Políticas del Programa para Desarrolladores

(con vigencia a partir del 28 de aseptiembre de 2022, a menos que se indique lo contrario)

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

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

Contenido restringido

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

Menores en situación de peligro

Las aplicaciones que no les prohíban a los usuarios crear, subir ni distribuir contenido que facilite la explotación o el abuso de niños estarán sujetas a la eliminación inmediata de Google Play. Esto incluye cualquier material de abuso sexual infantil. Para denunciar contenido de un producto de Google que pueda constituir explotación infantil, haga clic en **Denunciar abuso** . Si encuentra contenido de este tipo en cualquier otro sitio de Internet, comuníquese directamente con el organismo correspondiente de su país .

Prohibimos el uso de aplicaciones que pongan a los niños en riesgo. Esto incluye, sin limitaciones, el uso de aplicaciones para promover la conducta predatoria hacia los niños, como lo que se indica a continuación:

- Interacciones inapropiadas destinadas a un niño (por ejemplo, caricias inapropiadas o manoseo)
- Ciberacoso infantil (por ejemplo, establecer comunicación en línea con un niño para facilitar el contacto sexual o el intercambio de imágenes sexuales con ese menor, ya sea de forma virtual o fuera de Internet)
- Sexualización de un menor de edad (por ejemplo, imágenes que representen, fomenten o promuevan el abuso sexual de menores o la representación de menores de una manera que podría provocar la explotación sexual de menores)
- Extorsión sexual (por ejemplo, amenazar o chantajear a un niño por medio del acceso real o presunto a imágenes íntimas del menor)
- Tráfico de niños (por ejemplo, prostituir a un niño o publicar anuncios para la explotación sexual comercial de un menor)

Si detectamos contenido con material de abuso sexual infantil, tomaremos las medidas correspondientes, como la denuncia ante el National Center for Missing & Exploited Children. Si cree que un niño está en peligro o es víctima de abuso, explotación o trata de personas, comuníquese con su agencia local de orden público y con una de las organizaciones de seguridad infantil que se incluyen aquí .

Tampoco se permiten las aplicaciones atractivas para niños que tengan temas de adultos, lo que incluye, sin limitaciones, lo siguiente:

- Aplicaciones con excesiva violencia, sangre y derramamiento de sangre
- Aplicaciones que representen o fomenten actividades peligrosas y dañinas

Tampoco permitimos las aplicaciones que promuevan 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.

Contenido inapropiado

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

Contenido Sexual y Lenguaje Obsceno

No permitimos aplicaciones que incluyan o promuevan contenido sexual o lenguaje obsceno, como pornografía o cualquier contenido o servicio destinado a brindar placer de carácter sexual. No permitimos aplicaciones ni contenido que parezcan promocionar un acto sexual a cambio de una compensación. Se permite la publicación de contenido que incluya desnudez si su objetivo principal es educativo, documental, científico o artístico, y no injustificado.

Si una aplicación incluye contenido que incumpla esta política, pero se considera que dicho contenido es apropiado en una región en particular, es posible que se publique la aplicación para los usuarios de esa región, pero que no esté disponible para los de otras regiones.

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

- Representaciones de 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 de otro tipo que puedan interpretarse como servicios que proporcionan actos sexuales a cambio de una compensación, incluidos, sin limitaciones, las citas remuneradas o los acuerdos sexuales en los que se espere o esté implícito que un participante proporcione dinero, regalos o asistencia financiera a otro participante ("citas con compensación")
- Aplicaciones que degraden o deshumanicen a las personas, como aplicaciones que aseguren desvestir a las personas o ver a través de la ropa, incluso aunque estén etiquetadas como de bromas o entretenimiento

Incitación al odio o a la violencia

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

En ciertos países, es posible que se bloqueen las aplicaciones que incluyan contenido educativo, documental, científico o artístico relacionado con los nazis, de conformidad con las leyes y reglamentaciones locales.

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

- Contenido 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 aplicaciones que representan violencia ficticia en el contexto de un juego, como dibujos animados, o representaciones de caza o pesca.

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

- Representaciones gráficas o descripciones de violencia realista o amenazas violentas a personas o animales.
- Aplicaciones que promuevan acciones como autolesiones, el suicidio, trastornos de alimentación, juegos de asfixia u otras que puedan provocar lesiones graves o la muerte.

Contenido relacionado con el terrorismo

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

No permitimos aplicaciones que incluyan contenido relacionado con el terrorismo, como el que fomente actos terroristas, incite a la violencia o celebre ataques terroristas. Si publica contenido relacionado con el terrorismo con fines educativos, documentales, científicos o artísticos, tenga presente que debe brindar contexto relevante que explicite dichas finalidades.

Organizaciones y Movimientos Peligrosos

No permitimos que organizaciones ni movimientos publiquen aplicaciones en Google Play para ningún fin, incluido el reclutamiento, si participaron en actos de violencia contra civiles, se prepararon para cometerlos o asumieron la responsabilidad de ellos.

No permitimos aplicaciones que incluyan contenido relacionado con la planificación, preparación o glorificación de la violencia contra civiles. Si su aplicación incluye este tipo de contenido para fines educativos, documentales, científicos o artísticos, también debe ofrecer contexto relevante que explicite dichas finalidades.

Acontecimientos de carácter delicado

No permitimos aplicaciones que saquen provecho de sucesos delicados con un impacto significativo a nivel social, cultural o político, o que sean insensibles con respecto a ellos (como emergencias civiles, desastres naturales, emergencias de la salud pública, conflictos, muertes o cualquier otro tipo de acontecimiento trágico. Por lo general, se permiten las aplicaciones 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.

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

- Demostrar falta de sensibilidad ante la muerte de una persona o un grupo de personas por motivos de suicidio, sobredosis, causas naturales y otros
- Negar el suceso de un evento trágico importante y bien documentado
- Obtener ganancias a costa de un suceso delicado sin que se observe ningún beneficio para las víctimas
- Aplicaciones que incumplan los lineamientos del artículo Requisitos para las apps relacionadas con la enfermedad del coronavirus 2019 (COVID-19)

Bullying y acoso

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

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

- Hacer bullying a víctimas de conflictos religiosos o internacionales
- Intentar explotar a terceros con determinado contenido, 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 sus amigos y familiares

Productos peligrosos

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

- Los accesorios restringidos son aquellos que permiten que un arma de fuego simule disparos automáticos o que convierten un arma de fuego en una automática (p. ej., mecanismos de repetición o "bump stocks", 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 se permiten aplicaciones que faciliten la venta de marihuana ni productos de la marihuana, independientemente de su legalidad.

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

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

Tabaco y alcohol

No permitimos aplicaciones 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.

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

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

---

Servicios financieros

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

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

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

Opciones binarias

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

Criptomonedas

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

Préstamos Personales

Definimos los préstamos personales como aquellos préstamos de dinero que un individuo, una organización o una entidad otorga a un consumidor individual de manera no recurrente y que no tienen como objetivo financiar la compra de un activo fijo ni educación. Los consumidores de préstamos personales requieren información sobre la calidad, las características, las tarifas, 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
- Ejemplos no incluidos: Hipotecas, préstamos para la compra de vehículos, líneas de crédito rotativo (como tarjetas de crédito, líneas de crédito personales)

Las aplicaciones 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 tener establecida en Play Console la categoría de app "Finanzas" y divulgar la siguiente información en los metadatos de la aplicación:

- Período mínimo y máximo para el pago
- Tasa anual equivalente (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 la porción de capital y 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 se permiten aplicaciones que promuevan préstamos personales que requieran el pago íntegro en 60 días o menos desde la fecha de emisión del préstamo (nos referimos a estos como "préstamos personales a corto plazo").

Préstamos personales con TAE alta

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

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

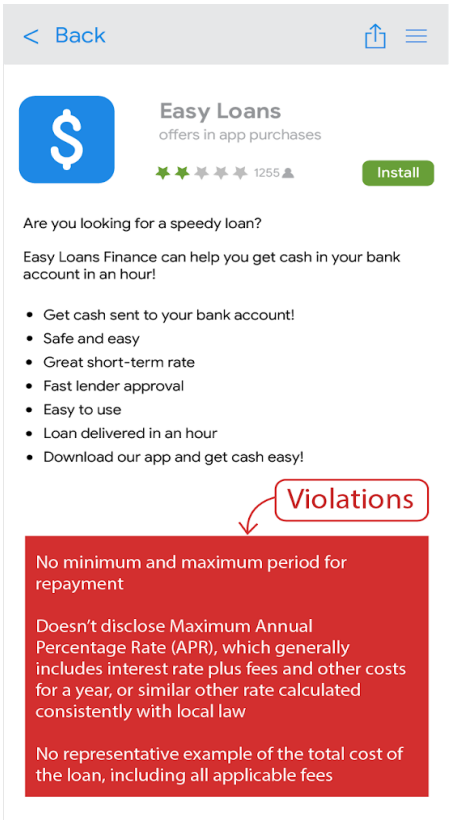
Requisitos adicionales para las aplicaciones de préstamos personales en la India, Indonesia y Filipinas

En la India, Indonesia y Filipinas, las aplicaciones de préstamos personales deben cumplir con los requisitos adicionales de validez de la elegibilidad que se indican a continuación.

1. **India**
   - Complete la Declaración de Aplicación de Préstamos Personales para la India y proporcione la documentación necesaria para respaldarla. Por ejemplo:
     - Si cuenta con una licencia emitida por el Banco de la Reserva de la India (RBI) para otorgar préstamos personales, debe enviar una copia de ella para que la revisemos.
     - Si no ejerce actividades de préstamo de dinero de forma directa y únicamente proporciona una plataforma para facilitar el préstamo de dinero a usuarios por medio de bancos o Empresas Financieras que No sean Bancos (NBFC), deberá reflejar esa información con exactitud en la declaración.
       - Además, los nombres de todos los bancos o NBFC registrados se deben divulgar de manera destacada en la descripción de la aplicación.
   - Asegúrese de que el nombre de la cuenta del desarrollador coincida con el nombre asociado de empresa registrada que proporcionó en su declaración.
2. **Indonesia**
   - Complete la Declaración de Aplicación de Préstamos Personales para Indonesia y proporcione la documentación necesaria para respaldarla. Por ejemplo:
     - Si su aplicación participa en actividades de Servicios de Préstamos de Dinero Basados en Tecnología de la Información de acuerdo con la Reglamentación de OJK N.º 77/POJK.01/2016 (según se enmiende ocasionalmente), debe enviar una copia de su licencia válida para que la revisemos.
   - Asegúrese de que el nombre de la cuenta del desarrollador coincida con el nombre asociado de empresa registrada que proporcionó en su declaración.
3. **Filipinas**
   - Complete la Declaración de Aplicación de Préstamos Personales para Filipinas y proporcione la documentación necesaria para respaldarla.
     - Todas las empresas financieras y crediticias que ofrezcan préstamos mediante Plataformas de Préstamos en Línea (OLP) deben obtener un Número de Registro en la SEC y el Número de Certificado de Autoridad (CA) de la Comisión de Bolsa y Valores de Filipinas (PSEC).
       - Además, debe divulgar su Nombre Corporativo, el Nombre de la Empresa, el Número de Registro en la PSEC y el Certificado de Autoridad para Operar una Empresa Financiera o Crediticia (CA) en la descripción de su aplicación.
     - Las aplicaciones involucradas en actividades de financiación colectiva basada en préstamos, como préstamos entre pares (P2P), o según se define en virtud de las Reglas y

Reglamentaciones que Rigen la Financiación Colectiva (CF Rules), deben procesar las transacciones a través de Intermediarios de CF registrados en la PSEC.

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



Juegos de apuestas

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 aplicaciones que habiliten o faciliten los juegos de apuestas en línea en países selectos, siempre y cuando el Desarrollador complete el proceso de solicitud para las aplicaciones de juegos de apuestas que se distribuyen en Google 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 aplicaciones válidas de juegos de apuestas autorizadas o con licencia que tengan los siguientes tipos de productos de juegos de apuestas en línea:

- Juegos de Casino en Línea
- Apuestas Deportivas
- Carreras de Caballos (en los casos en los que se regulen y se otorguen licencias por separado de las Apuestas Deportivas)
- Loterías
- Deportes de Fantasía Diarios

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

- El desarrollador debe completar el proceso de solicitud correctamente para distribuir la aplicación en Play.
- La aplicación 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 aplicación.
- 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 aplicación debe impedir que los usuarios menores de edad la usen.
- La aplicación 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 aplicación NO debe poder comprarse como una aplicación pagada en Google Play ni usar la Facturación integrada en Google Play.
- La descarga y la instalación de la aplicación desde Google Play Store deben ser gratuitas.
- La aplicación debe estar clasificada como "Solo para adultos" (AO) o un equivalente de la IARC.
- La aplicación y su ficha deben mostrar información clara sobre el uso responsable de los juegos de apuestas.

Otras apps de juegos, concursos y torneos con dinero real

En el caso de todas las demás aplicaciones que no cumplan con los requisitos de elegibilidad de las aplicaciones de juegos de apuestas que se indicaron anteriormente y que no se incluyan en los "Otros Pilotos de Juegos con Dinero Real" que se mencionan más abajo, no se admiten servicios ni contenido que permitan o faciliten a los usuarios realizar apuestas o participar con dinero real (incluidos los elementos integrados en la aplicación comprados con dinero) para obtener un premio de valor monetario real. Se incluyen, sin limitaciones, 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 Ludificados 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

Otros Pilotos de Juegos con Dinero Real

Con el fin de explorar posibles actualizaciones en la política de Otras Aplicaciones de Juegos, Concursos y Torneos con Dinero Real, Google Play está llevando a cabo pruebas por tiempo limitado para los tipos de juegos y en las regiones que se indican a continuación, sujetas a términos y condiciones adicionales:

Tipo de juego	Región	Período del piloto	Cómo participar
Juegos de Máquinas de Pinzas en Línea	Solo en Japón	11 de julio de 2022 al 11 de julio de 2023	Haga clic aquí para postularse
DFS/Rummy	Solo en la India	28 de septiembre de 2022 al 28 de septiembre de 2023	Haga clic aquí para postularse

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)

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
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 aplicaciones que faciliten o promuevan actividades ilegales.

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

- Facilitar la compra o venta de drogas ilegales
- 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

---

Entrada en vigencia: 11 de octubre de 2022

Contenido generado por usuarios

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

Las aplicaciones que contienen o presentan CGU, incluidas las que son clientes o navegadores especializados para dirigir a los usuarios a una plataforma de CGU, deben implementar una moderación de CGU robusta, eficiente y continua que cumpla con lo siguiente:

- Debe requerir que los usuarios acepten las condiciones de uso o políticas del usuario de la aplicación antes de crear o subir CGU.
- Debe definir el contenido censurable y los comportamientos inaceptables (de una manera que satisfaga las Políticas del Programa para Desarrolladores de Google Play) y prohibirlos en las condiciones de uso o las políticas del usuario de la aplicación.

- Debe implementar una moderación de CGU de forma razonable y coherente con el tipo de CGU que aloja la aplicación.
  - En el caso de las aplicaciones de realidad aumentada (RA), la moderación de CGU (incluido el sistema de informes en la aplicación) debe tener en cuenta tanto el CGU censurable 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).
- Debe proporcionar un sistema integrado en la aplicación para generar informes de usuarios y CGU censurables, así como tomar medidas contra esos usuarios o CGU según corresponda.
- Debe proporcionar un sistema integrado en la aplicación para bloquear usuarios y CGU.
- Debe brindar protecciones para evitar que la monetización dentro de la aplicación promueva un comportamiento inaceptable por parte del usuario.

Contenido Sexual Imprevisto

El contenido sexual se considera "imprevisto" si aparece en una aplicación de CGU que (1) proporciona acceso a contenido principalmente no sexual y (2) no promueve ni recomienda contenido sexual de forma activa. El contenido sexual definido como ilegal según la ley aplicable y el contenido de menores en situación de riesgo no se consideran "imprevistos" y están prohibidos.

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

- Ese contenido se oculta de forma predeterminada con filtros que requieren al menos dos acciones del usuario para inhabilitarse por completo (p. ej., detrás de una opción intersticial de ofuscación o excluido de la vista de forma predeterminada, a menos que se inhabilite una "búsqueda segura").
- Los niños, según se define en la política de Familias, tienen explícitamente prohibido acceder a su aplicación con sistemas para filtrar por edad, como una pantalla neutral de comprobación de edad o un sistema adecuado en virtud de lo definido en la ley aplicable.
- Su aplicación proporciona respuestas precisas al cuestionario de clasificación del contenido con respecto al CGU, según se requiere en virtud de la política de Clasificación del Contenido .

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

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

- Promoción de contenido sexual explícito generado por el usuario, incluida la implementación o autorización de funciones pagas 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.
- Aplicaciones que de manera continua no resuelvan las denuncias de los usuarios acerca del contenido inaceptable.

Servicios y Contenido Relacionados con la Salud

No permitimos aplicaciones que expongan a los usuarios a contenido y servicios de salud que sean nocivos.

Si su aplicación incluye contenido y servicios de salud o los promueve, debe asegurarse de que satisfaga las leyes y reglamentaciones aplicables.

Medicamentos de Venta con Receta

No permitimos aplicaciones que faciliten la venta o compra de medicamentos de venta con receta sin una receta.

Sustancias No Aprobadas

Google Play no permite que las aplicaciones promuevan ni vendan sustancias no aprobadas, independientemente de cualquier pretensión de legalidad.

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

- Todos los artículos de esta lista no exhaustiva de productos farmacéuticos y suplementos prohibidos
- Productos que contengan efedra
- Productos que contengan 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 regulatorias o gubernamentales
- Productos con nombres que puedan 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 .

Información Errónea sobre Salud

No permitimos aplicaciones que contengan declaraciones de salud engañosas que contradigan el consenso médico existente o que puedan causar daño a los usuarios.

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

- Declaraciones engañosas sobre vacunas (por ejemplo, que las vacunas pueden alterar el ADN)
- Apoyo a tratamientos dañinos no aprobados
- Apoyo a otras prácticas de salud dañinas, como terapia de conversión

Restricciones con relación al COVID-19

Las aplicaciones deben cumplir con las exigencias que se indican en el artículo Requisitos para las apps relacionadas con la enfermedad del coronavirus 2019 (COVID-19) .

