Políticas del Programa para Desarrolladores

(con vigencia a partir del 1 de enero de 2026, a menos que se establezca 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.

Política de Estándares de la Seguridad de los Niños

Google Play requiere que las aplicaciones de citas y redes sociales satisfagan nuestra política de Estándares de la Seguridad de los Niños.

Estas aplicaciones deben cumplir con lo siguiente:

- **Tener Estándares Publicados:** Su aplicación debe prohibir explícitamente la Explotación y Abuso Sexual Infantil (CSAE) en estándares accesibles públicamente, como las condiciones del servicio de la aplicación, los lineamientos de la comunidad o cualquier otra documentación de la política del usuario disponible de manera pública.
- **Proporcionar un mecanismo en la aplicación para los comentarios de los usuarios:** Debe autocertificar que su aplicación proporciona un mecanismo para que los usuarios envíen comentarios, dudas o denuncias en ella.
- **Abordar el CSAM:** Debe autocertificar que su aplicación toma las medidas adecuadas, incluida, sin limitaciones, la de quitar el CSAM después de obtener conocimiento real de este en virtud de sus estándares publicados y las leyes pertinentes.
- **Satisfacer las Leyes de Seguridad de los Niños:** Debe realizar una autocertificación para acreditar que su aplicación satisface las leyes y reglamentaciones aplicables con respecto a la seguridad de los niños, lo que incluye, sin limitaciones, tener un proceso vigente para denunciar el CSAM confirmado al National Center for Missing and Exploited Children o a la autoridad regional relevante.
- **Proporcionar un Punto de Contacto para la Seguridad de los Niños:** Su aplicación debe proporcionar un punto de contacto designado para recibir notificaciones potenciales de Google Play sobre contenido de CSAE detectado en su aplicación o en su plataforma. Este representante debe estar en posición de defender los procedimientos de aplicación y revisión asociados a su aplicación, y de tomar medidas cuando sea necesario.

Obtenga más información sobre estos requisitos y cómo satisfacerlos en el artículo de nuestro Centro de ayuda.

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 ofrecer o promocionar un acto sexual a cambio de una compensación. No permitimos aplicaciones que incluyan contenido asociado con conductas sexualmente predatorias, o lo promuevan, o que distribuyan contenido sexual sin consentimiento. Se permite la publicación de contenido que incluya imágenes de desnudos si su objetivo principal es educativo, documental, científico o artístico, y no injustificado.

Las aplicaciones de catálogos, es decir, aplicaciones que incluyen títulos de libros o videos como parte de un catálogo de contenido más amplio, pueden distribuir títulos de libros (tanto libros electrónicos como audiolibros) o videos que incluyan contenido sexual, siempre que se cumplan los siguientes requisitos:

- Los títulos de libros o videos con contenido sexual representan una pequeña fracción del catálogo general de la aplicación.

- La aplicación no promueve activamente títulos de libros o videos con contenido sexual. Estos títulos pueden aparecer de todos modos en las recomendaciones basadas en el historial del usuario o durante las promociones generales de precios.
- La aplicación no distribuye ningún título de libro o video que incluya contenido de situación de riesgo para menores, pornografía o cualquier otro contenido sexual definido como ilegal por la ley aplicable.
- La aplicación protege a los menores por medio de la restricción del acceso a títulos de libros o videos con contenido sexual.

Si una aplicación incluye contenido que incumple 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 ubicaciones.

Los siguientes son ejemplos de incumplimientos comunes:

- 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 ofrecen o 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
- Contenido o conductas que intenten amenazar o explotar a las personas de una manera sexual, como fotos sexualizadas sin que el sujeto se dé cuenta, cámaras ocultas, contenido sexual sin consentimiento creado mediante deepfake o tecnología similar, o contenido de abuso

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Extremismo Violento

No permitimos que organizaciones terroristas u otras organizaciones o movimientos peligrosos que se hayan involucrado en actos de violencia contra civiles, o que se hayan preparado para cometerlos o se adjudiquen la responsabilidad de haberlos cometido, publiquen aplicaciones en Google Play para ningún fin, incluido el reclutamiento.

