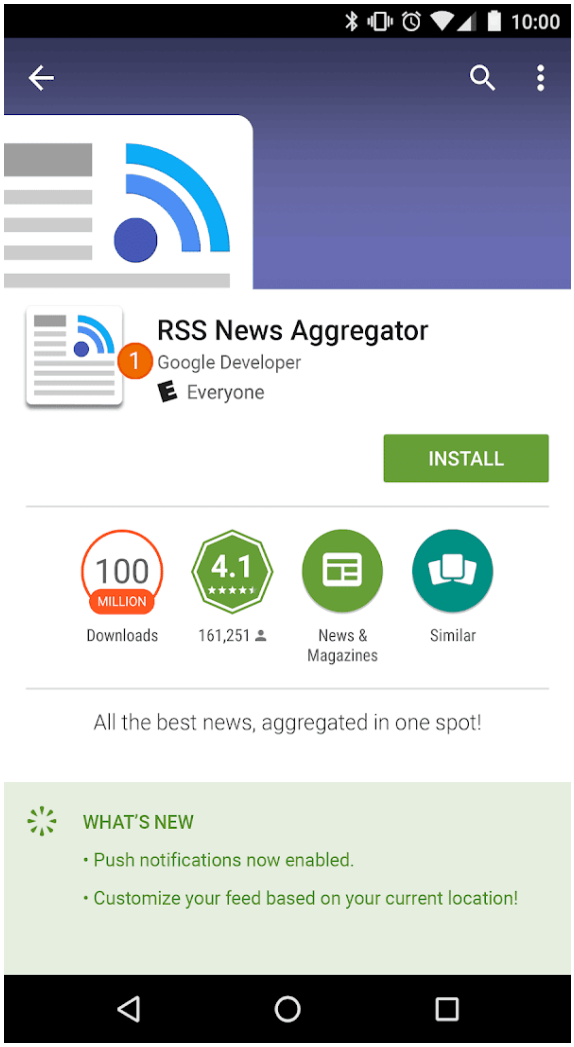
Un anuncio que aparece de repente en un área donde el usuario está acostumbrado a presionar para obtener funciones en la app

Interferencia con apps, anuncios de terceros y la funcionalidad del dispositivo

Los anuncios asociados a su app no deben interferir con otras apps, anuncios ni la operación del dispositivo, incluidos los botones y puertos del dispositivo o el sistema. Entre estos aspectos, se incluyen las superposiciones, las funciones complementarias y los bloques de anuncios con widgets. Los anuncios solo deben mostrarse dentro de la app que los ofrece.

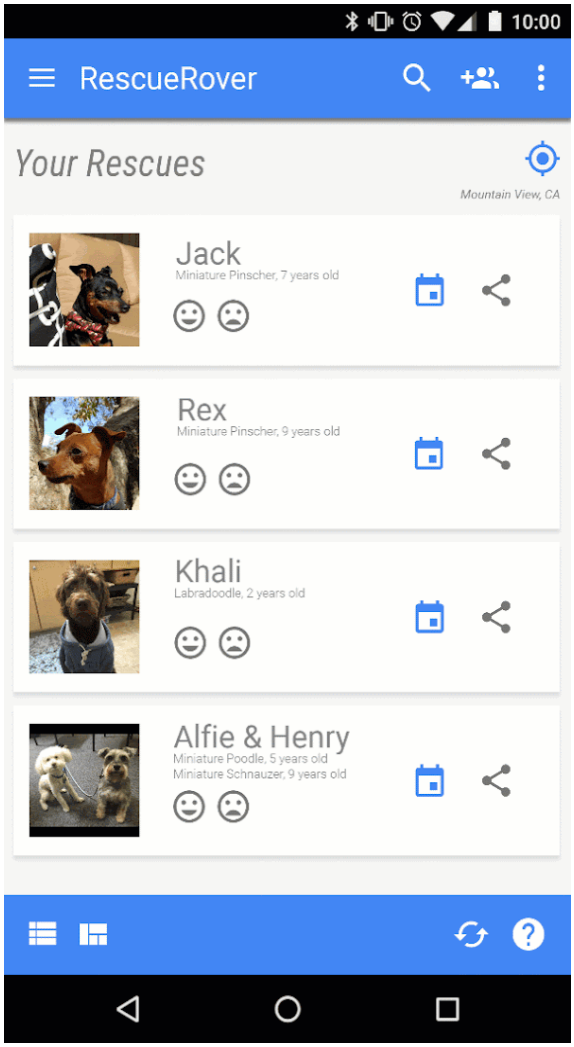
Los siguientes son ejemplos comunes de incumplimiento:

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



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

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

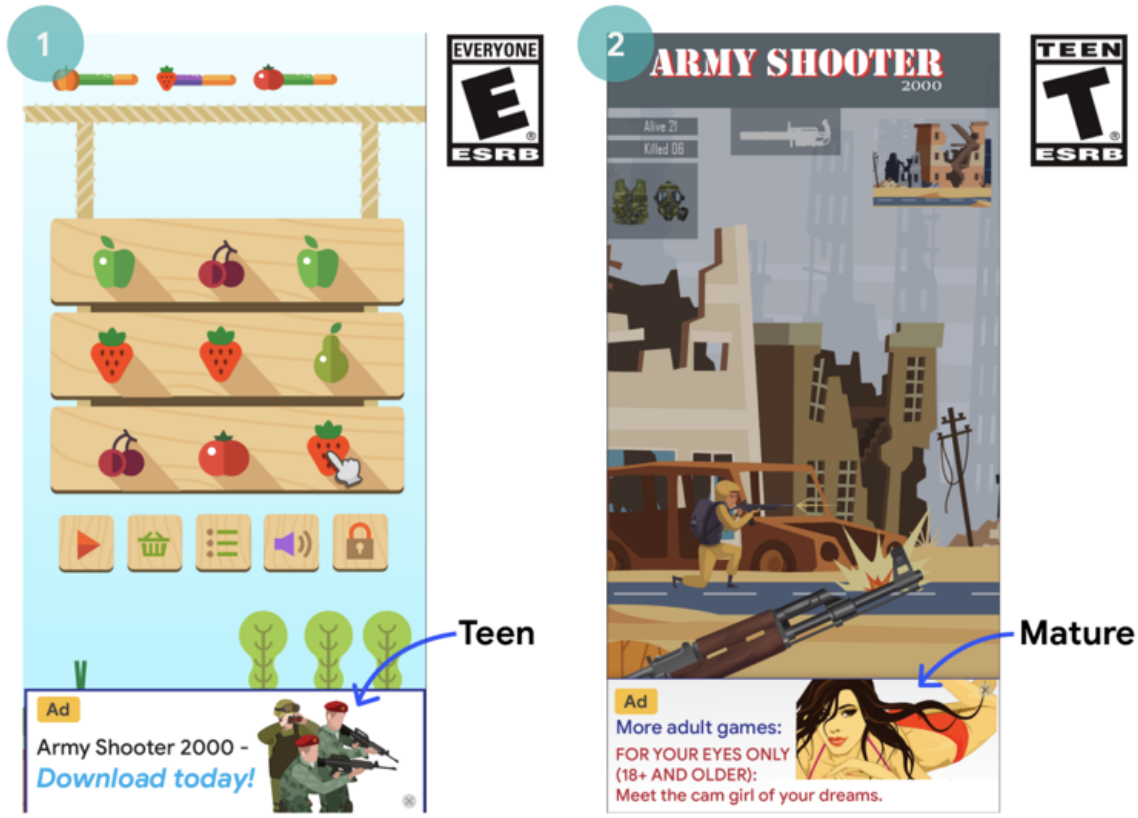


Descripción: El usuario intenta salir de la aplicación y navegar a la pantalla principal, pero un anuncio interrumpe el flujo esperado.

Anuncios inapropiados

Los anuncios que muestre la app deben ser adecuados para el público al que está orientada, incluso si el contenido cumple con nuestras políticas.

El siguiente es un ejemplo común de incumplimiento:



① Este anuncio es inapropiado (es para adolescentes) para el público objetivo de la app (que es para mayores de 7).
② Este anuncio es inapropiado (es para adultos) para el público objetivo de la app (que es para mayores de 12).