Funcionalidades Médicas

No permitimos aplicaciones que incluyan funciones médicas o relacionadas con la salud que sean engañosas o potencialmente perjudiciales. Por ejemplo, no se permiten las aplicaciones que declaren tener una función de oximetría que se base únicamente en la aplicación. Las aplicaciones de oximetría deben estar respaldadas por hardware externo, wearables o sensores dedicados de smartphones que se hayan diseñado para tal fin. Estas aplicaciones admitidas también deben contener renuncias de responsabilidad en los metadatos que afirmen que no están pensadas para uso médico, que no son un

dispositivo médico y que solo están diseñadas con fines generales de bienestar y fitness, y deben divulgar de forma correcta los modelos de dispositivo o hardware compatibles.

Pagos: Servicios Clínicos

Las transacciones que involucran servicios clínicos regulados no deben usar el sistema de facturación de Google Play. Para obtener más información, consulte Información sobre la política de Pagos de Google Play .

Datos de Health Connect

Los datos a los que se accede con los Permisos para Health Connect se consideran datos personales y sensibles de los usuarios, y están sujetos a la política de Datos del Usuario y a requisitos adicionales .

Propiedad intelectual

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

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

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

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

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

Uso no autorizado del contenido protegido por derechos de autor

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

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

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

- Material gráfico para álbumes de música, videojuegos y libros
- Imágenes de comercialización de películas, televisión o videojuegos.
- Material gráfico o imágenes de libros de cómics, dibujos animados, películas, videos de música o televisión.
- Logotipos de equipos deportivos profesionales y universitarios.
- Fotos tomadas de la cuenta de medios sociales de una persona pública.
- Imágenes profesionales de personas públicas.

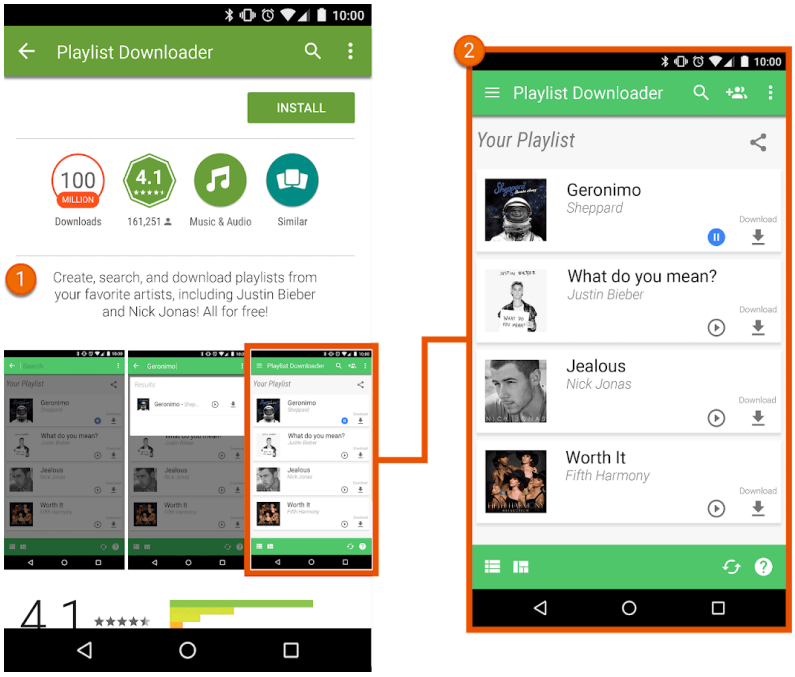
- Reproducciones o "fan art" que no puedan distinguirse de la obra original protegida por derechos de autor.
- aplicaciones que tienen consolas que reproducen clips de audio de contenido protegido por derechos de autor.
- Reproducciones completas o traducciones de libros que no son de dominio público

Acciones que fomentan el incumplimiento de los derechos de autor

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

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

- Apps de streaming que permitan que los usuarios descarguen copias locales de contenido protegido por derechos de autor sin autorización
- Aplicaciones que induzcan a los usuarios a transmitir y descargar obras protegidas por derechos de autor, incluido el contenido de música y video, que infringe la legislación vigente sobre derechos de autor:



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

Infracción de marca registrada

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

La infracción de marcas comerciales supone un uso inadecuado o no autorizado de una marca comercial idéntica o similar, de tal forma que es posible que provoque confusión con respecto al

origen de ese producto. Si tu aplicación usa una marca registrada de un tercero de tal forma que sea probable que provoque confusión, es posible que se suspenda.

Falsificación

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

Privacidad, engaño y abuso de dispositivos

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

Datos del usuario

Debe ser honesto en lo que respecta a la forma de manejar los datos del usuario (p. ej., la información que proporciona un usuario y la que se recopila sobre él, incluida la relacionada con dispositivos). Es decir, debe divulgar si su aplicación accede a los datos, así como cuándo los recopila, usa y comparte, además de limitar su uso a los fines divulgados. Por otra parte, si la aplicación administra datos personales y sensibles del usuario, consulte los requisitos adicionales en la sección "Datos Personales y Sensibles del Usuario" 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. Si incluye código de terceros (p. ej., SDK) en su aplicación, debe asegurarse de que ese código satisfaga las Políticas del Programa para Desarrolladores de Google Play.

Entrada en vigencia: 11 de octubre de 2022

Datos Sensibles y Personales del Usuario

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; inventario de otras aplicaciones en el dispositivo, el micrófono y la cámara, y otros datos sensibles relacionados con el uso o el dispositivo. Si su aplicación manipula datos sensibles y personales de los usuarios, asegúrese de hacer lo siguiente:

- Limite su acceso a los datos personales y sensibles adquiridos a través de la aplicación, así como la recopilación, el uso y el uso compartido de esa información, para fines directamente relacionados con la provisión y mejora de las funciones de la aplicación (p. ej., una función que espera el usuario y que se documenta y anuncia en la descripción de la aplicación en Google Play). El uso compartido de datos personales y sensibles de los usuarios incluye utilizar SDK u otros servicios de terceros que hagan que los datos se transfieran a una entidad externa. Las aplicaciones que extiendan el uso de datos personales y sensibles de los usuarios para mostrar publicidad deben satisfacer nuestra Política de Anuncios .
- Manipule todos los datos personales y sensibles de los usuarios de forma segura, lo que incluye transmitirlos con criptografía moderna (por ejemplo, a través de HTTPS).
- Cuando esté disponible, use una solicitud de permisos de tiempo de ejecución antes de acceder a los datos conpermisos de Android .
- No venda datos personales ni sensibles de los usuarios.

Divulgación Destacada y Requisito de Consentimiento

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

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

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

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

- Debe presentar el 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 (que incluye presionar los botones de inicio, salir o atrás).
- No debe usar mensajes que caduquen ni se descarten automáticamente como medio para obtener el consentimiento del usuario.

Para cumplir con los requisitos de la política, le recomendamos que siga el siguiente ejemplo de formato de divulgación destacada cuando sea necesario:

- "[Esta aplicación] recopila, transmite, sincroniza o almacena [tipos de datos] para activar ["función"], [en determinado caso]".
- *Por ejemplo, "Fitness Funds recopila datos de ubicación para activar el seguimiento de entrenamientos, incluso cuando la aplicación esté cerrada o no esté en uso, y también se usa para respaldar la publicidad".*
- *Por ejemplo, "Call buddy recopila datos del registro de llamadas de lectura y escritura para permitir la organización de contactos, incluso cuando no se usa la aplicación".*

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

- Una app que recopila la ubicación del dispositivo, pero no tiene una divulgación destacada que explique qué función usa estos datos ni indica el uso de la aplicación en segundo plano
- Una app que tiene un permiso de tiempo de ejecución que solicita acceso a datos **antes** de la divulgación destacada que especifica para qué se usan los datos
- Una app que accede al inventario de aplicaciones instaladas de un usuario y no trata estos datos como 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 de Acceso a Datos Personales y Sensibles

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

Actividad	Requisito
Su aplicación administra información financiera o de pago, o bien números de identificación nacional	Su aplicación nunca debe divulgar públicamente datos personales ni sensibles de los usuarios relacionados con actividades financieras o de pago, ni números de identificación nacional.
Su aplicación administra información de contacto o de agendas telefónicas no públicas	No permitimos la divulgación ni la publicación de los contactos no públicos de los usuarios.
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 aplicación debe publicar una política de privacidad que, junto con cualquier otro aviso de divulgación integrado, explique detalladamente qué datos del usuario se recopilan y transmiten, cómo se usan y con quién se comparten.
Su aplicación se orienta a niños	Su aplicación no debe incluir un SDK que no esté aprobado para usarse en servicios dirigidos a niños. Para conocer el texto y los requisitos completos de la política, consulte Cómo diseñar aplicaciones para niños y familias .
Su aplicación recopila o vincula identificadores de dispositivos persistentes (p. ej., IMEI, IMSI, número de serie de SIM, etc.)	Los identificadores de dispositivos persistentes no pueden vincularse a otros datos personales y sensibles de los usuarios, ni a identificadores de dispositivos que se puedan restablecer, excepto para los siguientes fines: • Telefonía vinculada a una identidad de SIM (p. ej., llamadas mediante Wi-Fi vinculadas a la cuenta del proveedor) • Aplicaciones de administración de dispositivos empresariales que usen el modo de propietario del dispositivo Estos usos se deben divulgar de forma destacada para los usuarios según se especifica en la Política de Datos del Usuario . Para conocer identificadores únicos alternativos, consulte este recurso . Si desea consultar otros lineamientos sobre el ID de Publicidad de Android, lea la política de Anuncios .

Sección de Seguridad de los datos

Todos los desarrolladores deben completar una sección clara y precisa de Seguridad de los datos para cada aplicación en la que se detalle el uso, la recopilación y el uso compartido de datos de los usuarios. El desarrollador es responsable de la exactitud de la etiqueta, así como de mantener esta información actualizada. Cuando corresponda, la sección debe ser coherente con las divulgaciones que se incluyan en la política de privacidad de la aplicación.

Consulte este artículo a fin de obtener información adicional para completar la sección de Seguridad de los datos.

Política de Privacidad

Todas las aplicaciones deben publicar un vínculo a una política de privacidad en el campo designado de Play Console, así como un vínculo a una política de privacidad o el texto correspondiente dentro de la aplicación en sí. En la política de privacidad, junto con cualquier otro aviso de divulgación de datos integrado en la aplicación, se debe explicar detalladamente cómo se recopilan, usan y comparten los datos del usuario, y cómo se accede a ellos, lo que incluye los datos divulgados en la etiqueta de privacidad. Se debe incluir lo siguiente:

- Información del desarrollador y un punto de contacto para temas relacionados con la privacidad o un mecanismo para enviar consultas
- Divulgación de los tipos de datos personales y sensibles de los usuarios a los que accede su aplicación y que esta recopila, usa y comparte, así como las partes con las que se comparten esos datos
- Procedimientos de manipulación segura de datos personales y sensibles de los usuarios
- La política del desarrollador relacionada con la retención y eliminación de datos
- Un etiquetado claro de la política de privacidad (por ejemplo, indicado como "política de privacidad" en el título)

La entidad (por ejemplo, el desarrollador, la empresa) mencionada en la ficha de Google Play de la aplicación debe aparecer en la política de privacidad, o la aplicación se debe nombrar en la política de privacidad. Las aplicaciones que no accedan a datos personales ni sensibles de los usuarios igualmente deben enviar una política de privacidad.

Asegúrese de que su política de privacidad esté disponible en una URL activa, accesible públicamente, sin geovallado (no en PDF) y que no se pueda editar.

Uso del ID del Conjunto de Aplicaciones

Android implementará un nuevo ID para abordar los casos de uso fundamentales, como el análisis y la prevención de fraudes. Las condiciones para el uso de este ID se encuentran a continuación.

- **Uso**: El ID del conjunto de aplicaciones no debe usarse para la personalización ni la medición de anuncios.
- **Asociación con información de identificación personal u otros identificadores:** El ID del conjunto de aplicaciones no debe estar conectado con identificadores de Android (p. ej., AAID) ni datos sensibles y personales con fines de publicidad.
- **Transparencia y consentimiento:** La recopilación y el uso del ID del conjunto de aplicaciones, y el compromiso con estas condiciones deben darse a conocer a los usuarios en un aviso de privacidad legalmente adecuado, lo que incluye su política de privacidad. Cuando se requiera, debe obtener el consentimiento de los usuarios con validez legal. Para obtener información sobre nuestros estándares de privacidad, revise nuestra política de Datos del Usuario .

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

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 haya originado 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.

A partir del 16 de julio de 2020, Google dejará de basarse en el EU-U.S. Privacy Shield (Escudo de Privacidad UE-EE.UU.) para transferir datos personales que se hayan originado en el Espacio Económico Europeo o el Reino Unido hacia los Estados Unidos. (Obtén más información.)Encontrarás más información en la sección 9 del DDA.

Permisos y API que Acceden a Información Sensible

Las solicitudes de permisos y el uso de API que accedan a información sensible deben tener sentido para los usuarios. Solo puede solicitar permisos y usar API que accedan a información sensible siempre y cuando estos sean necesarios para implementar funciones o servicios existentes en su aplicación que se promuevan en la ficha de Google Play. Se prohíbe el uso de permisos o API que accedan a información sensible que otorguen 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 o API que accedan a información sensible.

Solicite permisos y use API que accedan a información sensible para tener acceso a los datos en contexto (mediante solicitudes incrementales), de modo que los usuarios comprendan por qué su aplicación los solicita o usa. Use los datos solo con los fines para los que el usuario haya otorgado consentimiento. Si más adelante desea usar los datos para otros fines, debe solicitar el permiso de los usuarios y asegurarse de que acepten los propósitos adicionales.

Permisos Restringidos

Además de lo anterior, los permisos restringidos son aquellos que se designan como Riesgosos , Especiales , de Firma o según se documenta a continuación. Estos permisos 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 aplicación que recopiló esos datos. También puede transferir datos cuando sea necesario para cumplir con la legislación aplicable o como parte de una fusión, adquisición o venta de activos, habiendo proporcionado una notificación legal adecuada a los usuarios. Se prohíben todas las demás transferencias o ventas de los datos de los usuarios.
- Se debe respetar la decisión de los usuarios si rechazan una solicitud de permisos restringidos; no se debe manipular ni forzar a los usuarios para que den su consentimiento a cualquier permiso que no sea crítico. Se deben realizar todos los esfuerzos razonables para ajustar el contenido a los usuarios que no otorguen acceso a permisos sensibles (p. ej., permitir que un usuario ingrese un número de teléfono de forma manual si restringió el acceso a los Registros de llamadas).
- Se prohíbe expresamente el uso de permisos en contra de las prácticas recomendadas oficiales para desarrolladores de Android acerca de los permisos de las aplicaciones o que infrinjan las políticas existentes (incluido el Abuso de Privilegios Elevados).

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

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

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

Permisos de Ubicación

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 , a la política de Ubicación en Segundo Plano y a los siguientes requisitos:

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

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

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

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

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

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

Permiso "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 aplicaciones 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 aplicación.
- Los dispositivos Android que ejecuten la versión R o una posterior requerirán el permiso MANAGE_EXTERNAL_STORAGE para administrar el acceso en el almacenamiento compartido. Todas las aplicaciones que se orienten a Android R y soliciten 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 .

Permiso de Visibilidad de Paquetes (Aplicaciones)

Cuando se consulta el inventario de aplicaciones instaladas desde un dispositivo, dicho contenido se considera información sensible y personal del usuario, y está sujeto a la política de Información Personal y Sensible , así como a los requisitos que se detallan a continuación.

Las aplicaciones que tienen como propósito principal lanzar o explorar otras aplicaciones del dispositivo, o interoperar con ellas, pueden obtener visibilidad apropiada para el alcance de otras aplicaciones instaladas en el dispositivo, como se describe a continuación:

- **Visibilidad amplia de la aplicación:** La visibilidad amplia es la capacidad de una aplicación para tener una visibilidad extensa (o "amplia") de las aplicaciones instaladas ("paquetes") en un dispositivo.
  - En el caso de las aplicaciones segmentadas al nivel de API 30 o niveles superiores , la visibilidad amplia de las aplicaciones instaladas mediante el permiso QUERY_ALL_PACKAGES está restringida a casos de uso específicos en los que el conocimiento de las aplicaciones del dispositivo o la interoperabilidad con ellas son necesarios para que funcione la aplicación.
    - No puede usar QUERY_ALL_PACKAGES si su aplicación puede funcionar con una declaración de visibilidad de paquetes específicos segmentada más limitada (p. ej., consultar paquetes específicos e interactuar con ellos en lugar de solicitar una visibilidad amplia).
  - El uso de métodos alternativos para aproximar el nivel de visibilidad amplia asociado con el permiso QUERY_ALL_PACKAGES también está restringido a la funcionalidad principal para el usuario de la aplicación y la interoperabilidad con las aplicaciones que se detecten a través de este método.

- Si desea conocer los casos de uso admisibles para el permiso QUERY_ALL_PACKAGES, consulte este artículo del Centro de ayuda .

- **Visibilidad limitada de la aplicación**: La visibilidad limitada ocurre cuando una aplicación minimiza el acceso a los datos mediante búsquedas de aplicaciones específicas con métodos más puntuales (en lugar de métodos "amplios"), como búsquedas de aplicaciones específicas que satisfacen la declaración del manifiesto de la aplicación. Puede usar este método para realizar búsquedas de aplicaciones en los casos en que su aplicación tenga interoperabilidad en cumplimiento con las políticas o esté a cargo de la administración de esas aplicaciones.
- La visibilidad del inventario de las aplicaciones instaladas en un dispositivo debe estar directamente relacionada con el propósito o la funcionalidad principales a los que acceden los usuarios en su aplicación.

Los datos de inventario de las aplicaciones que se consultan desde las aplicaciones distribuidas en Play no se pueden vender ni compartir con fines de análisis o monetización de anuncios.

Accessibility API

No se puede usar la API de Accessibility para los siguientes fines:

- Cambiar los parámetros de configuración de los usuarios sin su permiso o impedir la posibilidad de que los usuarios inhabiliten o desinstalen cualquier aplicación o servicio, a menos que se cuente con la autorización de una madre, un padre o un tutor en una aplicación de control parental o de administradores autorizados en un software de administración empresarial
- Ignorar las notificaciones y los controles de privacidad integrados de Android
- Cambiar la interfaz de usuario o sacar provecho de ella de una manera engañosa o que de otro modo incumpla las Políticas para Desarrolladores de Google Play

La API de Accessibility no se puede solicitar para realizar grabaciones de audio de llamadas remotas, ya que no está diseñada para tal fin.

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

Lineamientos para el uso de la etiqueta IsAccessibilityTool

Las aplicaciones cuya funcionalidad principal pretenda brindar asistencia directa a las personas con discapacidades son aptas para usar la etiqueta **IsAccessibilityTool** a fin de designarse públicamente como aplicaciones de accesibilidad de forma adecuada.

Las aplicaciones que no sean aptas para usar **IsAccessibilityTool** no pueden usar la etiqueta y deben cumplir con los requisitos de consentimiento y divulgación destacada que se describen en la política de Datos del Usuario debido a que la función de accesibilidad no es obvia para el usuario. Para obtener más información, consulte el artículo del Centro de ayuda sobre la API de AccessibilityService .

Cuando sea posible, las aplicaciones deben usar API y permisos con alcances más restringidos en lugar de la API de Accesibility a fin de lograr la funcionalidad deseada.

En vigencia a partir del 29 de septiembre de 2022

Permiso Solicitar Paquetes de Instalación

El permiso REQUEST_INSTALL_PACKAGES autoriza a la aplicación a solicitar la instalación de los paquetes correspondientes. Para usar este permiso, la funcionalidad principal de su aplicación debe incluir lo siguiente:

- Envío o recepción de paquetes de aplicación
- Habilitación de instalaciones iniciadas por el usuario de paquetes de aplicación

Las funcionalidades permitidas incluyen las siguientes:

- Búsqueda o navegación web

- Servicios de comunicación que admiten archivos adjuntos
- Uso compartido, transferencia o administración de archivos
- Administración de dispositivos empresariales

La funcionalidad principal se define como el objetivo más importante de la aplicación. La funcionalidad principal, así como cualquier otra función importante que la constituya, deben documentarse de forma destacada y promoverse en la descripción de la aplicación.

El permiso REQUEST_INSTALL_PACKAGES no debe usarse para realizar actualizaciones automáticas, modificaciones o implementaciones de paquetes de otros APK en el archivo de activos, a menos que sea con fines de administración de dispositivos. Todas las actualizaciones o instalaciones de paquetes deben estar sujetas a la política de Abuso de Redes y Dispositivos de Google Play, y el usuario es quien debe iniciarlas.

Entrada en vigencia: 1 de noviembre de 2022

Servicio de VPN

VPNService es una clase básica para que las aplicaciones extiendan y compilen sus propias soluciones de VPN. Únicamente las aplicaciones que usan VPNService y tienen una VPN como su funcionalidad principal pueden crear un túnel seguro a nivel del dispositivo hacia un servidor remoto. Entre las excepciones se incluyen las aplicaciones que requieren un servidor remoto para la funcionalidad principal, como las siguientes:

- Aplicaciones de administración empresarial y control parental
- Opciones de seguimiento de uso de aplicaciones
- Aplicaciones de seguridad del dispositivo (por ejemplo, antivirus, administración de dispositivos móviles, firewall)
- Herramientas relacionadas con redes (por ejemplo, acceso remoto)
- Aplicaciones de navegación web
- Aplicaciones del operador que requieren el uso de funciones de la VPN para proporcionar servicios de conectividad o telefonía

VPNService no se puede usar para lo siguiente:

- Recopilar datos personales y sensibles de los usuarios sin su consentimiento y una divulgación destacada
- Redireccionar o manipular el tráfico de otras aplicaciones en un dispositivo con fines de monetización (por ejemplo, redireccionar el tráfico de anuncios por un país que no sea el del usuario)
- Manipular anuncios que puedan afectar la monetización de las aplicaciones

Las aplicaciones que usan VPNService deben hacer lo siguiente:

- Documentar el uso de VPNService en la ficha de Google Play
- Encriptar los datos que van del dispositivo al extremo del túnel de la VPN
- Cumplir con todas las Políticas del Programa para Desarrolladores, incluidas las políticas de Fraude Publicitario, Permisos y Software Malicioso.

Entrada en vigencia: 31 de julio de 2023

Permiso de Alarmas Exactas

Se implementará un nuevo permiso, USE_EXACT_ALARM, que otorgará acceso a la funcionalidad de alarmas exactas en las aplicaciones a partir de Android 13 (nivel de API objetivo 33).

USE_EXACT_ALARM es un permiso restringido, y las aplicaciones solo deben declarar este permiso si su funcionalidad principal admite la necesidad de una alarma exacta. Las aplicaciones que solicitan

este permiso restringido están sujetas a revisión, y no se permitirá la publicación en Google Play de las que no cumplan con los criterios de casos de uso aceptables.

Casos de uso aceptables para utilizar el Permiso de Alarmas Exactas

Su aplicación debe usar la funcionalidad de USE_EXACT_ALARM únicamente cuando la funcionalidad principal del lado del usuario requiera acciones con tiempos precisos, como en los siguientes ejemplos:

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

Si tiene un caso de uso para la funcionalidad de alarma exacta que no está abarcado más arriba, debe evaluar si el uso de SCHEDULE_EXACT_ALARM como alternativa es una opción.

Para obtener más información sobre la funcionalidad de alarma exacta, consulte esta orientación para desarrolladores .

Abuso de redes y dispositivos

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

Las apps que se publiquen en Google Play deben cumplir con los requisitos de optimización del sistema Android predeterminado documentados en los lineamientos de calidad de las apps en Google Play .

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

Las aplicaciones o código de terceros (p. ej., SDK) con lenguajes interpretados (JavaScript, Python, Lua, etc.) que se cargan durante el tiempo de ejecución (p. ej., que no se incluyen junto con la aplicación) no deben permitir que se incumplan las políticas de Google Play.

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 informaron a los desarrolladores.

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

- Aplicaciones que bloquean o interfieren con otra app debido a la exhibición de anuncios
- Aplicaciones de trucos de juegos que afectan la experiencia de juego en otras aplicaciones.
- Aplicaciones 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)

- Aplicaciones 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
- Aplicaciones que se vinculan a la distribución o instalación de software malicioso, o facilitan estas prácticas
- Aplicaciones o código de terceros (p. ej., SDK) en los que haya WebViews que contengan la interfaz de JavaScript y carguen contenido web que no sea de confianza (p. ej., URL http://) o URL sin verificar provenientes de fuentes no confiables (p. ej., URL obtenidas con intents que no sean de confianza)

Entrada en vigencia: 1 de noviembre de 2022

Requisitos de Flag Secure

FLAG_SECURE es un parámetro de visualización declarado en el código de una app para indicar que su IU contiene datos sensibles que tienen la intención de limitarse a una superficie segura mientras se usa la app. Este parámetro está diseñado para evitar que los datos aparezcan en capturas de pantalla o que se visualicen en pantallas no seguras. Los desarrolladores declaran este parámetro cuando no se debe anunciar, declarar o transmitir de otro modo el contenido de la app fuera de ella o del dispositivo del usuario.

Por cuestiones de seguridad y privacidad, todas las aplicaciones que se distribuyen en Google Play deben respetar la declaración de FLAG_SECURE de otras aplicaciones. Esto significa que las aplicaciones no deben facilitar ni crear métodos alternativos para evitar la configuración de FLAG_SECURE en otras aplicaciones.

Las apps que califican como Herramienta de accesibilidad son una exención de este requisito, siempre y cuando no transmitan, guarden ni almacenen en caché el contenido protegido con FLAG_SECURE para que se acceda a él fuera del dispositivo del usuario.

Comportamiento engañoso

No se permiten 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 modificación en la configuración del dispositivo debe realizarse con el conocimiento y consentimiento del usuario, y este debe poder revertirla.

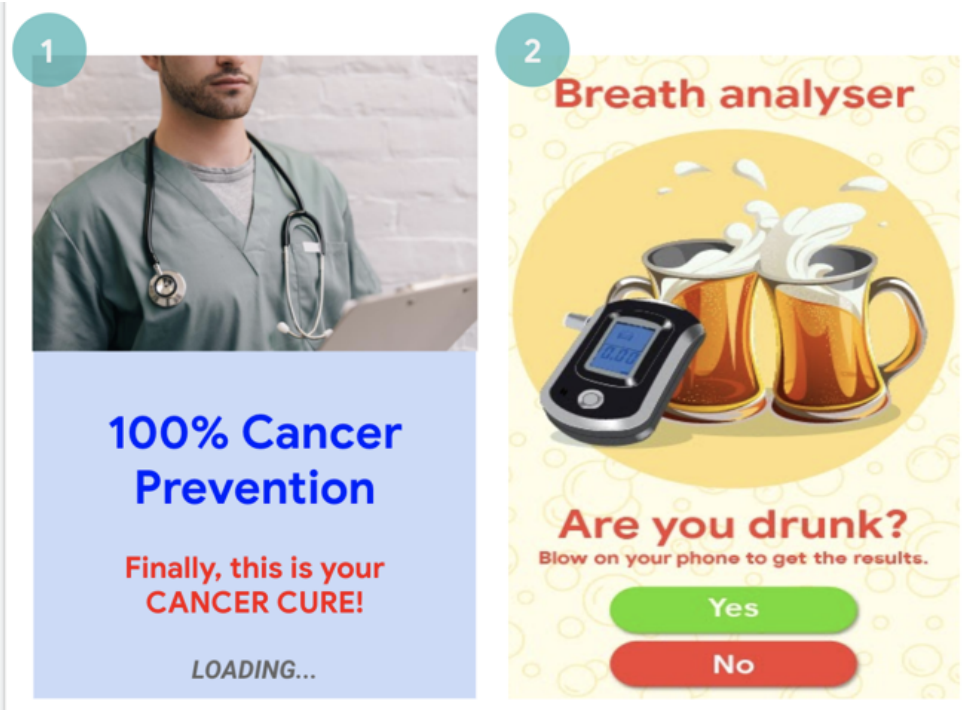
Afirmaciones Engañosas

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

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

- Aplicaciones que tergiversen o no describan de forma precisa y clara su funcionalidad:
  - Una aplicación que afirma ser un juego de carreras en la descripción y en las capturas de pantalla, pero que en realidad es un juego de estrategia que usa la imagen de un automóvil
  - Una aplicación que afirme ser un antivirus, pero solo tenga texto que explica cómo quitar virus
- Aplicaciones que afirmen tener funciones que no se pueden implementar (p. ej., aplicaciones repelentes de insectos), incluso si se representan como bromas, falsificaciones, chistes, etc.
- Aplicaciones que se categoricen de forma incorrecta, lo que incluye, sin limitaciones, que tengan una clasificación o una categoría de app errónea

- Contenido engañoso comprobable o falso que podría interferir con los procesos de votación
- Aplicaciones que afirmen falsamente mantener algún vínculo con una entidad gubernamental o proporcionar o facilitar servicios gubernamentales para los cuales no están debidamente autorizadas
- Aplicaciones que afirman falsamente ser la aplicación oficial de una entidad establecida (no se permite usar títulos como "Oficial de Justin Bieber" sin los permisos ni 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 se permiten aplicaciones que modifiquen la configuración o las funciones del dispositivo del usuario fuera de la aplicación sin el conocimiento y consentimiento del usuario. Las funciones y la configuración del dispositivo incluyen la configuración del sistema y el navegador, los marcadores, las combinaciones de teclas, los íconos, los widgets y la presentación de las apps en la pantalla principal.

Tampoco permitimos lo siguiente:

- Apps que modifiquen la configuración o las funciones con el consentimiento del usuario, pero 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
- Aplicaciones que fomentan o incentivan a los usuarios a que quiten o inhabiliten apps de terceros, o modifiquen la configuración o las funciones del dispositivo, a menos que sean parte de un servicio de seguridad comprobable

Prácticas que Fomentan un Comportamiento Fraudulento

No permitimos aplicaciones que faciliten que los usuarios engañen a otros ni que sean funcionalmente engañosas, incluidas, sin limitaciones, las aplicaciones que generen o faciliten la creación de tarjetas de identificación, números de seguridad social, pasaportes, diplomas, tarjetas de crédito, cuenta

bancarias y licencias de conducir. Las aplicaciones deben brindar información, títulos, descripciones, imágenes y videos precisos respecto de las funciones o el contenido que ofrecen, y funcionar de manera razonable y correcta tal como lo espera el usuario.

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

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

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

- 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 dependan 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 guíen al usuario ni indiquen el tamaño de la descarga antes de que se inicie el proceso

Manipulación de Contenido Multimedia

No se permiten aplicaciones que promuevan o ayuden a crear información falsa o engañosa, ni afirmaciones transmitidas a través de imágenes, videos o texto. No se permiten 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.

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

- Aplicaciones que agregan una figura pública a una protesta durante un evento políticamente sensible
- 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 (por ejemplo, pero sin limitarse a ello, las que ocultan o tergiversan su país de origen y dirigen su contenido a usuarios de otro país)
- 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

---

Entrada en vigencia: 1 de noviembre de 2022

Política de Nivel de API Objetivo de Google Play

A fin de proporcionarles una experiencia segura a los usuarios, Google Play requiere los siguientes niveles de API objetivo para **todas las aplicaciones**:

Las **aplicaciones nuevas y las actualizaciones DEBEN** orientarse a un nivel de API de Android que no supere el año de antigüedad respecto del lanzamiento de la versión principal de Android más reciente. No se podrán enviar a Play Console las aplicaciones nuevas o las actualizaciones que no cumplan con este requisito.

Las aplicaciones existentes de Google Play que no estén actualizadas y que no se orienten a un nivel de API con dos años de antigüedad o menos respecto del lanzamiento de la versión principal más reciente de Android no estarán disponibles para los usuarios nuevos que tengan dispositivos con versiones más nuevas del SO Android. Los usuarios que hayan instalado las aplicaciones con anterioridad desde Google Play aún podrán encontrarlas, volver a instalarlas y usarlas en cualquier versión del SO Android compatible con esas aplicaciones.

Para recibir asesoramiento técnico sobre el cumplimiento del requisito de nivel de API objetivo, consulte la guía de migración .

Para conocer los plazos exactos, consulte este artículo del Centro de ayuda .

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 .

Puerta trasera

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

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

resultado, en determinadas circunstancias, Google Play Protect trata a un subconjunto de puertas traseras como una vulnerabilidad.

Fraude en la facturación

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

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

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

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

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

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

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

Entrada en vigencia: 15 de febrero de 2023

Stalkerware

Código que recopila datos personales o sensibles de los usuarios de un dispositivo y los transmite a un tercero (empresa o persona física) con fines de supervisión.

Las aplicaciones deben proporcionar una divulgación destacada adecuada y obtener el consentimiento según lo exige la política de Datos del Usuario .

Lineamientos para las Aplicaciones de Supervisión

Las aplicaciones diseñadas y comercializadas exclusivamente para supervisar a otra persona, por ejemplo, para que los padres vigilen a sus hijos o los administradores empresariales supervisen a sus empleados, son las únicas aplicaciones de supervisión 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. Estas aplicaciones deben usar el parámetro de metadatos IsMonitoringTool en el archivo del manifiesto para designarse correctamente como aplicaciones de supervisión.

Las aplicaciones de supervisión deben satisfacer estos requisitos:

- No deben presentarse como una solución de espionaje ni vigilancia secreta.

- Las aplicaciones no deben ocultar ni encubrir el comportamiento relacionado con el seguimiento, 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 deben divulgar la funcionalidad de supervisión o seguimiento en la descripción de Google Play Store.
- Las aplicaciones y fichas que se muestran en Google Play no deben proporcionar ningún medio para activar o acceder a funcionalidades que incumplan estos términos y condiciones, como vínculos a archivos APK alojados fuera de Google Play que no satisfagan dichos términos.
- Las aplicaciones deben satisfacer todas las leyes aplicables. La responsabilidad de determinar la legalidad de la aplicación en el mercado de destino recae exclusivamente sobre usted.

Denegación del servicio (DoS)

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

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

Aplicaciones de descarga hostil

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

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

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

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

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

Amenaza no relacionada con Android

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

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

Suplantación de identidad (phishing)

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

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

Abuso de privilegios altos

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

Los siguientes son algunos ejemplos:

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

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

Ransomware

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

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

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

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

Modificación de dispositivos para obtener permisos de administrador

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

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

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

Spam

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

Software espía

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

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

- Lista de contactos
- Fotos y otros archivos que se guardan en la tarjeta SD, o que no pertenecen a la aplicación
- Contenido del correo electrónico del usuario

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

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

Troyano

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

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

Una nota sobre aplicaciones poco comunes

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

Una nota sobre la categoría de puerta trasera

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

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

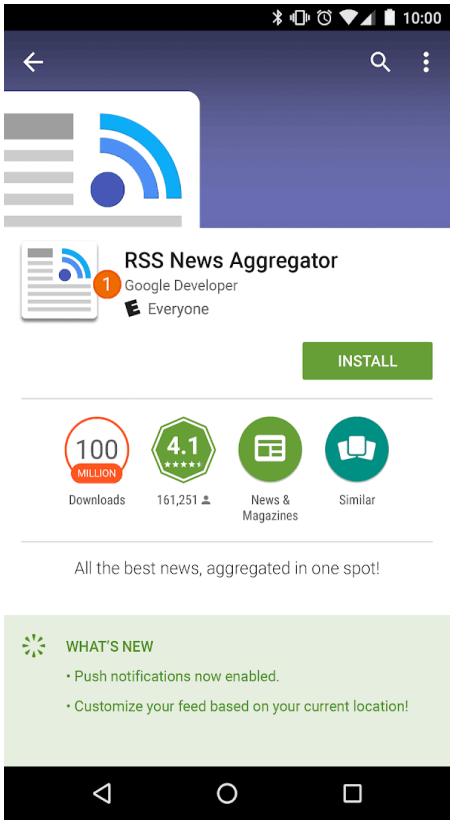
En vigencia a partir del 31 de agosto de 2022

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 insinúes que tu app está relacionada con otra persona ni autorizada por ella si no es verdad. Ten cuidado de no usar íconos, descripciones, títulos o elementos integrados en la app que puedan engañar a los usuarios sobre la relación de tu app con otra persona o con otra app.