Uso del ID de publicidad de Android

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

- **Uso**. El identificador de publicidad de Android solo debe usarse para publicidad y estadísticas de usuarios. El estado de la configuración para inhabilitar la publicidad basada en intereses o cancelar la personalización de anuncios se debe verificar cada vez que se ingrese el ID.
- **Asociación con información de identificación personal y otros identificadores**
  - Uso publicitario: El identificador de publicidad no puede estar conectado a identificadores de dispositivos persistentes (por ejemplo, SSAID, dirección MAC, IMEI, etc.) para ningún fin publicitario. El identificador de publicidad solo puede estar conectado a información de identificación personal con el consentimiento explícito del usuario.
  - Uso de estadísticas: El identificador de publicidad solo puede estar conectado a información de identificación personal o estar asociado con cualquier identificador de dispositivo persistente (por ejemplo, SSAID, dirección MAC, IMEI, etc.) con el consentimiento explícito del usuario.
- **Respeto de las selecciones de los usuarios**. Si se realiza el restablecimiento, un nuevo identificador de publicidad no debe estar conectado a uno anterior ni a datos derivados de un identificador de publicidad previo sin el consentimiento explícito del usuario. Además, debe respetar la configuración de la opción de "inhabilitar la publicidad basada en intereses" o "Cancelar personalización de anuncios" que haya seleccionado un usuario. Si un usuario habilitó esta configuración, no podrá usar el identificador de publicidad para crear perfiles de usuario con fines publicitarios ni para orientarse a los usuarios con anuncios personalizados. Las actividades permitidas incluyen la publicidad contextual, la limitación de frecuencia, el seguimiento de conversiones, la información y seguridad, y la detección de fraudes.

- **Transparencia para los usuarios**. La recopilación y el uso del identificador de publicidad, y el compromiso con estas condiciones deben darse a conocer a los usuarios en un aviso de privacidad legalmente adecuado. Para obtener información sobre nuestros estándares de privacidad, revise nuestra política de Datos del Usuario.
- **Cumplimiento de las Condiciones de uso**. El identificador de publicidad solo puede utilizarse de acuerdo con estas condiciones. Lo mismo se espera de cualquier tercero con quien se comparta durante el transcurso del negocio. Todas las apps que se suban a Google Play o se publiquen en esa plataforma deben usar el ID de publicidad (cuando esté disponible en el dispositivo) en lugar de cualquier otro identificador de dispositivo para fines publicitarios.

Programa de anuncios para familias

Si publica anuncios en su app y esta se orienta únicamente a niños según se describe en la Política de Familias, debe usar SDK de anuncios que cumplan con la autocertificación relacionada con las políticas de Google Play, incluso con los requisitos de certificación de SDK de anuncios que se incluyen a continuación. Si el público al que se orienta tu app incluye tanto niños como usuarios mayores, debe implementar medidas para filtrar por edad y asegurarse de que los anuncios que se muestren a los niños provengan exclusivamente de uno de los SDK de anuncios autocertificados. Las apps que participan en el programa Designed for Families solo pueden usar SDK de anuncios autocertificados.

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

- Publicidad interna en la que use SDK para administrar la promoción cruzada de tus apps o productos y otros medios de su propiedad
- Participación en ofertas directas con anunciantes y uso de SDK para la administración de inventario

Requisitos de certificación de SDK de anuncios

- Defina el significado de comportamientos y contenido de anuncio reprochables, y prohíbalos en las condiciones o políticas de los SDK de anuncios. Las definiciones deben cumplir con las Políticas del Programa para Desarrolladores de Play.
- Cree un método para calificar sus creatividades de anuncios según los grupos adecuados para la edad. Los grupos adecuados para la edad deben incluir, como mínimo, los grupos "Apto para todo público" y "Mayores de edad". La metodología de clasificación debe alinearse con la metodología que proporciona Google a los SDK una vez que los desarrolladores completan el formulario de interés que se incluye a continuación.
- Permite que los publicadores soliciten contenido dirigido a niños para la publicación de anuncios por solicitud o por app. Dicho contenido debe cumplir con las leyes y normas aplicables, como la Ley de Protección de la Privacidad de Menores en Internet (COPPA) de los EE.UU. y el Reglamento General de Protección de Datos (GDPR) de la UE. Google Play requiere que los SDK de anuncios inhabiliten los anuncios personalizados, la publicidad basada en intereses y el remarketing como parte del contenido dirigido a niños.
- Permita que los publicadores seleccionen formatos de anuncios que satisfagan la política de Monetización y Anuncios de Google Play y que cumplan con el requisito del Programa con contenido aprobado por profesores.
- Asegúrese de que se usen ofertas en tiempo real para mostrar anuncios a los niños, que se hayan revisado las creatividades y que se propaguen los indicadores de privacidad a los ofertantes.
- Proporciona a Google suficiente información, como la que se indica en el formulario de interés a continuación, para verificar el cumplimiento del SDK de anuncios con todos los requisitos de certificación, y responde de forma oportuna a cualquier solicitud de información adicional.

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

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

- Usa únicamente SDK de anuncios certificados por Google Play o implementa las protecciones necesarias para garantizar que todos los anuncios que se publiquen desde redes de mediación cumplan con estos requisitos.
- Brinda la información necesaria a las plataformas de mediación para indicar la clasificación del contenido del anuncio y cualquier contenido dirigido a niños que corresponda.

Si eres desarrollador, puedes consultar esta lista de SDK de anuncios autocertificados.

También puedes compartir este formulario de interés con SDK de anuncios que deseen autocertificarse.

Ficha de Play Store y promociones

La promoción y la visibilidad de una app afectan la calidad de Play Store de manera radical. Por este motivo, no debes incluir fichas de Play Store que contengan spam, promociones de mala calidad ni medios para aumentar la visibilidad de una app en Google Play artificialmente.

Promoción de apps

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

- El uso de anuncios engañosos en sitios web, apps y otras propiedades, lo que incluye las notificaciones que sean similares a las del sistema y alertas
- Las tácticas de promoción o de instalación que redireccionen a los usuarios a Google Play o a descargar apps sin previo aviso sobre la acción
- La promoción no solicitada mediante servicios por SMS.

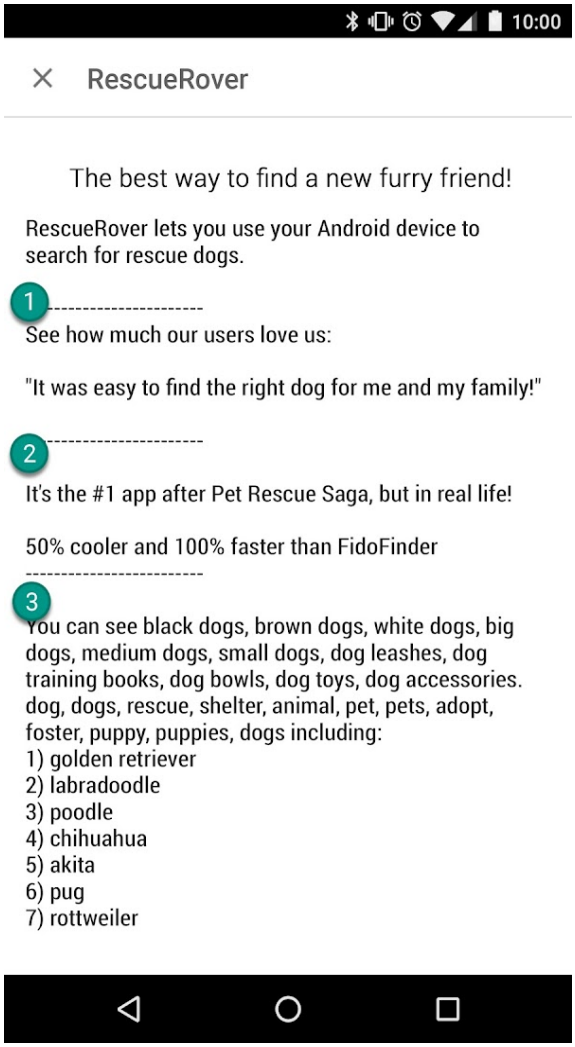
Es tu responsabilidad garantizar que todas las redes de publicidad o afiliados que estén asociados con la app cumplan con estas políticas y no participen de ninguna práctica de promoción que esté prohibida.