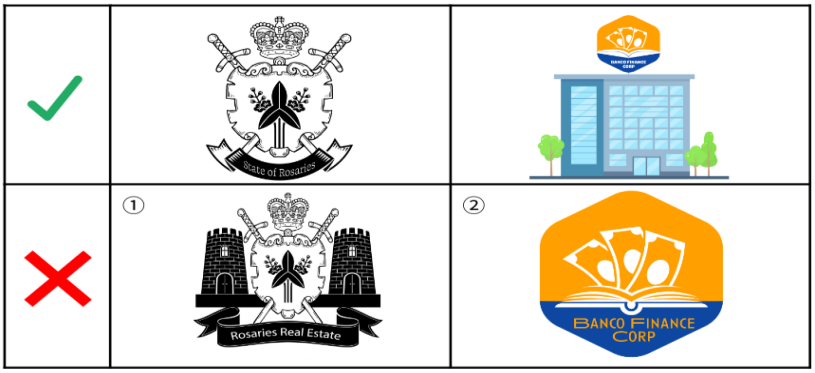
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Desarrolladores que insinúan falsamente una relación con otra empresa, desarrollador, organización o entidad



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

- Aplicaciones cuyos íconos y títulos impliquen falsamente una relación con otra empresa, desarrollador, organización o entidad



① La aplicación usa un emblema nacional y engaña a los usuarios para que crean que tiene una afiliación con el Gobierno.
② La aplicación copia el logotipo de una entidad de negocio para sugerir falsamente que es una aplicación oficial de ese negocio.

- Íconos y títulos de aplicaciones que son tan parecidos a los de otros productos o servicios existentes que pueden confundir a los usuarios

① La aplicación usa el logotipo de un sitio web popular de criptomonedas en su ícono para sugerir que es el sitio web oficial.
② La aplicación copia el personaje y el título de un programa de TV famoso en su ícono y engaña a los usuarios para que crean que tiene una afiliación con ese programa de TV.

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

---

Mobile Unwanted Software

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 del usuario, y tomaremos medidas para proteger a los usuarios al respecto.

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 que se hacen al usuario. Las aplicaciones deben proporcionar toda la funcionalidad comunicada y 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
- Ingeniería social

Proteja los datos del usuario

Sea claro y transparente sobre el acceso, la utilización, la recopilación y el uso compartido de datos personales y sensibles del usuario. Cuando corresponda, el uso de los datos del usuario debe cumplir con todas las Políticas de Datos del Usuario pertinentes 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 (consulte Software espía)
- Abuso de permisos restringidos

Ejemplo de políticas de datos del usuario:

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

No afecte de forma negativa la experiencia en dispositivos móviles

La experiencia del usuario debe ser directa y fácil de entender, y basarse en decisiones claras del usuario. Debe presentar una propuesta de valor clara al usuario y no interrumpir la experiencia

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

Aplicaciones de Descarga Hostil

Se trata de código que no es en sí software no deseado, pero que descarga otro tipo de software no deseado para dispositivos móviles (MUwS).

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

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

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

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

Fraude publicitario

Se prohíbe estrictamente el fraude publicitario. 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.

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

- Una 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

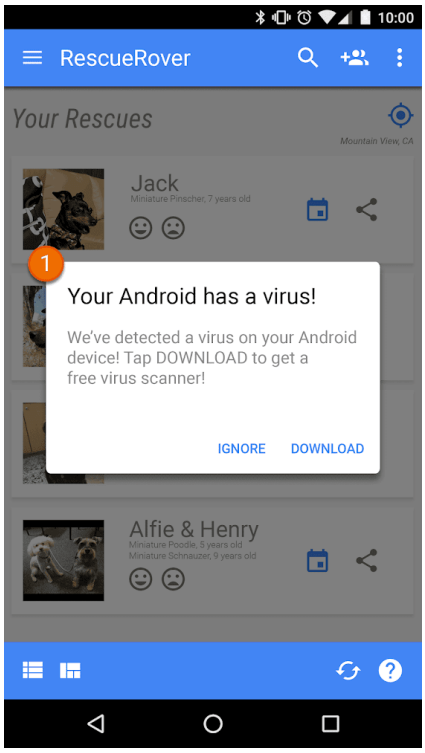
- Declaraciones falsas del inventario de anuncios de una app, p. ej., una app que comunica a las redes de publicidad que se ejecuta en un dispositivo iOS cuando en realidad lo hace en Android o una app que tergiversa el nombre del paquete que se está monetizando

Uso no autorizado o imitación de las funciones del sistema

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

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

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



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

Para ver más ejemplos que incluyan anuncios, consulta la política de Anuncios.

Social Engineering

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

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

Google Play admite varias estrategias de monetización en beneficio de los desarrolladores y usuarios, como la distribución paga, los productos integrados en la aplicación, las suscripciones y los modelos

basados en anuncios. Para garantizar la mejor experiencia del usuario, le solicitamos que cumpla con estas políticas.

Pagos

1. Los desarrolladores que cobran por descargar aplicaciones de Google Play deben usar el sistema de facturación de Google Play como forma de pago para esas transacciones.
2. Las aplicaciones distribuidas por Play que requieran o acepten pagos para acceder a funciones o servicios integrados en la aplicación, incluidos el contenido y los bienes digitales, así como cualquier funcionalidad de la aplicación (en conjunto, "compras directas desde la aplicación"), deben usar el sistema de facturación de Google Play para esas transacciones, a menos que se apliquen el Artículo 3 o el Artículo 8.

   Entre los ejemplos de funciones o servicios de la aplicación que requieren el uso del sistema de facturación de Google Play, se incluyen, entre otros, las compras directas desde la app de lo siguiente:

   - artículos (como monedas virtuales, vidas adicionales, tiempo de juego adicional, elementos complementarios, personajes y avatares)
   - servicios de suscripción (como los relacionados con entrenamiento físico, juegos, citas, educación, música, videos, actualizaciones de servicios y otros tipos de contenido)
   - funcionalidad o contenido de la aplicación (como una versión sin anuncios de una aplicación 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)

3. El sistema de facturación de Google Play no debe utilizarse en los siguientes casos:
   a. cuando el pago tiene principalmente uno de estos fines:
      - la compra o el alquiler de bienes físicos (como comestibles, ropa, artículos para el hogar o artículos electrónicos)
      - la compra de servicios físicos (como servicios de transporte, servicios de limpieza, pasajes de avión, membresías de gimnasio, envío de comida o 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)

   b. pagos que incluyen transacciones entre pares, subastas en línea y donaciones exentas de impuestos
   c. 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
   d. pagos relacionados con cualquier categoría de producto que se considere inaceptable según las Políticas de Contenido del Centro de Pago de Google

      Nota: En algunos mercados, ofrecemos Google Pay para apps que venden bienes físicos o servicios. Para obtener más información, visite nuestra página de Google Pay para desarrolladores.

4. Aparte de las condiciones que se describen en el Artículo 3 y el Artículo 8, las aplicaciones no pueden conducir a los usuarios a una forma de pago que no sea el sistema de facturación de Google Play. Esta prohibición incluye, entre otras restricciones, la posibilidad de dirigir a los usuarios a formas de pago alternativas a través de lo siguiente:
   - Una ficha de la aplicación 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

5. Las monedas virtuales integradas en la app solo pueden usarse dentro del título (juego o app) para el que se compraron.
6. 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 su 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.
7. Las aplicaciones 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.
8. A menos que se apliquen las condiciones que se describen en el Artículo 3, los desarrolladores de aplicaciones distribuidas por Play en teléfonos móviles y tablets que requieran o acepten pagos de los usuarios en Corea del Sur para acceder a compras directas desde la aplicación pueden ofrecer a los usuarios un sistema de facturación integrada, además del sistema de facturación de Google Play, para esas transacciones si completan correctamente el formulario de declaración de sistema de facturación integrada adicional y aceptan las condiciones adicionales y los requisitos del programa que se incluyen en ese documento.

Nota: Para ver los cronogramas y las preguntas frecuentes sobre esta política, visita nuestro Centro de ayuda.

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

No permitimos aplicaciones que contengan anuncios engañosos o invasivos. Los anuncios solo deben mostrarse dentro de la aplicación que los ofrece. Consideramos a los anuncios y sus ofertas asociadas publicadas en su aplicación como parte de ella. Los anuncios que se muestran en su aplicación deben satisfacer 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 aplicaciones que aumentan el uso de datos de ubicación del dispositivo basados en permisos para publicar anuncios están sujetas a la política de Información Personal y Sensible y también deben cumplir con los siguientes requisitos:

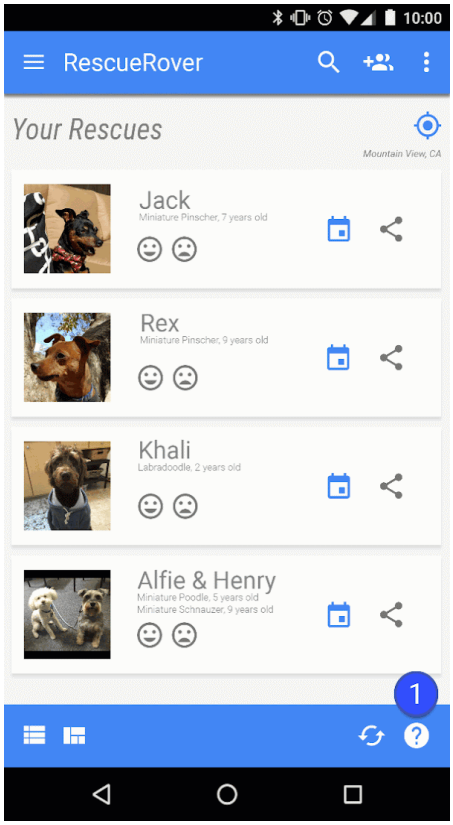
- El uso o la recopilación con fines publicitarios de los datos de ubicación del dispositivo basados en permisos deben estar claros para el usuario y documentados en la política de privacidad obligatoria de la aplicación, incluidos los vínculos a cualquier política de privacidad de redes publicitarias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

Anuncios Engañosos

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

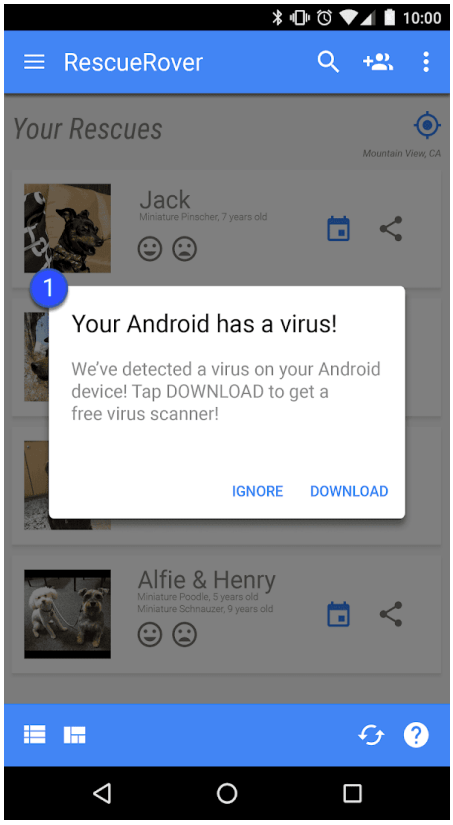
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

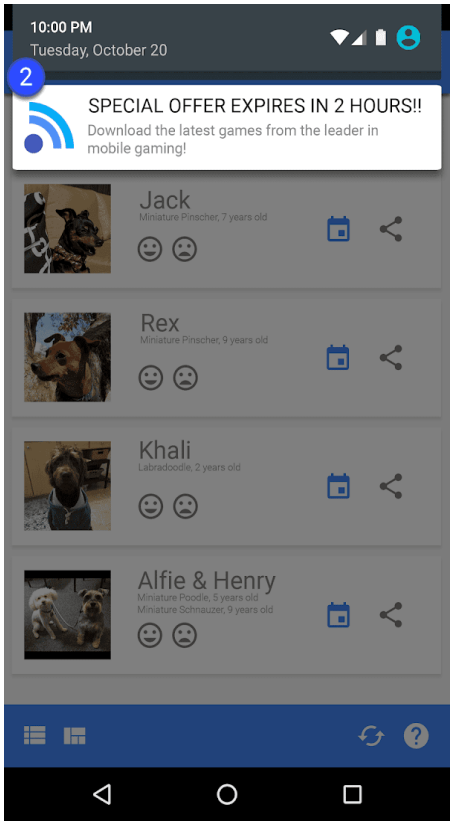
- Anuncios que imitan la IU de una aplicación:



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

- Anuncios que imitan una notificación del sistema:





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

Monetización de la Pantalla Bloqueada

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

Anuncios Invasivos

Los anuncios 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.

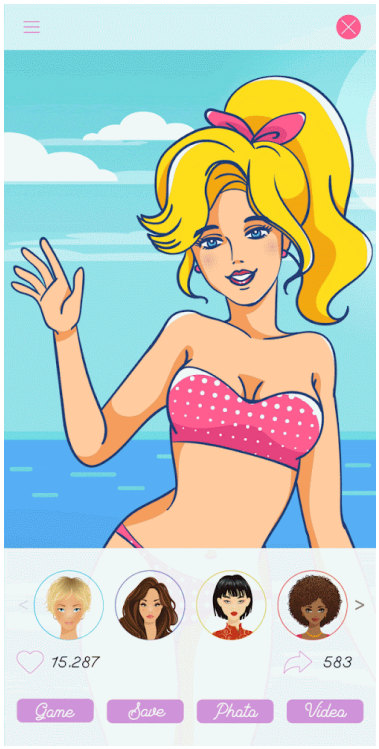
Tu app no puede obligar al usuario a hacer clic en un anuncio ni a enviar información personal con fines publicitarios antes de que pueda usarla por completo. Los anuncios intersticiales solo se pueden mostrar dentro de la app que los publica. Si tu app muestra anuncios intersticiales, o bien otros anuncios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

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

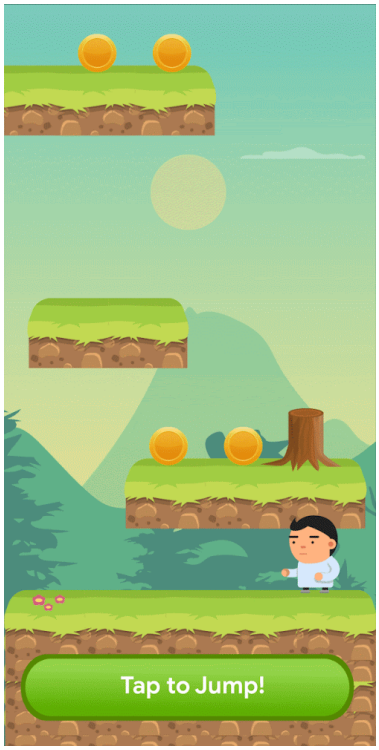
- Anuncios que ocupan toda la pantalla o interfieren con el uso normal y que no ofrecen una manera clara de descartar el anuncio:

① Este anuncio no tiene un botón para descartar

- 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 si el usuario suele presionar otra función



- Un anuncio que utiliza un botón para descartarlo falso



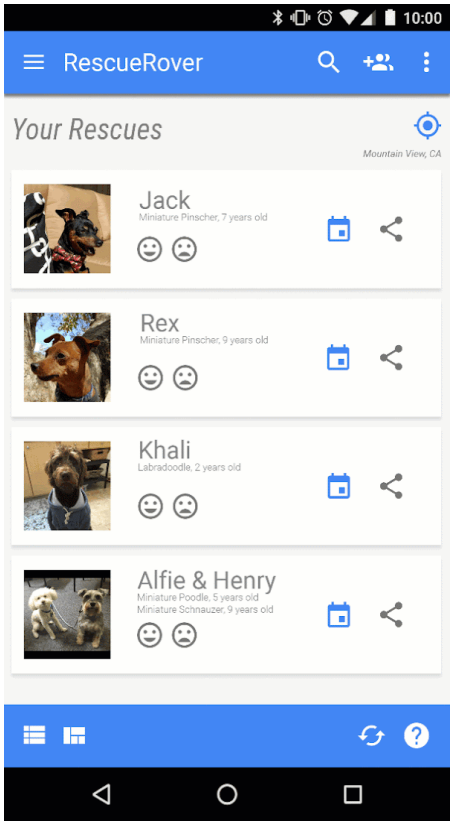
Un anuncio que aparece de repente en un área donde el usuario está acostumbrado a presionar para obtener funciones en la app

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

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

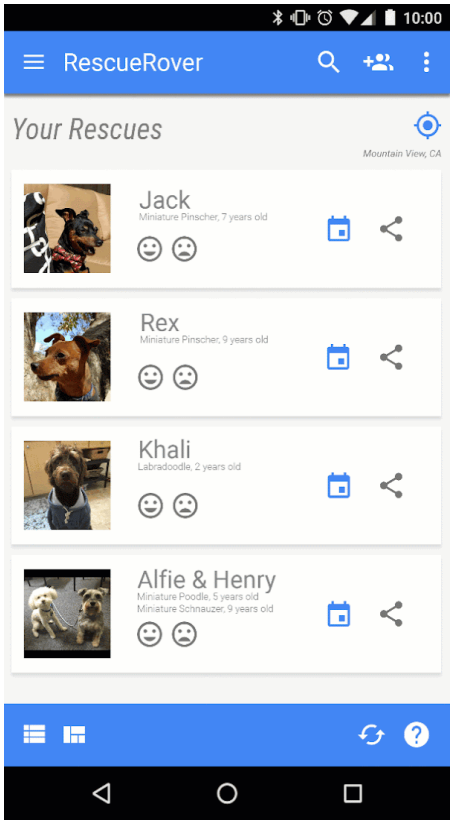
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