Metadatos

No permitimos apps con metadatos engañosos, no descriptivos, irrelevantes, excesivos, inapropiados ni con formato inadecuado, entre los que se incluye, la descripción de la app, el nombre del desarrollador, el título, el ícono, las capturas de pantalla y las imágenes promocionales. Los desarrolladores deben proporcionar una descripción clara y bien escrita de su app. Tampoco permitimos testimonios de usuarios anónimos o sin atribución en la descripción de la app.

Además de los requisitos mencionados aquí, es posible que las Políticas para Desarrolladores de Play te soliciten que proporciones información adicional sobre los metadatos.

Los siguientes son ejemplos comunes de incumplimiento:



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

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

- Imágenes o videos con contenido de carácter sexual (no incluyas imágenes con contenido provocativo, como pechos, nalgas, genitales o cualquier contenido anatómico vulgarizado, tanto real como ilustrado).
- Lenguaje profano, vulgar u otro lenguaje inapropiado para el público general en la ficha de Play Store de tu app.
- Violencia gráfica o representada de manera explícita en íconos de apps, videos o imágenes promocionales.
- Representaciones del uso de drogas ilegales. Incluso el contenido de carácter educativo, documental, científico o artístico (EDSA) debe ser apto para todo público en la ficha de Play Store.

A continuación, se detallan algunas prácticas recomendadas:

- Destaca lo mejor de la app. Comparte datos interesantes para que los usuarios entiendan qué tiene de especial.
- Asegúrese de que el título y la descripción de la app describan su funcionalidad de forma precisa.
- Evite el uso de palabras clave o referencias que sean repetitivas o que no estén relacionadas con la app.
- Use una descripción breve y directa. Por lo general, las descripciones cortas ofrecen una mejor experiencia del usuario, especialmente en los dispositivos con pantallas pequeñas. El uso de repeticiones, formato

inadecuado y longitud o detalles excesivos puede tener como resultado el incumplimiento de esta política.

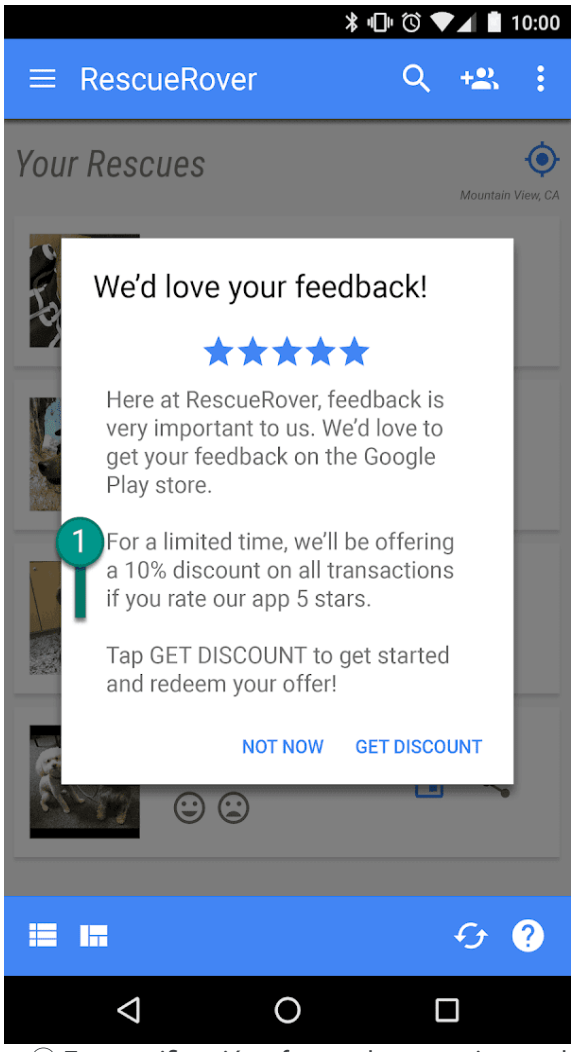
- Recuerde que la ficha debe ser apta para todo público. Evita el uso de texto, imágenes o videos inapropiados en la ficha, y cumple con los lineamientos mencionados.

Calificaciones, instalaciones y opiniones de usuarios

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

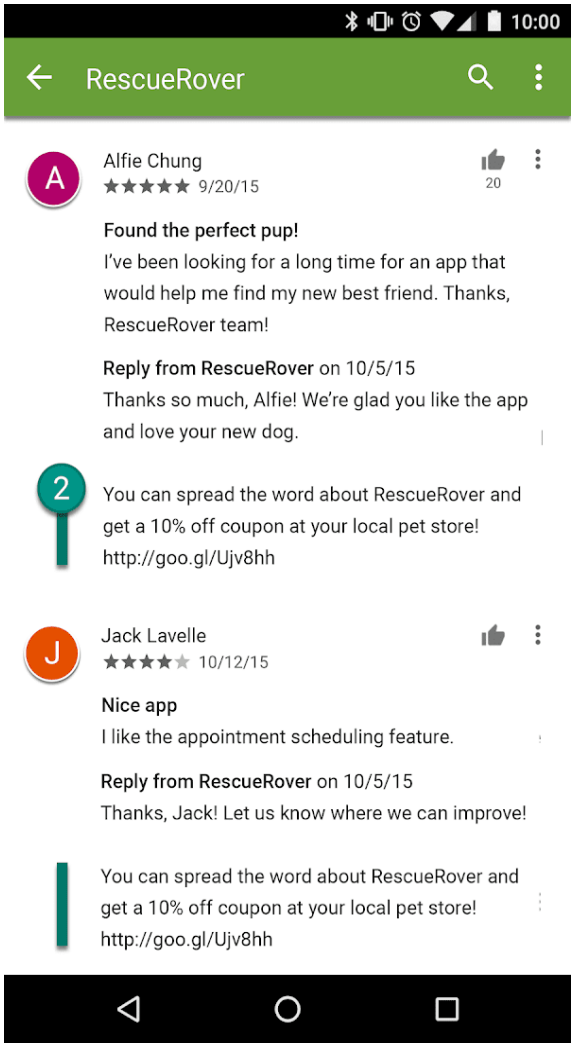
Los siguientes son ejemplos comunes de incumplimiento:

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



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

- Enviar calificaciones de forma reiterada para influir en la posición de la aplicación en Google Play
- Enviar o motivar a los usuarios a que envíen opiniones que incluyan contenido inapropiado, como afiliados, cupones, códigos de juegos, direcciones de correo electrónico o vínculos a otras aplicaciones o sitios web



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

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

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

Clasificaciones del contenido

La Coalición Internacional de Clasificación por Edad (IARC) proporciona las clasificaciones de contenido de Google Pla, que están diseñadas para ayudar a los desarrolladores a comunicar las clasificaciones de contenido relevantes a nivel local. Las autoridades regionales de la IARC mantienen lineamientos que se usan para determinar el nivel de madurez del contenido en una app. No permitimos apps que no tengan clasificación de contenido en Google Play.

Cómo se usan las clasificaciones del contenido

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

Cómo se determina la clasificación del contenido

Para recibir una clasificación del contenido, debes completar un cuestionario de clasificación en Play Console acerca de las características del contenido que incluyen tus apps. En función de las respuestas al cuestionario, se le asignará a la app una clasificación del contenido de varias autoridades de clasificación. Debes proporcionar respuestas precisas en el cuestionario de clasificación del contenido. Las respuestas falsas sobre el contenido de la app pueden tener como resultado su eliminación o suspensión.

Para evitar que la app aparezca como "Sin calificación", debes completar el cuestionario de clasificación del contenido para cada app nueva que envíes a Play Console y para todas las apps existentes activas en Google Play.

Si realizas cambios en el contenido o las funciones de la app que afecten las respuestas del cuestionario de clasificación, debes completar un nuevo cuestionario en Play Console.

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

Cómo apelar una clasificación

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

Noticias

Las aplicaciones que se declaren como pertenecientes a la categoría "Noticias" en Play Console ("aplicaciones de Noticias") deben cumplir con todos los requisitos que se indican a continuación.

Las aplicaciones de Noticias que requieren que se compre una membresía deben proporcionar a los usuarios una vista previa del contenido en la aplicación antes de que se realice la compra.

Las aplicaciones de noticias DEBEN hacer lo siguiente:

- proporcionar información de propiedad sobre el editor de noticias y sus colaboradores, incluidos, sin limitaciones, el sitio web oficial de las noticias publicadas en su aplicación, información de contacto válida y comprobable, y el editor original de cada artículo
- tener un sitio web dedicado o una página dentro de la aplicación que indique claramente que contiene información de contacto, sea fácil de encontrar (p. ej., un vínculo en la parte inferior de la página principal o en la barra de navegación del sitio) y proporcione información de contacto válida del editor de noticias (incluidos, al menos, un número de teléfono y una dirección de correo electrónico de contacto)

Recuerde que los vínculos a cuentas de redes sociales no se consideran una forma suficiente de información de contacto del editor. Además, las aplicaciones que contienen principalmente contenido generado por usuarios (p. ej., aplicaciones de redes sociales) no se deben declarar como aplicaciones de noticias.

Las aplicaciones de noticias NO DEBEN hacer lo siguiente:

- Contener errores ortográficos ni gramaticales significativos
- tener únicamente contenido estático (p. ej., contenido con varios meses de antigüedad)

- tener como objetivo principal el marketing de afiliación o los ingresos por anuncios

Tenga en cuenta que las aplicaciones de Noticias *pueden* usar anuncios y otras formas de marketing para monetizar, siempre y cuando el objetivo principal no sea vender productos ni servicios, ni generar ingresos publicitarios.

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

Spam y Funcionalidad Mínima

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

Spam

No permitimos apps que envíen spam a los usuarios o a Google Play, como las que envían mensajes no solicitados, o las apps repetitivas y de mala calidad.

Spam a través de mensajes

No permitimos apps que envíen SMS, correos electrónicos u otro tipo de mensajes en nombre del usuario sin darle la posibilidad de confirmar el contenido y los destinatarios.

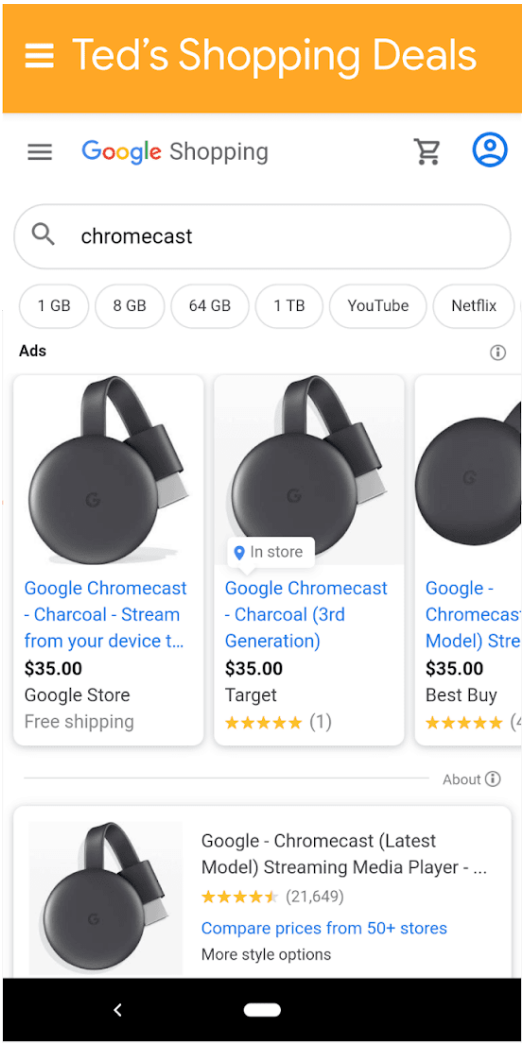
Spam de afiliados y de vistas web

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

Los siguientes son ejemplos comunes de incumplimiento:

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

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



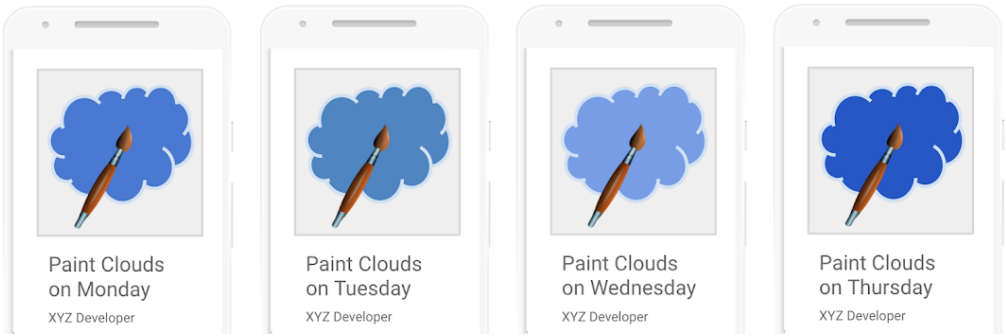
  Esta aplicación se denomina "Ofertas de Shopping de Ted" y simplemente proporciona una vista web de Google Shopping.

Contenido repetitivo

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

Los siguientes son ejemplos comunes de incumplimiento:

- Copiar elementos de otras apps sin agregar contenido o valor original
- Crear varias apps con un contenido y una experiencia del usuario muy similares (si estas apps tienen poco volumen de contenido, los desarrolladores deben considerar la creación de una sola app que incluya todo el contenido)



Apps creadas para la publicación de anuncios

No permitimos las apps cuyo objetivo principal sea publicar anuncios.

Los siguientes son ejemplos comunes de incumplimiento:

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

Funcionalidad mínima

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

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que no tienen ninguna función o que están diseñadas para no realizar ninguna acción

Funcionalidad dañada

No permitimos las apps que fallen, se cierren de manera forzada, se bloqueen o funcionen de manera anormal.

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que **no se instalan**
- Apps que se instalan, pero que **no se cargan**
- Apps que se cargan, pero que **no responden**

Otros programas

Además de cumplir con las políticas de contenido que se establecen en este Centro de políticas, es posible que las apps que se diseñen para otras experiencias de Android y se distribuyan mediante Google Play estén sujetas a requisitos de políticas específicas del programa. Por ello, asegúrate de revisar la lista que aparece a continuación para determinar si alguna de estas políticas se aplica a tu contenido.

Apps instantáneas Android

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

Los desarrolladores que elijan distribuir Apps instantáneas Android mediante Google Play deberán cumplir con las siguientes políticas, además de todas las otras Políticas del programa para desarrolladores de Google Play.

Identidad

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

Compatibilidad con vínculos

Los desarrolladores de Apps instantáneas Android deben proporcionar vínculos para otras apps. Si las apps instantáneas o instaladas del desarrollador contienen vínculos que pueden dirigir a una app instantánea, el desarrollador deberá enviar a los usuarios a esa app instantánea, en lugar de capturar los vínculos en una WebView.

Especificaciones técnicas

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

Ofertas para instalar la app

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

- Usar el ícono "Obtener app" de Material Design y la etiqueta "Instalar" para el botón de instalación
- No tener más de 2 a 3 solicitudes de instalación implícita en la app instantánea
- Abstenerse de usar banners o cualquier otra técnica de tipo publicitario para presentar una solicitud de instalación a los usuarios.

Para obtener detalles adicionales sobre las apps instantáneas y los lineamientos de UX, consulta las Prácticas recomendadas para la experiencia del usuario.

Cambios en el estado del dispositivo

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

Visibilidad de la app

Los programadores deberán asegurarse de que el usuario pueda ver las apps instantáneas de forma tal que sea consciente en todo momento de que se están ejecutando en su dispositivo.

Identificadores de dispositivos

Las apps instantáneas tendrán prohibido acceder a los identificadores del dispositivo que (1) persistan después de que la app instantánea haya dejado de ejecutarse y (2) el usuario no pueda restablecer. Entre algunos ejemplos, se incluyen los siguientes:

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

Las apps instantáneas podrán acceder al número de teléfono solo mediante el permiso de tiempo de ejecución. Los programadores no podrán tomar las huellas digitales del usuario mediante estos identificadores o cualquier otro medio.

Tráfico de red

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

Familias

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

Obtén más información sobre el proceso y consulta la lista de tareas interactiva en la Academia de apps.

Cómo diseñar apps para niños y familias

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

La palabra "niños" puede tener distintos significados en diferentes regiones y contextos. Es importante que consultes a tus asesores legales a fin de determinar qué obligaciones o restricciones relacionadas con la edad pueden corresponder a tu app. Dado que tú conoces mejor que nadie cómo funciona, contamos con tu ayuda a fin de garantizar que las apps de Google Play sean seguras para las familias.