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



Descripción: El usuario navega a la pantalla principal desde esta app, 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 app:

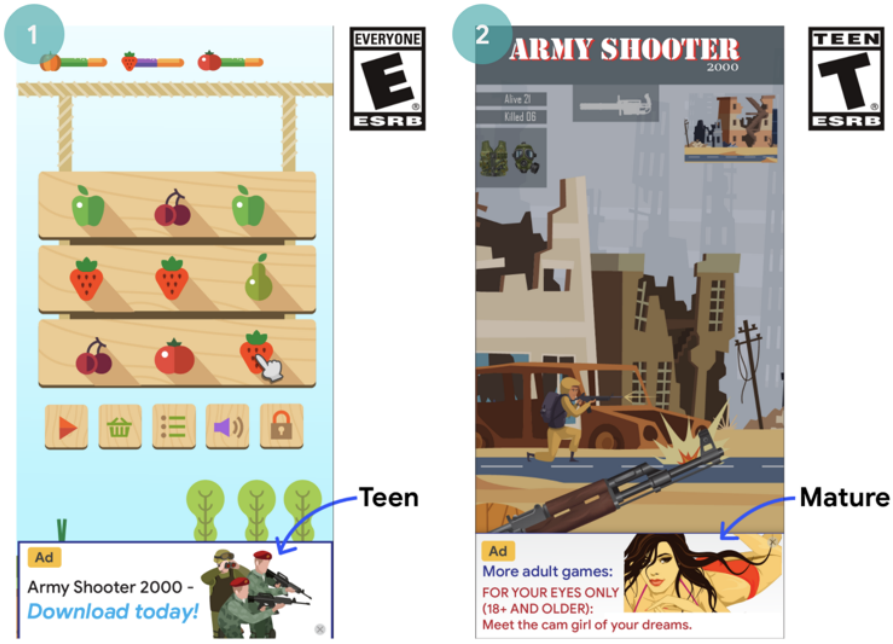


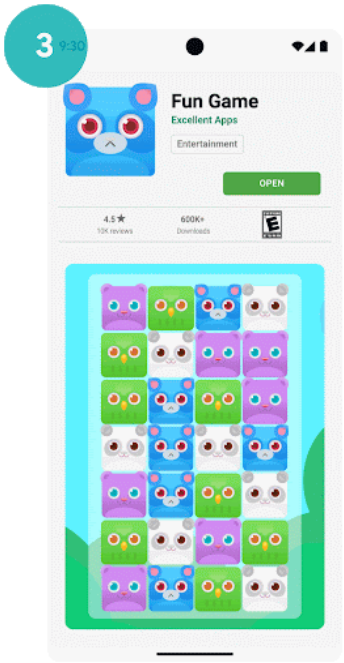
Descripción: El usuario intenta salir de la app y navegar a la pantalla principal, pero un anuncio interrumpe el flujo esperado.

Anuncios Inapropiados

Los anuncios y sus ofertas asociadas (por ejemplo, anuncios que promueven la descarga de otra aplicación) que se muestren dentro de su aplicación deben ser adecuados para la clasificación del contenido de su aplicación, incluso si el contenido en sí satisface nuestras políticas en otros aspectos.

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





① Este anuncio es inapropiado (Adolescentes) con respecto a la clasificación del contenido de la aplicación (Apta para todo público)
② Este anuncio es inapropiado (Adultos) con respecto a la clasificación del contenido de la aplicación (Adolescentes)
③ La oferta del anuncio (promoción de la descarga de una aplicación para Adultos) es inapropiada con respecto a la clasificación del contenido del juego en el que se mostró el anuncio (Apto para todo público)

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 (AAID) solo debe usarse para la publicidad y el análisis de los usuarios. El estado de la configuración para inhabilitar la publicidad basada en intereses o rechazar la personalización de anuncios se debe verificar cada vez que se ingrese el ID.
- **Asociación con información de identificación personal u 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 para estadísticas: El identificador de publicidad no puede estar conectado a información de identificación personal ni asociado con identificadores de dispositivos persistentes (por ejemplo, SSAID, dirección MAC, IMEI, etc.) para ningún fin relacionado con estadísticas. Para consultar otros lineamientos sobre los identificadores de dispositivos persistentes, lea la política de Datos 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.
  - Usted debe respetar los parámetros de configuración para inhabilitar la publicidad basada en intereses o rechazar la personalización de anuncios que haya seleccionado un usuario. Si un usuario habilitó esta configuración, usted no podrá usar el identificador de publicidad para crear perfiles de usuario con fines publicitarios ni para establecer la segmentación hacia los usuarios

con publicidad personalizada. Las actividades permitidas incluyen la publicidad contextual, la limitación de frecuencia, el seguimiento de conversiones, la generación de informes y la seguridad, y la detección de fraudes.
  - En los dispositivos nuevos, cuando un usuario borre el identificador de publicidad de Android, se quitará el identificador. Cuando se intente acceder a él, en su lugar se verá una string de ceros. Los dispositivos que no tengan un identificador de publicidad no deben conectarse a datos vinculados con un identificador de publicidad anterior ni derivados de él.
- **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 las Políticas del Programa para Desarrolladores de Google Play. Lo mismo se espera de cualquier tercero con quien se comparta durante el transcurso del negocio. Todas las aplicaciones que se suban a Google Play o se publiquen en esa plataforma deben usar el ID de publicidad (cuando esté disponible en el dispositivo) en lugar de cualquier otro identificador de dispositivo para fines publicitarios.

En vigencia a partir del 30 de septiembre de 2022

Experiencias de Better Ads

Los desarrolladores deben satisfacer los siguientes lineamientos para anuncios a fin de garantizar experiencias de alta calidad para los usuarios cuando usen aplicaciones de Google Play. Sus anuncios no deben mostrarse a los usuarios de las siguientes formas inesperadas:

- No se permiten los anuncios intersticiales de pantalla completa en ningún formato (video, GIF, estáticos, etc.) que se muestren de forma inesperada, por lo general cuando el usuario eligió realizar otra acción.
  - No se permiten los anuncios que aparecen durante el juego al principio de un nivel o durante el comienzo de un segmento de contenido.
  - No se permiten los anuncios intersticiales de video en pantalla completa que aparecen antes de la pantalla de carga de una aplicación (pantalla de presentación).
- No se permiten los anuncios intersticiales de pantalla completa en ningún formato que no se puedan cerrar después de 15 segundos. Los anuncios intersticiales de pantalla completa que incluyan una opción de habilitación o que no interrumpan a los usuarios en sus acciones (por ejemplo, después de la pantalla de puntuaciones en una aplicación de juego) pueden persistir más de 15 segundos.

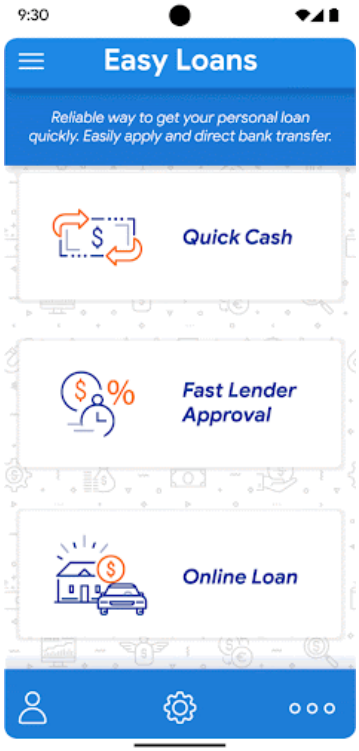
Esta política no se aplica a los anuncios recompensados que estén habilitados de forma explícita por los usuarios (por ejemplo, un anuncio que los desarrolladores ofrezcan mirar explícitamente a los usuarios a cambio de desbloquear una característica o contenido específico del juego). Esta política tampoco se aplica a la monetización ni a la publicidad que no interfiera con el uso normal de la aplicación o el juego (por ejemplo, contenido de video con anuncios integrados o anuncios de banner que no sean de pantalla completa).

Estos lineamientos se inspiran en los de Better Ads Standards - Mobile Apps Experiences . Para obtener más información sobre los estándares de Better Ads Standards, consulte la página de Coalition for Better Ads .

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

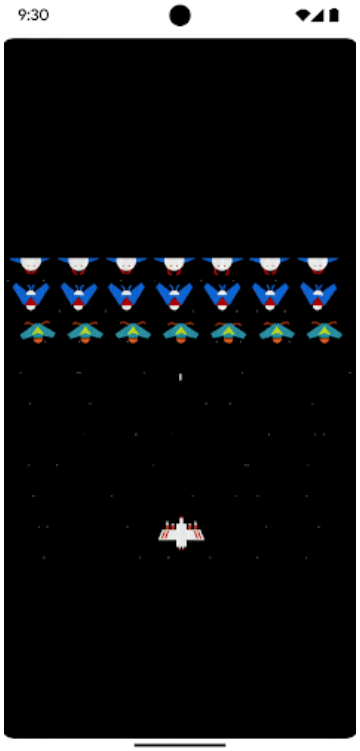
- Anuncios inesperados que aparecen durante el juego o al comienzo de un segmento de contenido (por ejemplo, después de que un usuario hizo clic y antes de que la acción prevista del clic en el botón haya surtido efecto); Estos anuncios son inesperados para los usuarios, ya que ellos esperan comenzar un juego o interactuar con contenido

① El anuncio estático inesperado aparece durante el juego al principio de un nivel.



② El anuncio de video inesperado aparece durante el comienzo de un segmento de contenido.

- Un anuncio en pantalla completa que aparece durante el juego y no se puede cerrar después de 15 segundos



① Aparece un anuncio intersticial durante el juego, el cual no les ofrece a los usuarios la opción de omitirlo en el transcurso de 15 segundos.

En vigencia a partir del 30 de septiembre de 2022

Suscripciones

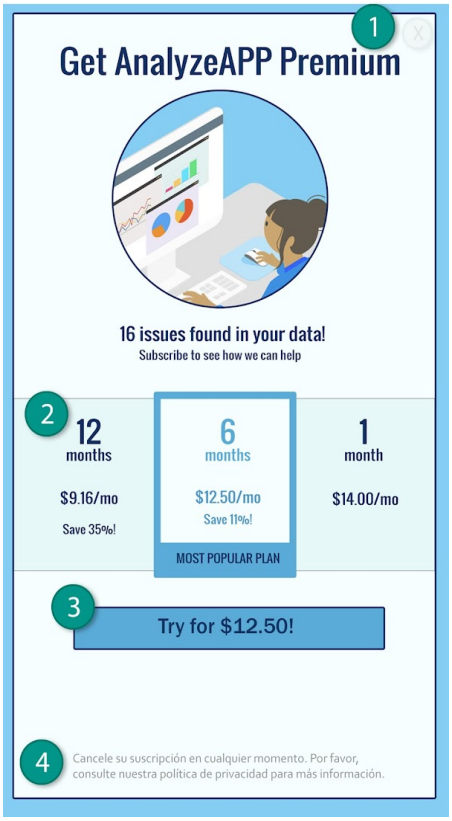
Como desarrollador, no debe engañar a los usuarios acerca de ningún servicio de suscripción o contenido que ofrezca dentro de su aplicación. Es fundamental que, en promociones dentro de la aplicación o pantallas de presentación, la comunicación sea clara. No permitimos aplicaciones que lleven a los usuarios a tener experiencias de compra engañosas o manipuladoras (lo que incluye suscripciones o compras directas desde la aplicación)

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

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

- Suscripciones mensuales que no informan a los usuarios que se les renovará el plan de forma automática y se les cobrará cada mes
- Suscripciones anuales que muestran sus precios de forma más prominente en términos del costo mensual
- Precios y condiciones de las suscripciones que no están totalmente localizados
- Promociones integradas en la aplicación que no demuestran con claridad que el usuario puede acceder al contenido sin una suscripción (cuando esté disponible)
- Nombres de SKU que no representan con precisión la naturaleza de la suscripción, como "Prueba gratuita" o "Prueba la membresía Premium: 3 días gratis", en una suscripción que tiene un cargo automático recurrente
- Múltiples pantallas en el flujo de compra que llevan a los usuarios a hacer clic de forma accidental en el botón de suscripción

Ejemplo 1:



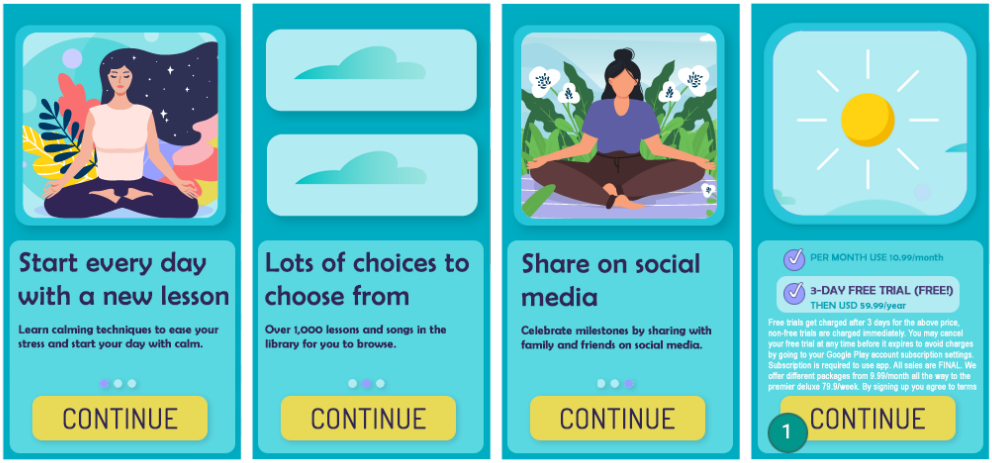
① El botón para descartar no está claramente visible, por lo que es posible que los usuarios no comprendan que pueden acceder a la función sin aceptar la oferta de suscripción.

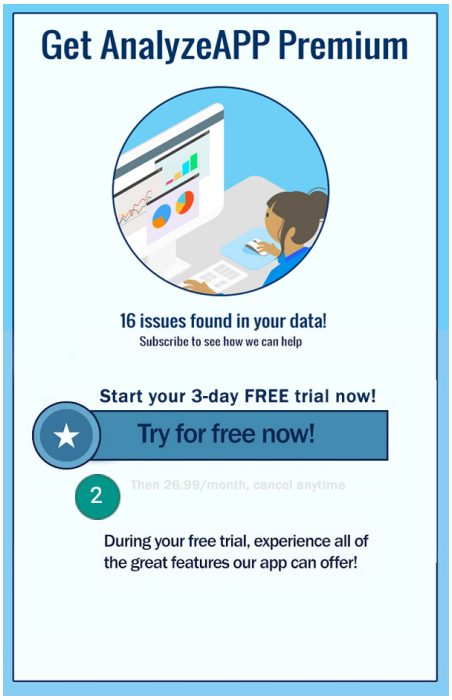
② La oferta solo muestra los precios en términos del costo mensual, por lo que es posible que los usuarios no comprendan que se les cobrarán seis meses en el momento de la suscripción.

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.

Ejemplo 2:





① Cuando el usuario hace varios clics en el mismo botón, termina seleccionando sin darse cuenta el botón "Continuar" final que activa la suscripción.

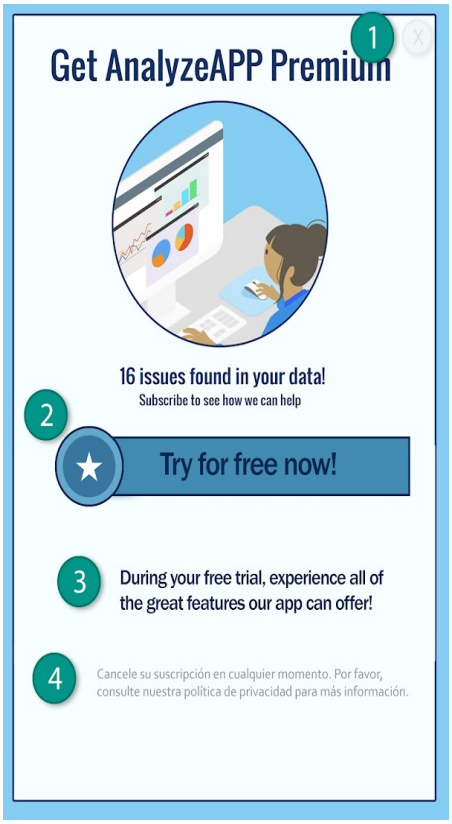
② El importe que se les cobra a los usuarios al final de la prueba es difícil de leer, y eso les hace creer que el plan es gratuito.

Pruebas gratuitas y ofertas de lanzamiento

Antes de que se inscriba un usuario en su suscripción: Debe describir de manera clara y precisa los términos de su oferta, incluidos el precio, la duración y la descripción de los servicios o el contenido a los que se dará acceso. Asegúrese de permitir que los usuarios tengan conocimiento de cuándo y cómo se convertirá una prueba gratuita en una suscripción pagada, cuánto costará la suscripción pagada y que pueden cancelarla si no quieren convertirse en suscriptores que pagan.

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

- Ofertas que no explican de manera clara la duración de la prueba gratuita o del precio de lanzamiento
- Ofertas que no explican de manera clara que se inscribirá de forma automática al usuario en una suscripción pagada 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.

En vigencia a partir del 30 de septiembre de 2022

Administración, Cancelación y Reembolso de Suscripciones

Si vende suscripciones en su aplicación, debe asegurarse de que esta divulgue claramente cómo el usuario puede administrar o cancelar la suscripción. También debe incluir en su aplicación acceso a un método en línea fácil de usar para cancelar la suscripción. En la configuración de cuentas de su aplicación (o una página equivalente), puede satisfacer este requisito si incluye lo siguiente:

- Un vínculo al Centro de Suscripciones de Google Play (en el caso de las aplicaciones que usen el sistema de facturación de Google Play)
- Acceso directo a su proceso de cancelación

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

Como proveedor de contenido o acceso, usted debe implementar una política de reembolso más flexible directamente con los usuarios. Es su responsabilidad notificarles sobre los cambios

implementados en las políticas de suscripción, la cancelación y el reembolso, y garantizar que las políticas satisfagan la legislación vigente.