Las apps que estén diseñadas específicamente para niños deben participar en el programa Designed for Families. Si tu app está orientada tanto a niños como a mayores, igualmente puedes participar en el programa Designed for Families. Todas las apps que acepten participar en el programa Designed for Families serán aptas para participar en el Programa con Contenido Aprobado por Profesores, pero no podemos garantizar que se incluyan en el mismo. Si decides no participar en el programa Designed for Families, debes cumplir con los siguientes requisitos de la Política de Familias de Google Play, así como con todas las demás Políticas del Programa para Desarrolladores de Google Play y el Acuerdo de Distribución para Desarolladores.

Requisitos de Play Console

Público objetivo y contenido

En la sección Público objetivo y contenido de Google Play Console, debes seleccionar el público objetivo de tu app antes de publicarlo. Para ello, selecciona uno de los grupos de edades disponibles. Independientemente de tu selección en Google Play Console, si decides incluir en tu app imágenes y terminología que pudiera considerarse que se dirige a niños, esto podría afectar la evaluación de Google Play sobre el público objetivo declarado. Google Play se reserva el derecho de revisar por su cuenta la información que brindes sobre la app, a fin de determinar si el público objetivo declarado es el correcto.

Si seleccionas un público objetivo que solo incluye adultos, pero Google determina que tu selección es incorrecta porque tu app se orienta tanto a niños como a adultos, tendrás la opción de aclararles a los usuarios que tu app no se orienta a niños mediante la incorporación de una etiqueta de advertencia.

Solo debes seleccionar más de un grupo de edades como público objetivo de tu app si la diseñaste para los usuarios que se incluyen en los grupos de edades seleccionados y te aseguraste de que fuera apta para ellos. Por ejemplo, las apps diseñadas para bebés, niños pequeños y niños de edad preescolar solo deben tener seleccionado el grupo "Hasta 5 años" como público objetivo. Si la app está diseñada para un nivel educativo específico, elige el grupo de edades que mejor represente ese nivel educativo. Solo debes seleccionar grupos de edades que incluyan niños y adultos si tienes la certeza de haber diseñado tu app para todas las edades.

Actualizaciones de la sección Público objetivo y contenido

Podrás actualizar la información de tu app en la sección Público objetivo y contenido de Google Play Console en cualquier momento. Para que la información se vea reflejada en Google Play Store, deberás realizar una actualización de la app. Sin embargo, es posible que se revisen los cambios que realices en esta sección de Google Play Console a fin de garantizar que cumplan con las políticas, incluso antes de que se envíe la actualización de la app.

Te recomendamos que les avises a los usuarios actuales si realizas algún cambio en el grupo de edades objetivo de tu app o si comienzas a usar anuncios o compras directas desde ella, ya sea en la sección "Novedades" de la ficha de Play Store de la app o mediante notificaciones dentro de ella.

Tergiversación en Play Console

La tergiversación de cualquier información relacionada con tu app en Play Console, incluida la sección "Público objetivo y contenido", puede tener como resultado la eliminación o suspensión de tu app, por lo que es fundamental proporcionar la información correcta.

Requisitos de la Política de Familias

Si los niños son uno de los públicos objetivo de tu app, debes cumplir con los requisitos que se detallan a continuación. El incumplimiento de estos requisitos puede dar lugar a la eliminación o suspensión de la app.

1. **Contenido de la app:** El contenido de la app al que pueden acceder niños debe ser apto para ellos.
2. **Respuestas en Google Play Console:** Debes responder con precisión las preguntas relacionadas con tu app en Google Play Console y actualizar esas respuestas para que reflejen con exactitud cualquier cambio que realices en ella.
3. **Anuncios:** Si tu app muestra anuncios para niños o usuarios de edad desconocida, debes hacer lo siguiente:
   - usar únicamente SDK de anuncios certificados por Google Play para mostrar anuncios a esos usuarios
   - asegurarte de que los anuncios que se muestren a esos usuarios no incluyan publicidad basada en intereses (publicidad orientada a usuarios individuales que tienen determinadas características según su comportamiento de navegación en línea) ni remarketing (publicidad orientada a usuarios individuales según su interacción previa con una app o un sitio web)
   - asegurarse de que los anuncios que se muestren a esos usuarios presenten contenido apropiado para niños
   - asegurarse de que los anuncios que se muestren a esos usuarios sigan los requisitos de formato del anuncio para Familias
   - garantizar el cumplimiento de todas las normativas legales aplicables y los estándares de la industria relacionados con la publicidad dirigida a niños
4. **Recopilación de Datos:** Debe divulgar todo tipo de recopilación de información personal y sensible de los niños en su aplicación, incluidos los casos en que esta se recopile mediante API o SDK que se llamen o usen en su aplicación. La información sensible de los niños incluye, entre otros datos, información de autenticación, datos del sensor del micrófono y la cámara, datos del dispositivo, ID de Android, ID de publicidad y datos de uso de anuncios.
5. **API y SDK:** Debes asegurarte de que tu app implemente cualquier API y SDK de forma adecuada.

- Las apps que se orienten únicamente a niños no deben contener API ni SDK cuyo uso no esté aprobado para servicios dirigidos a niños. Esto incluye el Acceso con Google (o cualquier otro Servicio de las API de Google que acceda a datos asociados con una Cuenta de Google), los Servicios de Juego de Google Play y cualquier otro Servicio de las API que use tecnología OAuth para la autenticación y autorización.
- Las aplicaciones orientadas tanto a niños como a públicos mayores no deben implementar API ni SDK cuyo uso no esté aprobado para servicios dirigidos a niños, a menos que se usen detrás de una pantalla neutral de comprobación de edad o se implementen de una manera que no implique la recopilación de datos de niños (p. ej., ofrecer el Acceso con Google como una función opcional). Las apps que se orienten tanto a niños como a usuarios mayores no deben requerir que los usuarios accedan a su cuenta o accedan al contenido de la app mediante una API o un SDK que no esté aprobado para su uso en servicios dirigidos a niños.

6. **Política de Privacidad:** Debes proporcionar un vínculo a la Política de Privacidad de tu app en la página de la ficha de Play Store correspondiente. El vínculo se debe mantener activo mientras la app esté disponible en Play Store y debe llevar a una Política de Privacidad que, entre otras cosas, describa correctamente cómo tu app recopila y usa los datos.
7. **Restricciones especiales:**
   - Si tu app usa realidad aumentada, debes incluir una advertencia de seguridad que aparezca tan pronto como se abra la sección de RA. La advertencia debe contener los siguientes elementos:
     - Un mensaje adecuado sobre la importancia de la supervisión parental
     - Un recordatorio sobre los riesgos físicos en el mundo real (p. ej., estar atento al entorno)
   - La app no debe requerir el uso de un dispositivo no recomendado para niños (p. ej., Daydream, Oculus)
8. **Cumplimiento Legal:** Debe asegurarse de que su aplicación, incluidos todos los SDK o API a los que llame o use, cumpla con la Ley de Protección de la Privacidad de Menores en Internet (COPPA) de los EE.UU., el Reglamento General de Protección de Datos (GDPR) de la UE y cualquier otra ley o reglamentación aplicable.

Los siguientes son ejemplos comunes de incumplimiento:

- Apps que promueven juegos para niños en sus fichas de Play Store, pero cuyo contenido solo es apropiado para adultos
- Apps que implementan API con Condiciones del Servicio que prohíben su uso en apps dirigidas a niños
- Apps que exaltan el consumo de alcohol, tabaco o sustancias controladas
- Apps que incluyen apuestas reales o simuladas
- Apps que incluyen violencia, imágenes sangrientas o contenido ofensivo no apto para niños
- Apps que proporcionan servicios de citas o que brindan consejos sexuales o asesoramiento matrimonial
- Apps que contienen vínculos a sitios web que presentan contenido que infringe las Políticas del Programa para Desarrolladores de Google Play
- Apps que muestran anuncios para adultos (p. ej., contenido violento, sexual o de juegos de apuestas) a niños Consulta las políticas de Monetización y Anuncios de Familias para obtener más información sobre las políticas de Google Play sobre publicidad, compras directas desde la app y contenido comercial para niños.

Programa Designed for Families

Las apps que estén diseñadas específicamente para niños deben participar en el programa Designed for Families. Si tu app está diseñada para un público general, incluidos niños y familias, también puedes solicitar participar en el programa.

Para que se acepte su aplicación en el programa, esta debe cumplir con todos los requisitos de la Política de Familias y los requisitos de elegibilidad de Diseñado para Familias, además de los que se indican en

las Políticas del Programa para Desarrolladores de Google Play y el Acuerdo de Distribución para Desarrolladores.

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

Elegibilidad para participar en el programa

Todas las apps que participen en el programa Designed for Families deben incluir contenido de la app y anuncios que sean relevantes y apropiados para niños y, además, satisfacer todos los requisitos que se detallan a continuación. Las apps que se acepten en el programa Designed for Families deben mantenerse en pleno cumplimiento de todos los requisitos del programa. Google Play puede rechazar, quitar o suspender cualquier app que se considere inapropiada para el programa Designed for Families.

Requisitos de Designed for Families

1. Las apps deben estar clasificadas por la ESRB como "Aptas para todo público" o "Para mayores de diez años", o tener una clasificación equivalente.
2. Debe divulgar correctamente los elementos interactivos de la app en el Cuestionario de Clasificación del Contenido de Google Play Console, incluidos los siguientes casos:
   - si los usuarios pueden interactuar o intercambiar información
   - si la app comparte con terceros la información personal proporcionada por los usuarios
   - si la app comparte la ubicación física del usuario con otros usuarios
3. Si tu app usa la API de Android Speech, el parámetro RecognizerIntent.EXTRA_CALLING_PACKAGE debe configurarse con su PackageName.
4. Las apps solo deben usar SDK de anuncios certificados por Google Play.
5. Las apps que estén diseñadas específicamente para niños no pueden solicitar permisos de ubicación.
6. Las apps deben usar el Administrador de dispositivo complementario (CDM) cuando soliciten Bluetooth, a menos se orienten únicamente a las versiones del sistema operativo (SO) del dispositivo no compatibles con CDM.

Los siguientes son ejemplos comunes de apps que no son aptas para el programa:

- Apps que están clasificadas por la ESRB como Aptas para todo público, pero contienen anuncios de juegos de apuestas
- Apps para padres o cuidadores (p. ej, las dedicadas al seguimiento de la lactancia o guías sobre desarrollo)
- Guías para padres o apps de administración de dispositivos diseñadas para que las usen únicamente padres o cuidadores
- Apps que usan un ícono de la app o un ícono de selector que es inadecuado para niños

Categorías

Si se acepta la participación de tu app en el programa Designed for Families, puedes elegir una segunda categoría específica para Familias que describa tu app. A continuación, se indican las categorías disponibles para las apps que participan en el programa Designed for Families:

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

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

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

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

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

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

Anuncios y monetización

Las siguientes políticas se aplican a cualquier publicidad que aparezca en tu app, incluidos los anuncios de tus apps y apps de terceros, las ofertas de compra directa desde la app o cualquier otro contenido comercial (como colocaciones de productos pagadas) que se muestran a los usuarios de apps sujetas a los requisitos de la Política de Familias y/o los requisitos del programa Designed for Families. Toda publicidad y oferta de compras directas desde la app, así como el contenido comercial de estas apps, deben cumplir con las leyes y normas aplicables (incluidos los lineamientos autorregulatorios o de la industria que sean relevantes).

Google Play se reserva el derecho de rechazar, quitar o suspender apps por usar tácticas comerciales demasiado agresivas.

Requisitos del formato de los anuncios

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

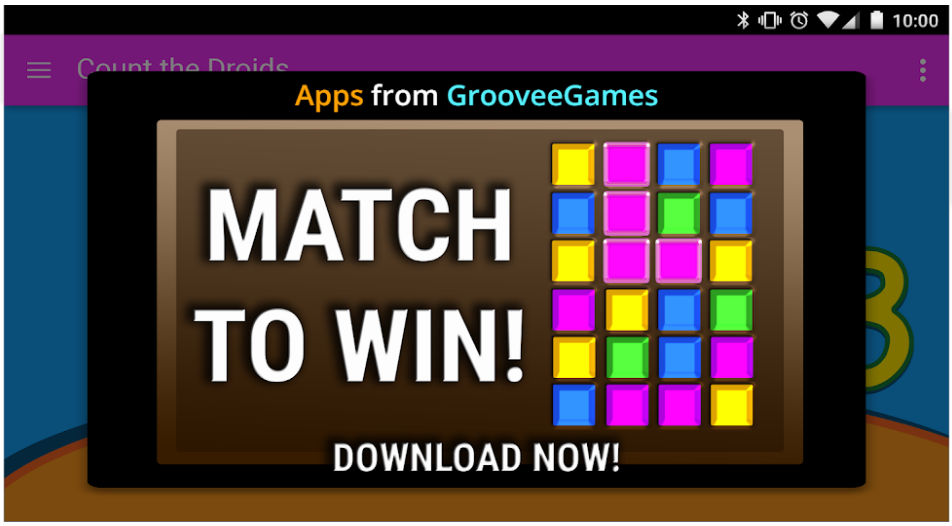
- Anuncios invasivos, incluidos los anuncios que ocupen toda la pantalla o interfieran con el uso normal y no proporcionen un medio claro para descartar el anuncio (p. ej., paneles de anuncios)
- Anuncios que interfieran con el uso normal de la app o el juego y que no se puedan cerrar después de 5 segundos; los anuncios que no interfieran con el uso normal de la app o el juego pueden persistir durante más de 5 segundos (p. ej., contenido de video con anuncios integrados)
- Anuncios intersticiales y ofertas de compras directas desde la app que aparezcan inmediatamente después de que se abra la app
- Varias colocaciones de anuncios en una página (p. ej., no se permiten anuncios de banner que muestren varias ofertas en una ubicación o que muestren más de un anuncio de banner o video)
- Anuncios y ofertas de compras directas desde la app que no se distingan fácilmente del contenido de la app
- Tácticas ofensivas o emocionalmente manipuladoras para promover la visualización de anuncios o las compras directas desde la app
- Falta de distinción entre el uso de monedas virtuales de juego y dinero real para hacer compras directas desde la app

Los siguientes son ejemplos comunes de incumplimiento en el formato del anuncio:

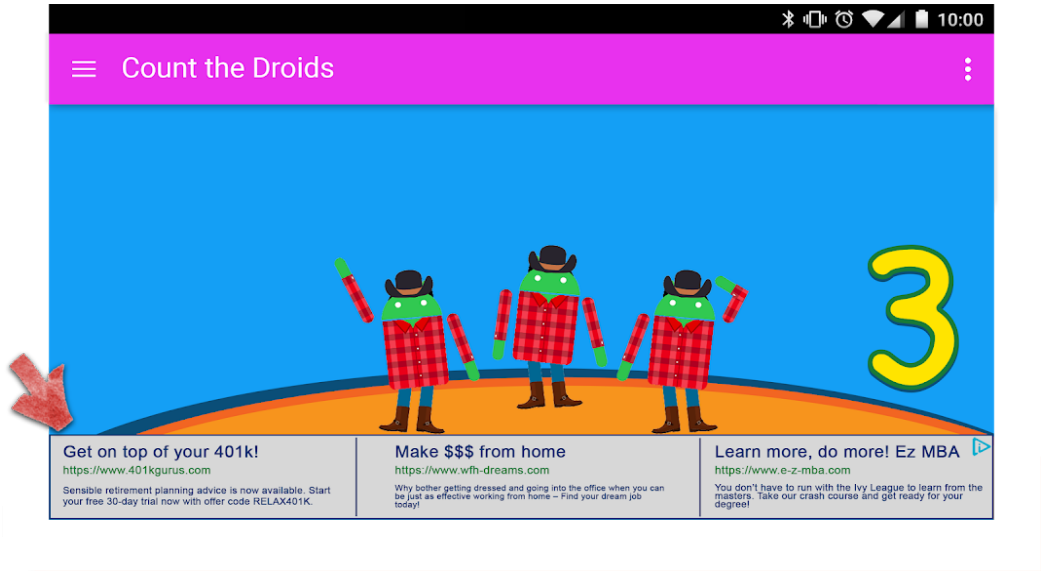
- Anuncios que se alejan del dedo del usuario cuando este trata de cerrarlos