Entrada en vigencia: 1 de noviembre de 2022

Programa del SDK de Anuncios con Autocertificación para Familias

Si publica anuncios en su aplicación y esta tiene como usuarios objetivo 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, lo que incluye los Requisitos de Autocertificación de SDK de Anuncios que se indican más abajo.

Si el público objetivo de su aplicación incluye tanto niños como usuarios mayores, debe asegurarse de que los anuncios que se muestren a los niños provengan exclusivamente de uno de los SDK de anuncios con autocertificación (por ejemplo, mediante el uso de medidas en pantallas neutrales de comprobación de edad). Las aplicaciones que participan en el programa Diseñado para familias solo pueden usar SDK de anuncios con autocertificación.

Tenga en cuenta que es su responsabilidad asegurarse de que todas las versiones de SDK que implemente en su aplicación, incluidos los SDK de Anuncios con Autocertificación, satisfagan todas las políticas, leyes y reglamentaciones locales. Google no proporciona representaciones ni garantías sobre la precisión de la información que brinden los SDK de anuncios durante el proceso de autocertificación.

El uso de SDK de anuncios con autocertificación para Familias solo se requiere si usa SDK de anuncios a fin de publicar anuncios para niños. Si bien usted es responsable de garantizar que el contenido del anuncio y las prácticas de recopilación de datos satisfagan la Política de Datos del Usuario y la Política de Familias de Google Play, se permite lo siguiente sin el requisito de autocertificación de los SDK de anuncios ante Google Play:

- Publicidad interna en la que use SDK para administrar la promoción cruzada de sus aplicaciones 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 SDK de Anuncios con Autocertificación para Familias

- Defina el significado de comportamientos y contenido del anuncio reprochables, y prohíbalos en las condiciones o políticas de los SDK de anuncios. Las definiciones deben satisfacer las Políticas del programa para desarrolladores de Google Play.
- Cree un método para clasificar 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 reglamentaciones 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 para Familias de Google Play y que cumplan con el requisito del Programa con contenido aprobado por profesores .
- Asegúrese de que, cuando se usen ofertas en tiempo real para mostrar anuncios a los niños, se hayan revisado las creatividades y que se propaguen los indicadores de privacidad a los ofertantes.
- Proporcione a Google suficiente información, por ejemplo mediante el envío de una aplicación de prueba y de los datos que se indican en el formulario de interés que se incluye más abajo, para

verificar el cumplimiento de la política del SDK de anuncios con todos los requisitos de autocertificación, y responda de forma oportuna a cualquier solicitud de información adicional, como el envío de nuevas versiones para verificar el cumplimiento de la versión del SDK de anuncios con todos los requisitos de autocertificación.
- Realice la autocertificación para verificar que todas las versiones nuevas cumplan con las Políticas del Programa para Desarrolladores de Google Play más recientes, incluidos los Requisitos de la Política de Familias.

Nota: Los SDK de Anuncios con Autocertificación para Familias deben admitir un proceso de publicación de anuncios que satisfaga todos los estatutos y reglamentaciones relevantes relacionados con niños que podrían aplicarse a sus publicadores.

Aquí se incluyen los requisitos de mediación para las plataformas de publicación cuando se publican anuncios dirigidos a niños:

- Use únicamente SDK de Anuncios con Autocertificación para Familias o implemente las protecciones necesarias para garantizar que todos los anuncios que se publiquen desde plataformas de mediación satisfagan estos requisitos.
- Brinde la información necesaria a las plataformas de mediación para indicar la clasificación del contenido del anuncio y cualquier contenido dirigido a niños que corresponda.

Los desarrolladores pueden encontrar una lista de SDK de Anuncios con Autocertificación para Familias aquí .

Además, los desarrolladores pueden compartir este formulario de interés con los SDK de anuncios que deseen autocertificarse.

Ficha de Play Store y promociones

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

Promoción de aplicaciones

No se permiten las aplicaciones que, de forma directa o indirecta, participen o se beneficien de prácticas de promoción (como anuncios) engañosas o perjudiciales para los usuarios o el ecosistema de desarrolladores. Las prácticas de promoción son engañosas o perjudiciales si su comportamiento o contenido incumplen nuestras Políticas del Programa para Desarrolladores.

Ejemplos de incumplimientos comunes:

- El uso de anuncios engañosos en sitios web, aplicaciones y otras propiedades, lo que incluye las notificaciones y alertas que sean similares a las del sistema
- El uso de anuncios sexualmente explícitos con el fin de dirigir a los usuarios a la ficha de Google Play de su aplicación para que realicen la descarga
- Las tácticas de promoción o de instalación que redireccionen a los usuarios a Google Play o a descargar aplicaciones sin previo aviso sobre la acción que van a realizar
- La promoción no solicitada mediante servicios por SMS

Es su responsabilidad asegurarse de que todos los anuncios, redes de publicidad y afiliados asociados con su aplicación satisfagan estas políticas.

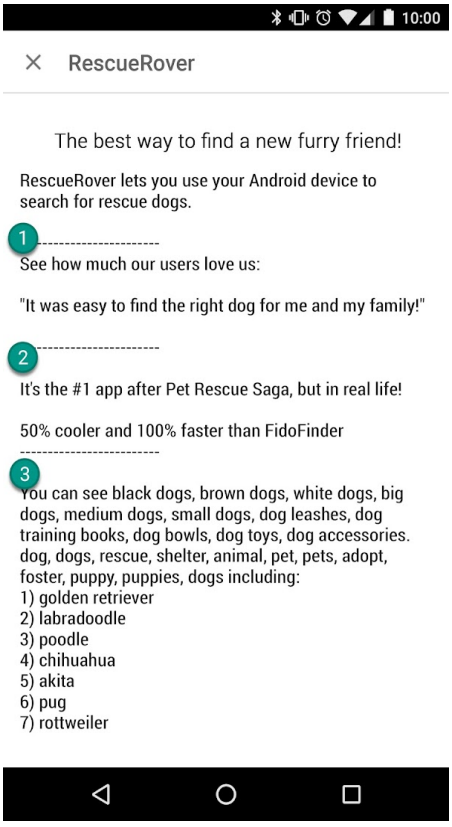
Metadatos

No se permiten apps con metadatos engañosos, no descriptivos, irrelevantes, excesivos, inapropiados ni con formato inadecuado, entre los que se incluyen, sin limitarse a ello, la descripción de la 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 aplicación. Tampoco permitimos testimonios de usuarios anónimos o sin atribución en la descripción de la aplicación.

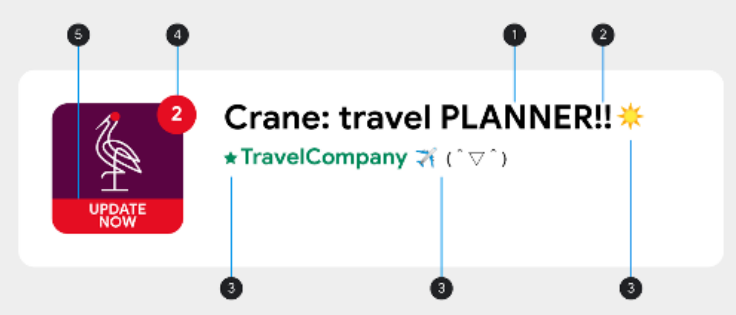
El título, el ícono y el nombre del desarrollador son datos particularmente útiles para que los usuarios puedan encontrar su aplicación y obtener información acerca de ella. No use emojis, emoticones ni caracteres especiales repetidos en esos elementos de metadatos. Evite usar SOLO MAYÚSCULAS, a menos que sea parte del nombre de su marca. No se permite el uso de símbolos engañosos en los íconos de las aplicaciones, como un indicador de mensaje nuevo cuando realmente no hay ninguno o los símbolos de descarga e instalación cuando la aplicación no está relacionada con la descarga de contenido. El título de la aplicación debe tener 30 caracteres o menos.

Además de los requisitos mencionados aquí, es posible que, según las Políticas para Desarrolladores de Google Play, se le exija que proporcione información adicional sobre los metadatos.

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



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



① SOLO MAYÚSCULAS, aunque no sean parte del nombre de la marca
② Secuencias de caracteres especiales que son irrelevantes para la aplicación
③ Uso de emojis, emoticones (incluidos los kaomojis) y caracteres especiales
④ Símbolos engañosos
⑤ Texto engañoso

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 debe ser apto para todo público en la ficha de Play Store.

A continuación, se detallan algunas prácticas recomendadas:

- Destaque lo mejor de la aplicación. Comparta hechos 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. Evite el uso de texto, imágenes o videos inapropiados en la ficha, y cumpla con los lineamientos mencionados.

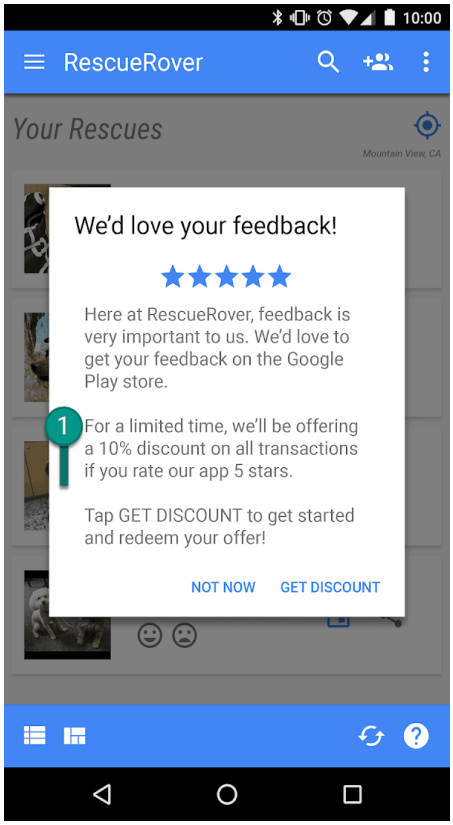
Calificaciones, instalaciones y opiniones de usuarios

Los desarrolladores no deben manipular la posición de las aplicaciones en Google Play, lo que incluye, sin limitaciones, 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. Las instalaciones, opiniones y calificaciones incentivadas incluyen el uso de texto o imágenes en el título, el ícono o el nombre del desarrollador de la aplicación que indiquen el precio o brinden otra información promocional.

Los desarrolladores no deben agregar texto ni imágenes que indiquen la calificación o el rendimiento en Play Store, o sugieran alguna relación con programas de Google Play existentes en el título, el ícono o el nombre de desarrollador de la aplicación.

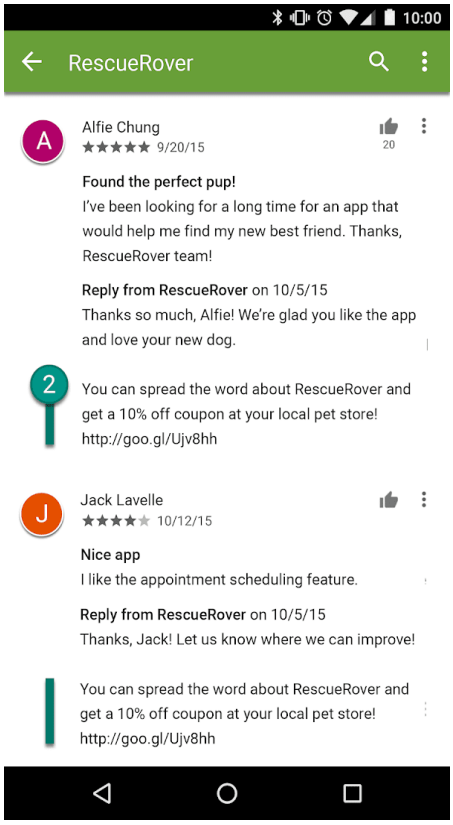
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Solicitarles a los usuarios que califiquen una app 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 app 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 apps o sitios web



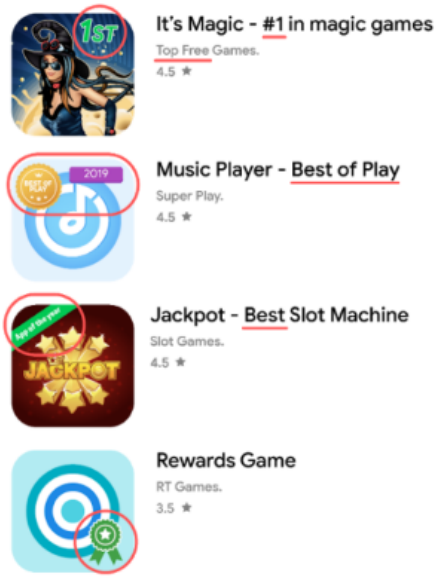
② Esta opinión motiva a los usuarios a promocionar la app de RescueRover a cambio de una oferta de cupón.

Las calificaciones y opiniones representan la calidad de una app. 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:

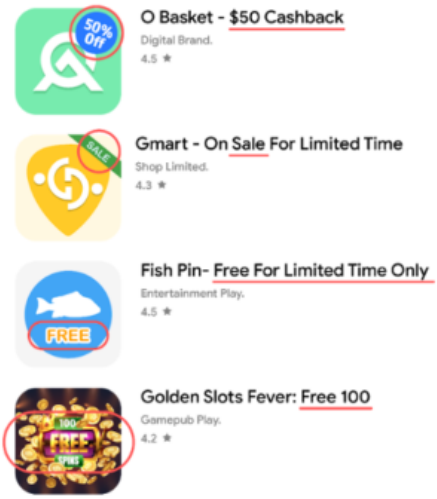
- Asegúrate de que la respuesta se centre en el problema que se indica en los comentarios del usuario, y no solicites una calificación superior.
- Se deben incluir referencias a recursos útiles, como una dirección de asistencia o una página de preguntas frecuentes.

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

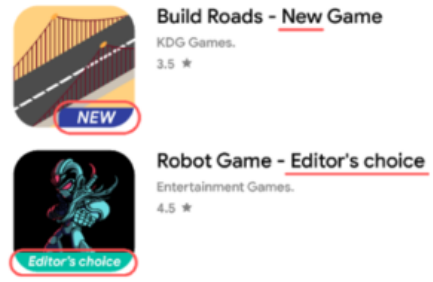
- Imágenes o texto que indiquen la calificación o el rendimiento en Play Store, como "App del año", "Núm. 1", "La mejor de Google Play en 20XX", "Popular", íconos de premios, etcétera



- Imágenes o texto que brinden información promocional o sobre el precio, como "10% de descuento", "Devolución de USD 50", "Gratis por tiempo limitado únicamente", etcétera



- Imágenes o texto que indiquen programas de Google Play, como "Selección del editor", "Nuevas", etcétera



Clasificaciones del contenido

La Coalición Internacional de Clasificación por Edad (IARC) proporciona las clasificaciones de contenido de Google Play, 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 aplicación. También ayudan a filtrar o bloquear el contenido en ciertos territorios o a usuarios específicos cuando lo exige la ley; además, determinan la elegibilidad de una aplicación para participar en programas especiales para desarrolladores.

Cómo se determina la clasificación del contenido

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

Para evitar que la aplicación aparezca como "Sin clasificación", se debe completar el cuestionario de clasificación del contenido para cada aplicación nueva que se envíe a Play Console y para todas las

aplicaciones existentes activas en Google Play. Se quitarán de Play Store las aplicaciones que no tengan una clasificación del contenido.

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

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

Apelación de clasificación

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

En vigencia a partir del 11 de agosto de 2022

Noticias

Una aplicación de Noticias tiene una de las siguientes características:

- Se declara como perteneciente a la categoría "Noticias" en Google Play Console.
- Se incluye dentro de la categoría "Noticias y revistas" en Google Play Store y se describe como de "noticias" en su título, ícono o descripción, o en el nombre del desarrollador.

Ejemplos de aplicaciones dentro de la categoría "Noticias y revistas" que califican como aplicaciones de Noticias:

- Aplicaciones que se describen como de "noticias" en su descripción, incluidas, sin limitaciones, las siguientes:
  - Noticias recientes
  - Periódicos
  - Noticias de último momento
  - Noticias locales
  - Noticias diarias
- Aplicaciones con la palabra "Noticias" en su título o ícono, o en el nombre del desarrollador

Sin embargo, si las aplicaciones contienen principalmente contenido generado por usuarios (p. ej., aplicaciones de redes sociales), no se deben declarar como aplicaciones de Noticias ni se considerarán como tales.

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 la aplicación y la fuente de los artículos de noticias, incluidos, sin limitaciones, el autor o el editor original de cada artículo. En los casos en que no es habitual especificar los autores individuales de los artículos, la aplicación de noticias debe ser el editor original de los artículos. Recuerde que los vínculos a cuentas de redes sociales no se consideran una forma suficiente de información del editor o el autor.
- 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 un número de teléfono o 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.

Las aplicaciones de noticias no deben hacer lo siguiente:

- Contener errores ortográficos ni gramaticales significativos
- Tener únicamente contenido estático (p. ej., contenido con más de tres meses de antigüedad)
- Tener como objetivo principal el marketing de afiliación o los ingresos publicitarios

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.

Para conocer la mejor manera de proporcionar la información requerida, consulte este artículo .