- Anuncios que no proporcionan al usuario una forma de salir de la experiencia del anuncio después de cinco (5) segundos, como se muestra en el siguiente ejemplo:

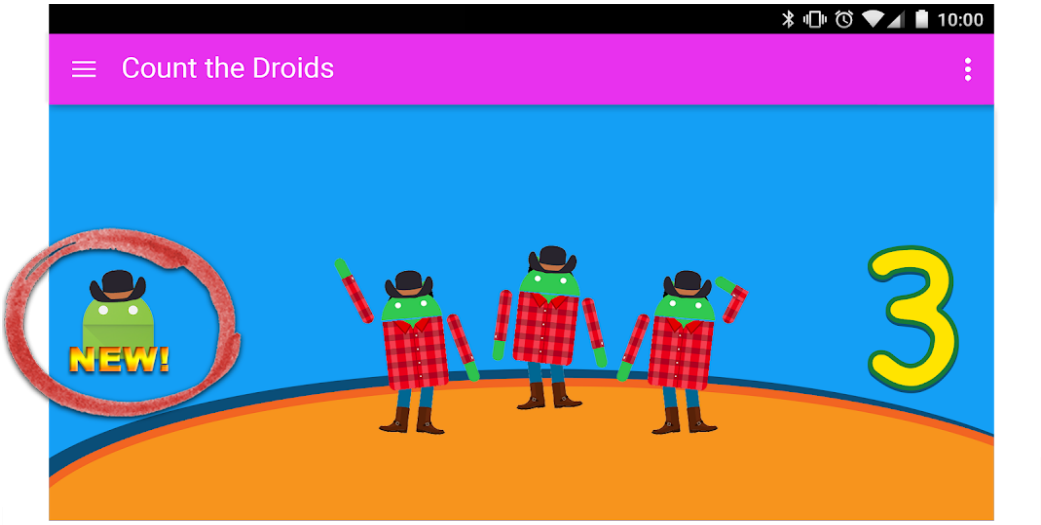
- Anuncios que ocupan la mayor parte de la pantalla del dispositivo sin brindar al usuario una manera clara de descartarlos, como se muestra en el siguiente ejemplo:



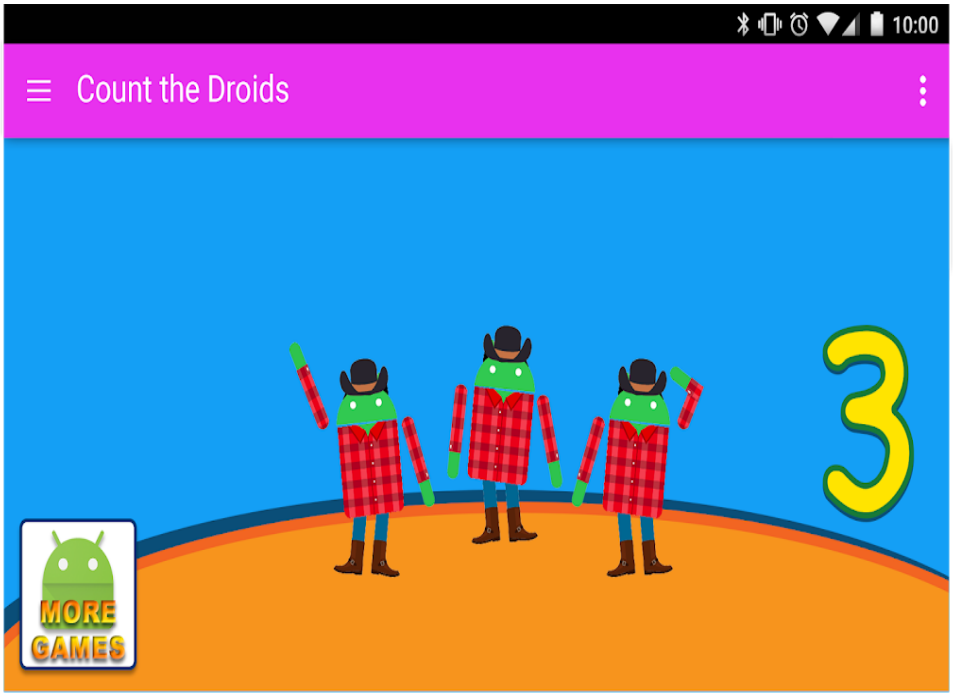
- Anuncios de tipo banner que muestran varias ofertas, como se muestra en el siguiente ejemplo:



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



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



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

- **Contenido multimedia inapropiado**: Incluye anuncios de programas de TV, películas, álbumes de música o cualquier otro medio de difusión que no sea apto para niños.
- **Videojuegos y software descargable inapropiados**: Incluye anuncios de software y videojuegos electrónicos descargables que no sean aptos para niños.
- **Sustancias controladas o dañinas**: Incluye anuncios sobre alcohol, tabaco, sustancias controladas o cualquier otra sustancia dañina.
- **Juegos de apuestas**: Incluye anuncios que simulen juegos de apuestas, concursos o promociones de sorteos, aunque la participación sea gratuita.
- **Contenido adulto y sexualmente provocativo**: Incluye anuncios con contenido sexual, provocativo o para mayores de edad.
- **Citas o relaciones**: Incluye anuncios de sitios de citas o relaciones adultas.
- **Contenido violento**: Incluye anuncios con contenido violento y explícito que no sea apto para niños.

SDK de anuncios

Si publicas anuncios en tu app y tu público objetivo solo incluye niños, debes usar los SDK de anuncios certificados de Google Play. Si el público objetivo de tu app incluye niños y usuarios mayores, debes implementar medidas para filtrar por edad, como una pantalla neutral de comprobación de edad, y asegurarte de que los anuncios que se muestran a niños provengan exclusivamente de SDK de anuncios autocertificados por Google Play. Las apps que participan en el programa Designed for Families solo pueden usar SDK de anuncios autocertificados.

Consulta la página de la Política del Programa de Anuncios para Familias a fin de obtener más detalles sobre estos requisitos y ver la lista actual de SDK de anuncios aprobados.

Si usas AdMob, ve al Centro de ayuda de AdMob para obtener más información sobre sus productos.

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

Compras directas desde apps

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

Aplicación de políticas

Es mejor evitar el incumplimiento de una política que tener que ocuparse de él una vez que sucede. Sin embargo, en caso de incumplimiento, nos comprometemos a garantizar que los desarrolladores entiendan qué medidas deben tomar para que sus apps cumplan con las Políticas. Comunícate con nosotros si ves algún incumplimiento o tienes alguna pregunta para administrar un incumplimiento.

Alcance de las políticas

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

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

Los términos descritos que se usan en estas políticas tienen el mismo significado que en el Acuerdo de Distribución para Desarrolladores (DDA). Además de cumplir con estas políticas y el DDA, el contenido de las aplicaciones debe estar clasificado de acuerdo con nuestros Lineamientos de Clasificación del Contenido.

No permitimos aplicaciones ni contenido que socaven la confianza de los usuarios en el ecosistema de Google Play. En el momento de evaluar la inclusión o eliminación de aplicaciones de Google Play, tenemos en cuenta varios factores, incluidos, sin limitaciones, un patrón de comportamiento dañino o un riesgo alto de abuso. A fin de identificar el riesgo de abuso, entre otros factores, tenemos en cuenta elementos como reclamos específicos de una aplicación o del desarrollador, denuncias de noticias, historial de incumplimientos anteriores, comentarios de los usuarios y el uso de marcas, personajes y otros elementos populares.

Cómo funciona Google Play Protect

Google Play Protect verifica las apps cuando las instalas. También analiza tu dispositivo periódicamente. Si detecta una app potencialmente dañina, es posible que haga lo siguiente:

- Enviarte una notificación. Para quitar la app, presiona la notificación y, luego, Desinstalar.
- Inhabilitar la app hasta que la desinstales.
- Quitar la app automáticamente. En la mayoría de los casos, si se detecta una app dañina, recibirás una notificación que te indicará que se quitó.