Spam y funcionalidad mínima

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

Spam

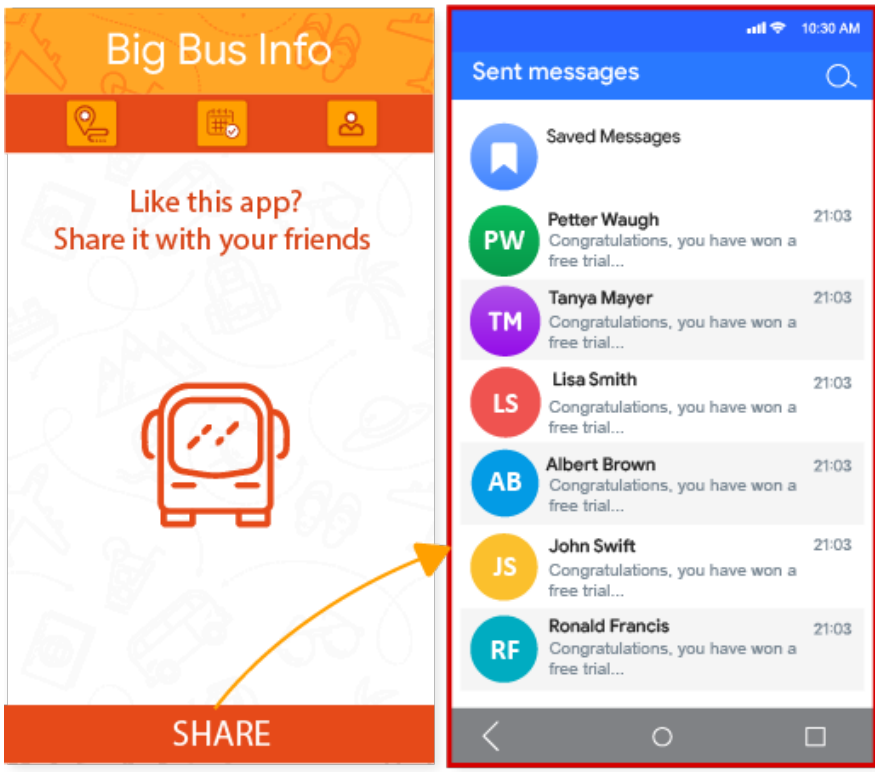
No se permiten aplicaciones que envíen spam a los usuarios o a Google Play, como las que envían mensajes no solicitados o aplicaciones repetitivas y de baja calidad.

Spam a través de mensajes

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

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

- Cuando el usuario presiona el botón "Compartir", la app envía mensajes en nombre suyo sin darle la posibilidad de confirmar el contenido y los destinatarios:

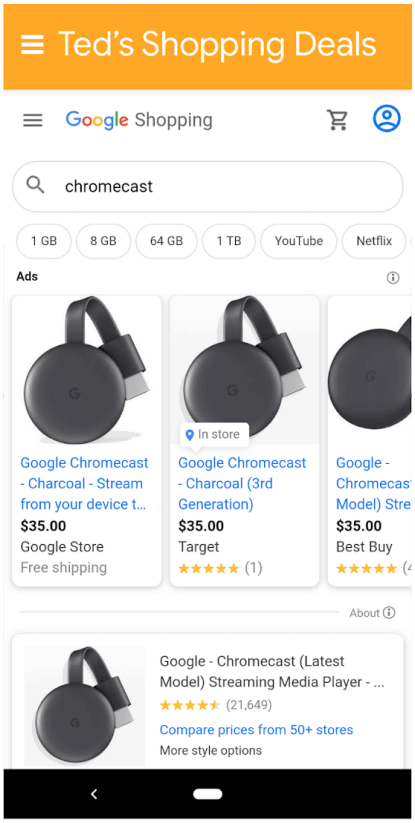


Spam de afiliados y de vistas web

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

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

- Una aplicación cuyo objetivo sea dirigir tráfico de referencia a un sitio web para recibir beneficios por los registros o compras del usuario en ese sitio
- Apps cuyo objetivo principal sea proporcionar una vista web de un sitio sin permiso:



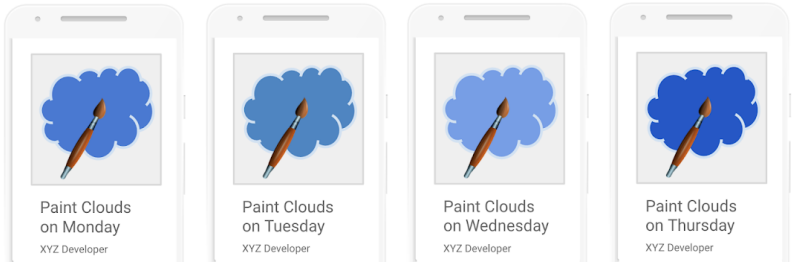
① Esta app se llama "Ofertas de compras de Ted" y solo proporciona una vista web de Google Shopping.

Contenido repetitivo

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

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

- Copiar elementos de otras aplicaciones sin agregar contenido o valor original
- Crear varias 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)

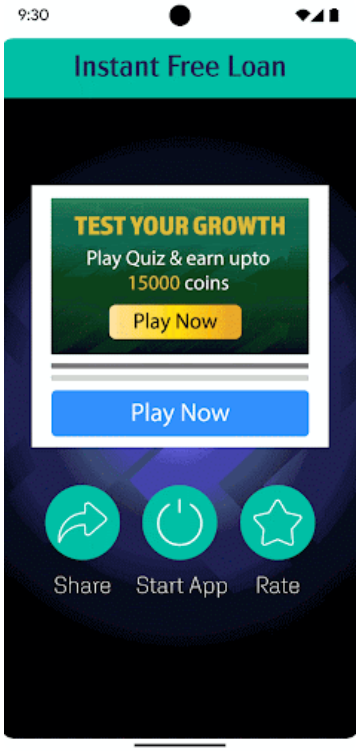


Apps creadas para la publicación de anuncios

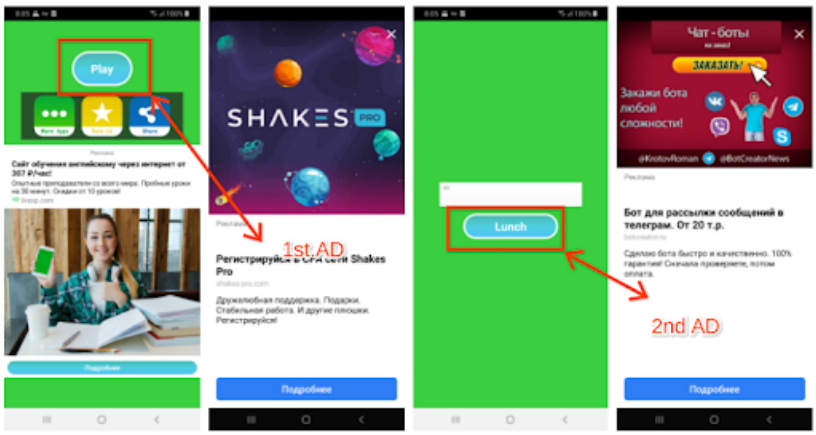
No permitimos aplicaciones que muestren anuncios intersticiales de forma reiterada para distraer a los usuarios y evitar que interactúen con una aplicación y realicen tareas en ella.

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

- Aplicaciones en las que se ubique un anuncio intersticial después de una acción del usuario (incluidos, sin limitaciones, los clics, deslizamientos, etc.) de manera consecutiva



La primera página en la aplicación tiene múltiples botones con los que se puede interactuar. Cuando el usuario selecciona **Start app** para usar la aplicación, aparece un anuncio intersticial. Después de que se cierra el anuncio, el usuario regresa a la aplicación y selecciona **Service** para comenzar a usar el servicio, pero aparece otro anuncio intersticial.



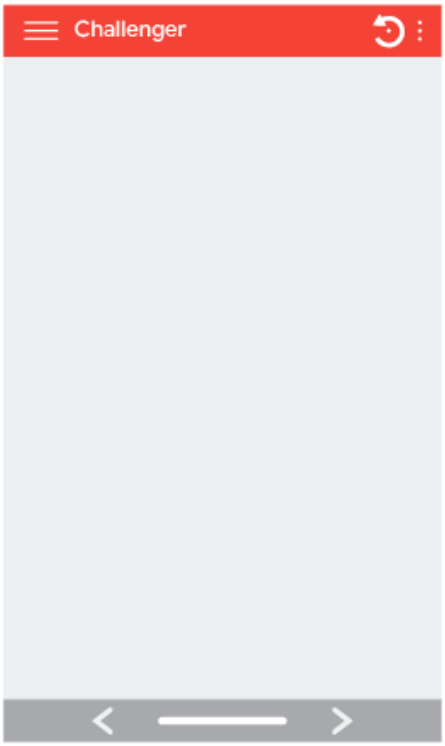
En la primera página, el usuario debe seleccionar **Play**, ya que es el único botón disponible para usar la aplicación. Cuando el usuario lo selecciona, aparece un anuncio intersticial. Después de que se cierra el anuncio, el usuario selecciona **Launch**, ya que es el único botón con el cual se puede interactuar, y aparece otro anuncio intersticial.

Funcionalidad mínima

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

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

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



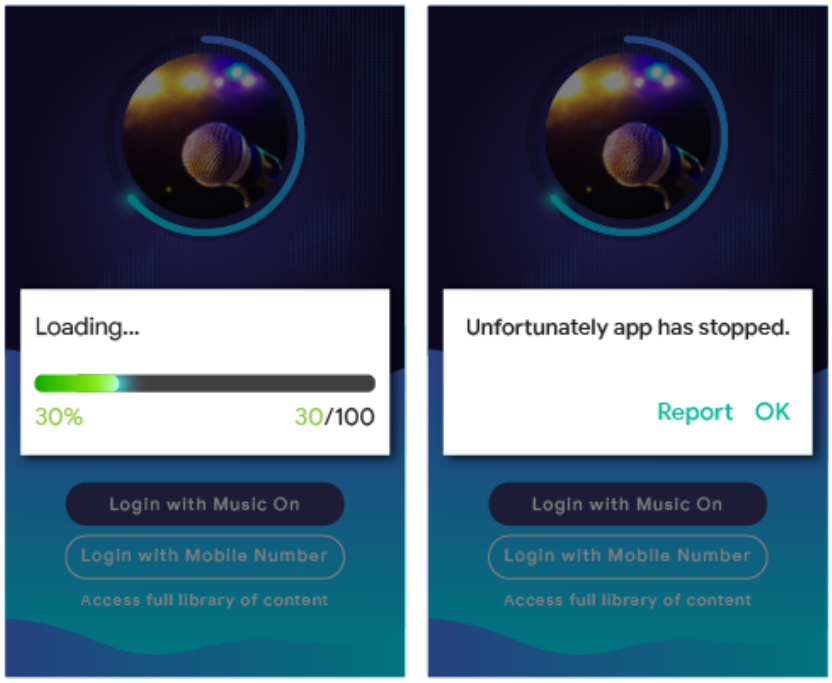
Funcionalidad dañada

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

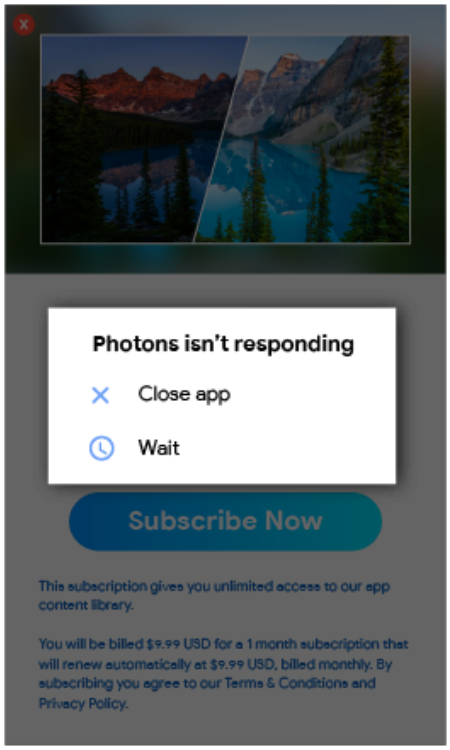
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Apps que **no se instalan**

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



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



Otros programas

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

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

Apps instantáneas Android

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

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

Identidad

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

Compatibilidad con vínculos

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

Especificaciones técnicas

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

Ofrecimiento de instalación de aplicaciones

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

- Usar el ícono "Obtener app" de material design y la etiqueta "Instalar" para el botón de instalación.
- Tener más de 2 a 3 solicitudes de instalación implícita en la aplicación instantánea.
- Abstenerse de usar banners o cualquier otra técnica de tipo publicitario para presentar una solicitud de instalación a los usuarios.

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

Cambios en el estado del dispositivo

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

Visibilidad de la aplicación

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

Identificadores de dispositivos

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

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

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

Tráfico de red

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

Política de Emojis para Android

Nuestra política de emojis está diseñada para promover una experiencia del usuario inclusiva y coherente. Para lograrlo, todas las aplicaciones deben admitir la versión más reciente de Emojis Unicode cuando se ejecutan en Android 12 y versiones posteriores.

Las aplicaciones que usan los Emojis Unicode predeterminados sin implementaciones personalizadas ya usan la versión más reciente de Emojis Unicode cuando se ejecutan en Android 12 y versiones posteriores.

Las aplicaciones con implementaciones personalizadas de emojis, incluidas las que se proporcionan mediante bibliotecas de terceros, deben tener que admitir por completo la versión más reciente de Unicode cuando se ejecuten en Android 12 y versiones posteriores en un plazo de 4 meses después de que se lancen nuevos Emojis Unicode.

Para obtener más información sobre cómo admitir emojis modernos, consulte esta guía .

Use los siguientes ejemplos de emojis para probar si su aplicación satisface los requisitos de la versión más reciente de Unicode:

Ejemplos	Versión de Unicode
🫠 🫱🏽 🫵🏾	14.0
😶‍🌫️ 👩🏻 💏	13.1
🥲 🫅🏿 🐻‍❄️	13.0
🧑‍🦰 🧍🏻‍♂️ 👫	12.1
🦩 🦬 👭	12.0

Familias

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

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

Cómo diseñar aplicaciones para niños y familias

A medida que aumenta el uso de la tecnología como herramienta para enriquecer las vidas de las familias, los padres buscan más contenido seguro y de alta calidad para compartir con sus hijos. Quizá 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 el Programa con Contenido Aprobado por Profesores, pero no podemos garantizar que se incluyan en este último. Incluso si decides no participar en 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 Desarrolladores.

Requisitos de Play Console

Público Objetivo y Contenido

En la sección Público Objetivo y Contenido de Google Play Console, debes indicar el público objetivo de tu aplicación antes de publicarla. Para ello, selecciona uno de los grupos de edades disponibles. Independientemente de lo que selecciones en Google Play Console, si decides incluir en la aplicación terminología o imágenes dirigidas a niños, o que se puedan juzgar como tales, esto podría afectar la evaluación de Google Play sobre el público objetivo declarado. Google Play se reserva el derecho de revisar por su cuenta la información que 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 la selección es incorrecta porque la aplicación se orienta tanto a niños como a adultos, podrás aclararles a los usuarios que la aplicación no se orienta a niños incorporando una etiqueta de advertencia.

Solo debes seleccionar más de un grupo de edades como público objetivo de tu aplicación 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 aplicaciones diseñadas para bebés, niños pequeños y niños de edad preescolar solo deben tener seleccionado el grupo "Hasta 5 años" como público objetivo. Si la 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 aplicación en la sección "Público Objetivo y Contenido" de Google Play Console en cualquier momento. Para que esta información se pueda ver reflejada en Google Play Store, primero se debe publicar una actualización de la aplicación. Sin embargo, es posible que se revisen los cambios que 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 aplicación.

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 aplicación en Play Console, incluida la sección "Público Objetivo y Contenido", puede causar que se elimine o suspenda la aplicación, por lo que es fundamental que proporciones información correcta.

Requisitos de la Política de Familias

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

1. **Contenido de la aplicación:** El contenido de la aplicación al que pueden acceder niños debe ser apto para ellos. Si su aplicación incluye contenido que no es adecuado a nivel mundial, pero ese contenido se considera adecuado para usuarios menores de edad en una región específica, la aplicación podría estar disponible en ella (regiones limitadas), pero seguirá sin estar disponible en otras regiones.
2. **Funciones de la app:** Su aplicación no debe proporcionar simplemente una vista web de un sitio web ni tener un objetivo principal de atraer tráfico afiliado a un sitio web, más allá de la propiedad del sitio.
   - Exploramos continuamente formas de habilitar nuevas experiencias para desarrolladores de aplicaciones para niños. Si le interesa unirse al piloto de Aplicaciones Web de Confianza para aplicaciones educativas, exprese su interés aquí .
3. **Respuestas en Play Console:** Debe responder con precisión las preguntas relacionadas con su aplicación en Google Play Console y actualizar esas respuestas para que reflejen con exactitud cualquier cambio que realice en ella. Esto incluye, sin limitaciones, usar el Cuestionario de Clasificación del Contenido para divulgar con precisión información sobre los elementos interactivos de la aplicación, como los siguientes:
   - Si los usuarios de la aplicación pueden interactuar o intercambiar información
   - Si la aplicación comparte con terceros la información proporcionada por los usuarios
   - Si la aplicación comparte la ubicación física del usuario con otros usuarios
4. **Anuncios:** Si la aplicación muestra anuncios a niños o usuarios de edades desconocidas, debe respetar los siguientes lineamientos:
   - Usar únicamente SDK de anuncios certificados por Google Play para mostrar anuncios a esos usuarios
   - Asegurarse de que los anuncios que se muestren a esos usuarios no incluyan publicidad basada en intereses (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 aplicación 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 de los anuncios para Familias
   - Garantizar el cumplimiento de todas las reglamentaciones legales aplicables y los estándares de la industria relacionados con la publicidad dirigida a niños
5. **Prácticas de datos:** Debe divulgar la recopilación de información personal y sensible de los niños en su aplicación, incluidos los casos en que esta se reúna a través de API o SDK que se llamen o se usen en su aplicación. La información sensible de los niños incluye, sin limitaciones, información de autenticación, datos de sensores del micrófono y la cámara, datos del dispositivo, el ID de Android y datos de uso de anuncios. Además, debe asegurarse de que su aplicación implemente las prácticas de datos que se mencionan a continuación:
   - Las aplicaciones que se dirijan únicamente a niños no deben transmitir identificadores de publicidad de Android (AAID), números de serie de SIM, Build Serial, BSSID, MAC, SSID, IMEI ni IMSI.

- Las aplicaciones que se dirijan tanto a niños como a públicos mayores no deben transmitir AAID, números de serie de SIM, Build Serial, BSSID, MAC, SSID, IMEI ni IMSI de niños o usuarios de edades desconocidas.
- No se deben solicitar números de teléfono de dispositivos a TelephonyManager de la API de Android.
- Las aplicaciones que se orientan únicamente a niños no deben solicitar el permiso de ubicación ni recopilar, usar o transmitir la ubicación precisa .
- Las aplicaciones deben usar el Administrador de Dispositivos Complementario (CDM) cuando soliciten Bluetooth, a menos que se orienten únicamente a las versiones del Sistema Operativo (SO) del dispositivo no compatibles con CDM.