Cómo funciona la protección contra software malicioso

Para brindarte protección contra las URL y el software maliciosos de terceros, así como otros problemas de seguridad, es posible que Google reciba información sobre lo siguiente:

- Las conexiones de red de tu dispositivo
- Las URL potencialmente dañinas
- El sistema operativo y las apps instalados en tu dispositivo mediante Google Play o alguna otra fuente

Si una app o URL es potencialmente no segura, Google te enviará una advertencia. Google quitará o bloqueará su instalación si se confirma que es dañina para el dispositivo, los datos o los usuarios.

Puedes inhabilitar algunas de estas protecciones en la configuración de tu dispositivo. Sin embargo, es posible que Google continúe recibiendo información sobre las apps instaladas mediante Google Play y analizando las apps que hayas instalado desde otros orígenes para detectar problemas de seguridad sin enviar información a Google.

Cómo funcionan las alertas de privacidad

Google Play Protect te alertará cuando se quite alguna app de Google Play Store, dado que esta podría acceder a tu información personal, y tendrás la opción de desinstalarla.

Proceso de aplicación de las políticas

Si tu app no cumple con alguna de nuestras políticas, tomaremos las medidas correspondientes según se indica a continuación. Además, te enviaremos por correo electrónico información relevante sobre las medidas que tomamos, junto con instrucciones para apelar si crees que se tomaron medidas por error.

Es posible que los avisos administrativos o de eliminación no indiquen cada uno de los incumplimientos presentes en la app o en el catálogo completo de apps. Los desarrolladores son responsables de abordar los problemas de incumplimiento que se denuncien y de tomar cualquier medida adicional para garantizar que las apps cumplan, por completo, con las políticas. Si no resuelves los incumplimientos de política en todas tus apps, es posible que se apliquen medidas adicionales.

Los incumplimientos graves o repetidos (como software malicioso, fraude o apps que perjudiquen al dispositivo o al usuario) de estas políticas o del Acuerdo de Distribución para Desarrolladores (DDA) darán lugar a la rescisión de cuentas de desarrollador de Google Play individuales o relacionadas.

Acciones de aplicación de las políticas

Las diferentes acciones aplicadas pueden tener diversos efectos en tu app. En la siguiente sección, se describen las diversas acciones que Google Play puede realizar y el impacto en tu app o cuenta de desarrollador de Google Play. Esta información también se explica en este video.

Rechazo

- Una app nueva o una actualización de una app que se envíe para su revisión no estará disponible en Google Play.
- Si se rechazó una actualización de una app existente, la versión de la app publicada antes de la actualización seguirá disponible en Google Play.
- Los rechazos no afectan el acceso a las instalaciones, las estadísticas y las calificaciones de los usuarios rechazados.

- Los rechazos no afectan el estado de tu cuenta de desarrollador de Google Play.

Nota: No intentes volver a enviar una app rechazada hasta que hayas corregido todos los incumplimientos de política.

Eliminación

- La app, junto con sus versiones anteriores, se quitarán de Google Play y ya no estarán disponibles para que los usuarios la descarguen.
- Como consecuencia, los usuarios no podrán ver la ficha de Play Store, las instalaciones de los usuarios, las estadísticas ni las calificaciones. Esta información se restablecerá una vez que envíes una actualización de la app en cuestión que cumpla con la política.
- Es posible que los usuarios no puedan realizar compras directas desde la app ni utilizar funciones de facturación integrada en la app hasta que Google Play apruebe una versión que cumpla con las políticas.
- Las eliminaciones no afectan de inmediato el estado de tu cuenta de desarrollador de Google Play, pero, si recibes varias, esta podría suspenderse.

Nota: No intentes volver a publicar una app que se quitó hasta que hayas corregido todos los incumplimientos de política.

Suspensión

- La app, junto con las versiones anteriores, se quitarán de Google Play y ya no estarán disponibles para que los usuarios la descarguen.
- La suspensión puede ocurrir como resultado de incumplimientos graves o reiterados de las políticas, así como de rechazos o eliminaciones reiteradas de apps.
- Debido a que la app está suspendida, los usuarios no podrán ver la ficha de Play Store, las instalaciones de usuarios existentes, las estadísticas ni las calificaciones. Esta información se restablecerá una vez que envíes un reemplazo que cumpla con las políticas para la app que se quitó.
- Ya no puedes usar el APK ni el paquete de app de una app suspendida.
- Los usuarios no podrán realizar compras directas desde la app ni utilizar funciones de facturación integrada en la app hasta que Google Play apruebe una versión que cumpla con las políticas.
- Las suspensiones cuentan como advertencias para tu cuenta de desarrollador de Google Play. Si recibes varias advertencias, es posible que se rescindan cuentas de desarrollador de Google Play individuales y relacionadas.

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

Visibilidad limitada

- La visibilidad de tu app en Google Play está restringida. Tu app seguirá estando disponible en Google Play y los usuarios podrán acceder a ella con un vínculo directo a la ficha de Play Store.
- El estado de visibilidad limitada de la app no afecta el estado de tu cuenta de desarrollador de Google Play.
- El estado de visibilidad limitada de la app no afecta la capacidad de los usuarios de ver la ficha de Play Store, las instalaciones, las estadísticas y las calificaciones existentes.

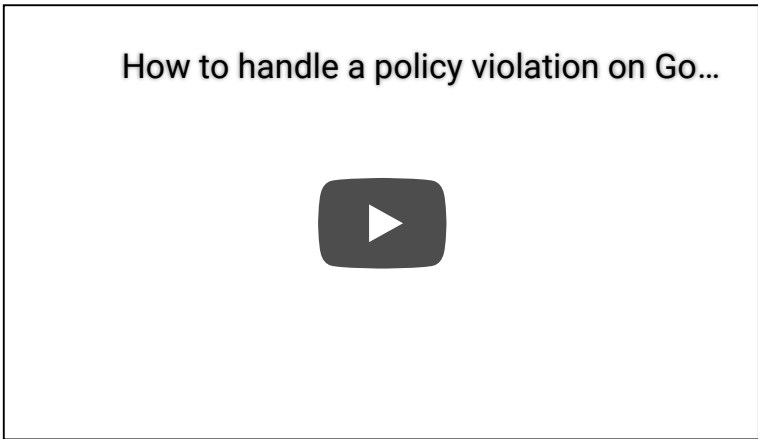
Rescisión de la cuenta

- Si se cancela tu cuenta de desarrollador, se quitarán de Google Play todas las apps de tu catálogo y ya no podrás publicar apps nuevas. Esto también significa que las cuentas de desarrollador de Google Play

relacionadas también se suspenderán de forma permanente.
- Además, las suspensiones reiteradas o que se deban a incumplimientos graves de las políticas pueden dar lugar a la rescisión de tu cuenta de Play Console.
- Dado que las apps de la cuenta cancelada se eliminan, los usuarios no podrán ver la ficha de Play Store, las instalaciones de usuarios existentes, las estadísticas ni las calificaciones.

Nota: También se cancelará cualquier cuenta nueva que intentes abrir (sin un reembolso de la tarifa de registro del desarrollador), así que no intentes registrarte para obtener una nueva cuenta de Play Console.

Cómo administrar y denunciar incumplimientos de políticas



Apelación a una acción de aplicación de políticas

Volveremos a publicar la app si decidimos que se cometió un error y que la app no incumple las Políticas del Programa y el Acuerdo de Distribución para Desarrolladores de Google Play. Si revisaste las políticas detenidamente y crees que nuestra decisión pudo haber sido un error, sigue las instrucciones que se proporcionan en la notificación por correo electrónico de aplicación de políticas para apelar nuestra decisión.

Recursos adicionales

Si necesitas más información sobre una acción de aplicación de una política o una calificación o comentario de un usuario, puedes consultar algunos de los siguientes recursos o comunicarte con nosotros a través del Centro de ayuda de Google Play. Sin embargo, no podemos brindarte asesoramiento legal. Si necesitas asesoramiento legal, consulta a un asesor legal.

- Apelaciones y verificación de las apps
- Informar una infracción de las políticas
- Comunícate con Google Play para obtener detalles sobre la rescisión de una cuenta o la eliminación de una app
- Advertencias
- Cómo denunciar apps y comentarios inapropiados
- Se quitó mi app de Google Play
- Casos de cancelación de cuenta de desarrollador de Google Play

¿Necesitas más ayuda?

Prueba estos próximos pasos:

Comunícate con nosotros

Cuéntanos más para que podamos ayudarte