6. **API y SDK:** Debe asegurarse de que la aplicación implemente cualquier API y SDK de forma adecuada.
   - Las aplicaciones que se orienten únicamente a niños no deben contener API ni SDK cuyo uso no esté aprobado para servicios dirigidos principalmente 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. Las aplicaciones que se orienten tanto a niños como a públicos mayores no deben requerir que los usuarios accedan a su cuenta o al contenido de la aplicación desde una API o un SDK que no esté aprobado para su uso en servicios dirigidos a niños.

7. **Realidad Aumentada (RA):** Si su aplicación usa Realidad Aumentada, debe incluir una advertencia de seguridad que aparezca tan pronto como se abra la sección de RA y que contenga los siguientes elementos:
   - Un mensaje adecuado sobre la importancia de la supervisión parental
   - Un recordatorio sobre los riesgos físicos en el mundo real (p. ej., estar atento al entorno)
   - La aplicación no debe requerir el uso de un dispositivo no recomendado para niños (p. ej., Daydream, Oculus).

8. **Funciones y Aplicaciones Sociales:** Si sus aplicaciones les permiten a los usuarios compartir o intercambiar información, debe divulgar de forma precisa estas funciones en el cuestionario de clasificación del contenido de Play Console.
   - Aplicaciones Sociales: Una aplicación social tiene como objetivo principal permitirles a los usuarios compartir contenido de formato libre o comunicarse con grupos numerosos de personas. Todas las aplicaciones sociales que incluyan niños entre el público objetivo deben mostrar a los usuarios un recordatorio integrado de que se mantengan seguros en línea y sean conscientes del riesgo real que existe en la interacción en línea antes de permitir a los usuarios menores de edad intercambiar información o contenido multimedia de formato libre. Además, usted debe solicitar la intervención de un adulto antes de permitirles a los usuarios menores de edad intercambiar información personal.
   - Funciones Sociales: Son funciones adicionales de las aplicaciones que les permiten a los usuarios compartir contenido de formato libre o comunicarse con grupos numerosos de personas. Las aplicaciones que incluyan niños entre el público objetivo y tengan funciones sociales deben mostrar a los usuarios un recordatorio integrado de que se mantengan seguros en línea y sean conscientes del riesgo real que existe en la interacción en línea antes de permitir a los usuarios menores de edad intercambiar información o contenido multimedia de formato libre. Además, usted debe ofrecer un método con el que los adultos puedan administrar las funciones sociales de los usuarios menores de edad, incluida, sin limitaciones, la posibilidad de habilitar o inhabilitar la función social o seleccionar diferentes niveles de funcionalidad. Por último, debe solicitar la

intervención de un adulto antes de habilitar funciones que les permitan a los niños intercambiar información personal.

- Con intervención de un adulto nos referimos a un mecanismo que permita verificar que el usuario no es menor y no aliente a los niños a falsificar su edad (por ejemplo, con el uso de PIN, contraseñas, fechas de nacimiento, verificación por correo electrónico, ID de foto, tarjetas de crédito o NSS que pertenezcan a adultos) para acceder a áreas de su aplicación diseñadas para adultos.
- Las aplicaciones sociales cuyo objetivo principal es chatear con personas desconocidas no deben orientarse a niños. Entre algunos ejemplos, se incluyen aplicaciones con el estilo de Chatroulette, aplicaciones de citas, salas de chat abiertas enfocadas en niños, etcétera.

9. **Cumplimiento legal:** Debe asegurarse de que la aplicación, incluidos todos los SDK o API que esta llame o use, satisfaga la Ley de Protección de la Privacidad de Menores en Internet (COPPA) de EE.UU. , el Reglamento General de Protección de Datos (GDPR) de la UE y cualquier otra ley o reglamentación aplicable.

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

- 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 con vínculos a sitios web que presentan contenido que infringe las Políticas del Programa para Desarrolladores
- 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 para Familias a fin de obtener más información sobre las políticas de Google Play sobre publicidad, compras directas desde las aplicaciones y contenido comercial para niños.

Programa Diseñado para Familias

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

Para que se acepte su app en el programa, esta debe cumplir con todos los requisitos de la Política de Familias y los 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 el Programa

Las aplicaciones que participen en el programa Diseñado para Familias y los anuncios que se incluyan en ellas solo pueden tener contenido pertinente y apropiado para niños (las aplicaciones deben estar clasificadas por la ESRB como "Aptas para todo público" o "Para mayores de diez años", o tener una clasificación equivalente), y deben usar únicamente SDK de anuncios certificados por Google Play . Las aplicaciones que se acepten en el programa Diseñado para Familias deben mantenerse en pleno

cumplimiento de todos los requisitos del programa. Google Play puede rechazar, quitar o suspender cualquier aplicación que se considere inapropiada para el programa Diseñado para Familias.

Here are some examples of common apps that are ineligible for the program:

- Aplicaciones 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 aplicaciones de administración de dispositivos diseñadas para que las usen únicamente padres o cuidadores

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

Anuncios y monetización

Si monetiza una aplicación que se orienta a niños en Play, es importante que esta cumpla con los Requisitos de la Política de Monetización y Anuncios para Familias.

Las siguientes políticas se aplican a cualquier actividad de monetización y publicidad que se realice en su aplicación, incluidos los anuncios, las promociones cruzadas (de aplicaciones propias y de terceros), las ofertas de compra directa desde la aplicación o cualquier otro contenido comercial (como colocación de producto pagada). Todos los componentes de monetización y publicidad de estas aplicaciones deben satisfacer las leyes y reglamentaciones aplicables (incluidos los lineamientos autorregulatorios o de la industria que sean relevantes).

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

Requisitos de formato

Los elementos monetizados y los anuncios que muestre su aplicación no deben incluir contenido engañoso ni estar diseñados de manera tal que los niños que usen la aplicación hagan clic en ellos de forma involuntaria. Están prohibidas las siguientes acciones:

- Monetización y publicidad invasivas, incluidas aquellas cuyos componentes ocupen toda la pantalla o interfieran con el uso normal y no ofrezcan un medio claro para descartar los anuncios

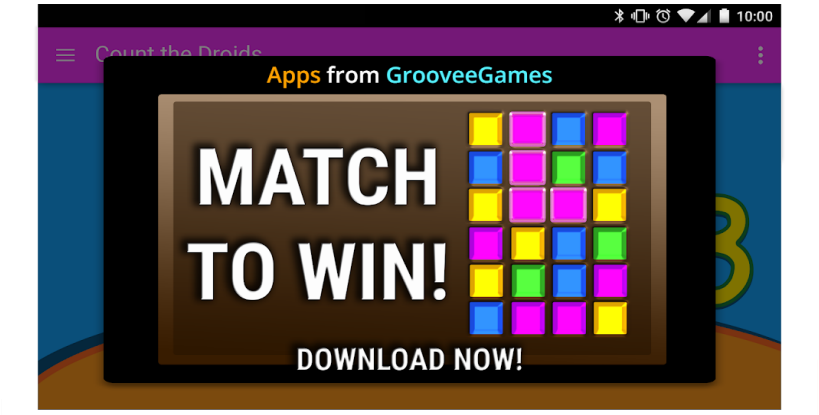
(p. ej., paneles publicitarios)

- Monetización y publicidad que interfieran con el uso normal de la aplicación o el juego y que no se puedan cerrar después de 5 segundos;
- la monetización o publicidad cuyos componentes no interfieren 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)
- Monetización y publicidad con anuncios intersticiales que se muestran inmediatamente después de que se abre la aplicación
- Varias colocaciones de anuncios en una página (p. ej., no se permiten anuncios de banner que publiquen varias ofertas en una posición o que muestren más de un anuncio de banner o video)
- Monetización o publicidad cuyos componentes no se distingan fácilmente del contenido de la aplicación
- Tácticas ofensivas o emocionalmente manipuladoras para promover la visualización de anuncios o las compras directas desde la aplicación
- Falta de distinción entre el uso de monedas virtuales de juego y dinero real para hacer compras directas desde la aplicación

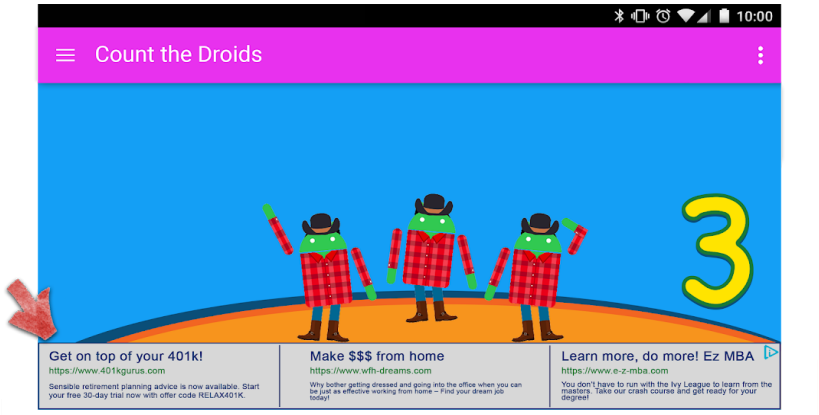
Para garantizar que Google Play continúe siendo una plataforma segura y respetuosa, creamos estándares que definen y prohíben el contenido dañino o inapropiado para nuestros usuarios.

- Monetización y publicidad cuyos componentes se alejan del dedo del usuario cuando este trata de cerrarlos
- Monetización y publicidad que no proporcionan al usuario una forma de salir de la oferta después de cinco (5) segundos, como se muestra en el siguiente ejemplo:

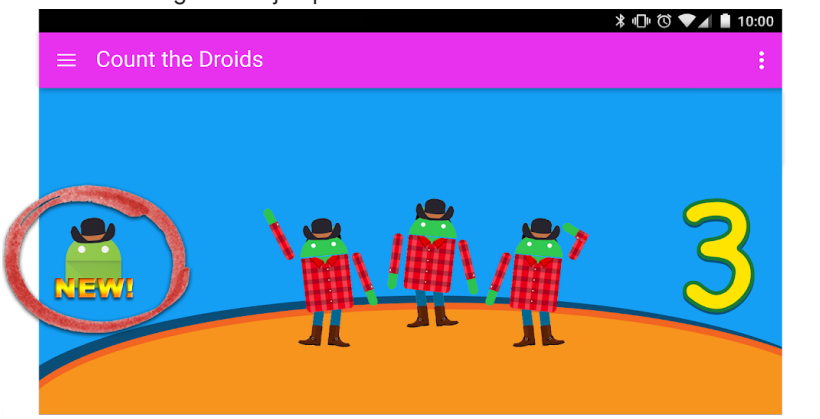
- Monetización y publicidad que ocupan la mayor parte de la pantalla del dispositivo sin brindarle al usuario una manera clara de descartarlos, como se muestra en el siguiente ejemplo:



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

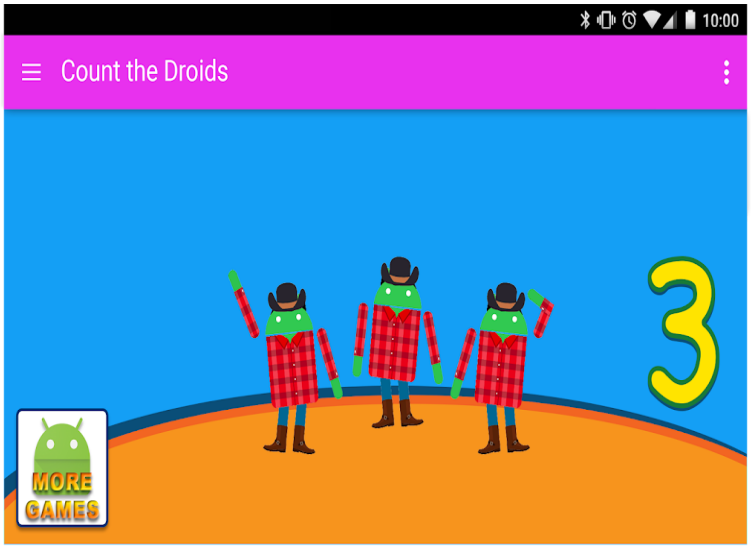


- Monetización y publicidad que el usuario podría confundir con contenido de la aplicación, como se muestra en el siguiente ejemplo:



- Botones, anuncios o cualquier otro componente de monetización que promuevan sus otras fichas de Google Play Store, pero que no se distingan del contenido de la aplicación, 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 gráfico y violento que no sea apto para niños.

Entrada en vigencia: 1 de noviembre de 2022

SDK de Anuncios

Si publica anuncios en su aplicación y su público objetivo solo incluye niños, debe usar únicamente SDK de anuncios con autocertificación para Familias . Si el público objetivo de su aplicación incluye niños y usuarios mayores, debe implementar medidas para filtrar por edad, como una pantalla neutral de comprobación de edad , y asegurarse de que los anuncios que se muestran a niños provengan exclusivamente de SDK de anuncios con autocertificación para Familias. Las aplicaciones que participan en el programa Diseñado para familias solo pueden usar SDK de anuncios con autocertificación.

Consulte la página de la política del Programa de SDK de Anuncios con Autocertificación para Familias para obtener más detalles sobre estos requisitos y consultar la lista actual de SDK de anuncios con autocertificación.

Si usa AdMob, consulte el Centro de ayuda de AdMob para obtener más detalles sobre sus productos.

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

Compras directas desde la aplicación

Google Play volverá a autenticar a todos los usuarios antes de que se complete cualquier compra directa desde la aplicación en las aplicaciones que participen en el programa Diseñado para familias. 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.

Enforcement

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

Alcance de las políticas

Nuestras políticas 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 sobre cómo 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 .

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 sus 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 una actualización que cumpla con las políticas.
- Ya no puedes usar el APK ni el paquete de aplicación 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.
- Ese estado tampoco afecta la capacidad de los usuarios de ver la ficha de Play Store, las instalaciones, las estadísticas y las calificaciones existentes de la app.

Restricción por Regiones

- Los usuarios pueden descargar su aplicación mediante Google Play solo en determinadas regiones.
- Los usuarios de otras regiones no podrán encontrar la aplicación en Play Store.
- Los usuarios que hayan instalado la aplicación podrán seguir usándola en sus dispositivos, pero ya no recibirán actualizaciones.
- La restricción por regiones no afecta el estado de su cuenta de desarrollador de Google Play.

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 rescindirá 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 mientra se lleva a cabo la rescisión de una de tus otras cuentas.

Cuentas Inactivas

Las cuentas inactivas son cuentas de desarrollador que no están en uso o que se abandonaron, y, por lo tanto, no están en regla según el Acuerdo de Distribución para Desarrolladores .

Las Cuentas de Desarrollador de Google Play están destinadas a desarrolladores activos que publican aplicaciones y llevan a cabo un mantenimiento continuo de ellas. Con el fin de evitar casos de abuso, cerramos las cuentas que están inactivas o que no se utilizan o involucran con frecuencia, por ejemplo, para publicar y actualizar aplicaciones, acceder a estadísticas o administrar fichas de Play Store.

Si su cuenta está inactiva, se borrará junto con todos los datos asociados a ella. Además, no se le devolverá el valor de la tarifa de registro, dado que no es reembolsable. Antes de cerrar su cuenta por estar inactiva, usaremos la información de contacto que proporcionó en ella para enviarle una notificación.

El cierre de una cuenta inactiva no limita su capacidad para crear una cuenta nueva en el futuro si decide volver a publicar aplicaciones en Google Play. Sin embargo, no podrá reactivar la cuenta anterior, y las aplicaciones o los datos asociados a ella no estarán disponibles en la cuenta nueva.

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 asistencia de este tipo, consulta a un asesor legal.

- Verificación de apps
- Cómo denunciar incumplimientos de políticas
- Comunícate con Google Play para obtener detalles sobre la rescisión de una cuenta o la eliminación de una aplicación
- Advertencias
- Cómo denunciar aplicaciones y comentarios inapropiados
- Se eliminó mi aplicación de Google Play
- Información sobre la rescisión de cuentas de desarrollador de Google Play

---

Requisitos de Play Console

Google Play tiene como objetivo brindar a los usuarios experiencias seguras y maravillosas con las aplicaciones, así como una gran oportunidad para que todos los desarrolladores puedan alcanzar el éxito. Nos esforzamos por garantizar que el proceso de publicar su aplicación para los usuarios sea lo más simple posible.

Para evitar los incumplimientos comunes que podrían enlentecer el proceso de revisión o generar un rechazo, tenga en cuenta los requisitos que se indican a continuación a la hora de enviar información a través de Play Console.

Antes de enviar su aplicación, debe hacer lo siguiente:

- Proporcionar con exactitud toda la información y los metadatos de su aplicación
- Asegurarse de que su información de contacto esté actualizada
- Subir la política de privacidad de la aplicación y completar los requisitos relacionados con la sección de **Seguridad de los datos**
- Proporcionar una cuenta de demostración activa, así como la información de acceso y todos los demás recursos necesarios para que revisemos su aplicación (es decir, credenciales de acceso, código QR, etcétera)

Como siempre, debe asegurarse de que su aplicación proporcione una experiencia del usuario estable, interesante y responsiva; compruebe que todos los elementos de su aplicación, incluidos los servicios de estadísticas, las redes de publicidad y los SDK de terceros, satisfagan las Políticas del Programa para Desarrolladores de Google Play, y si el público objetivo de su aplicación incluye niños, asegúrese de satisfacer nuestra Política de Familias.

Recuerde que es su responsabilidad revisar el Acuerdo de Distribución para Desarrolladores y todas las Políticas del Programa para Desarrolladores a fin de garantizar que su aplicación satisfaga a cabalidad todos los lineamientos.

Developer Distribution Agreement

¿Necesitas más ayuda?
Prueba estos próximos pasos:

Comunícate con nosotros
Cuéntanos más para que podamos ayudarte