No permitimos aplicaciones que incluyan contenido relacionado con el extremismo violento, ni con la planificación, preparación o glorificación de la violencia contra civiles, como contenido que promueva actos terroristas, incite a la violencia o celebre ataques terroristas. Si publica contenido relacionado con el extremismo violento con fines educativos, documentales, científicos o artísticos, tenga presente que debe brindar 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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

Bullying y acoso

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

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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 o productos que contengan nicotina (como cigarrillos electrónicos, vaporizadores bolígrafo y bolsas de nicotina) ni que fomenten el consumo ilegal o inadecuado de alcohol, tabaco o nicotina.

Información adicional

- No se permite representar ni promover el uso o la venta de alcohol o tabaco a menores.
- No se permite insinuar que el consumo de tabaco puede mejorar la condición social, sexual, profesional, intelectual o atlética.
- No se permite mostrar el consumo excesivo de alcohol como algo positivo, incluida la representación favorable del consumo excesivo, sostenido o competitivo.
- No se permiten anuncios, promociones ni elementos destacados de productos relacionados con el tabaco (lo que incluye anuncios, banners, categorías y vínculos a sitios de venta de tabaco).
- Podríamos permitir la venta limitada de productos relacionados con el tabaco en aplicaciones de entrega de comida o artículos de almacén, en determinadas regiones y sujeto a protecciones de control de acceso por edad (como verificación de ID en la entrega).
- Podríamos permitir la venta de productos que se comercializan como ayudas para dejar de consumir nicotina, sujeto a protecciones de control de acceso por edad.

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 su aplicación contiene o promueve productos y servicios financieros, usted debe satisfacer las reglamentaciones estatales y locales de todas las regiones o países que incluya en la segmentación de su aplicación; por ejemplo, debe incluir las divulgaciones específicas que requiera la legislación local.

Las aplicaciones que contengan funciones financieras deben completar el Formulario de Declaración de Funciones Financieras disponible en Play Console.

Opciones binarias

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

Préstamos

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

- Ejemplos: Préstamos personales, préstamos inmediatos, 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)

Acceso al Salario Ganado: Definimos los préstamos de acceso al salario ganado (EWA) como un servicio financiero que permite que personas físicas tengan acceso a una parte de sus salarios que ya se haya ganado pero que sus empleadores no hayan pagado aún. A diferencia de los préstamos tradicionales, los servicios de EWA se caracterizan por lo siguiente:

- Mecanismo de Devolución: El préstamo se devuelve automáticamente por medio de una deducción de la nómina o de un pago automático vinculado a la cuenta bancaria del usuario. Si el pago automático no se realiza correctamente, no se aplican intereses, recargos ni comisiones adicionales.
- Acceso Basado en los Ingresos: El importe disponible para el usuario está estrictamente limitado a los salarios que ya se ganaron durante el período de pago en curso y excluye los ingresos futuros.
- Estructura de las Comisiones: Los servicios de EWA no cobran intereses y, en su lugar, cobran una comisión fija reducida o una comisión por transacción porcentual por el uso. Una comisión razonable sería mínima y transparente, y debe reflejar el costo real de la prestación del servicio sin que represente una carga para el usuario, posiblemente entre USD 1 y USD 5 por transacción, o 1% y 5% del adelanto.
- Sin Creación de Deuda: Los servicios de EWA normalmente no informan sobre sus transacciones a las agencias de informes crediticios, por lo tanto no afectan la calificación crediticia del usuario ni contribuyen a la creación de deuda a largo plazo.

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 aplicación "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 comisiones 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, que incluya el capital y todas las comisiones aplicables

- Una política de privacidad que divulgue de manera exhaustiva el acceso, la recopilación, la utilización y el uso compartido de datos personales y sensibles de los usuarios, sujeta a las restricciones que se describen en esta política

No permitimos 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").

Las aplicaciones que proporcionen préstamos de Acceso al Salario Ganado, incluidas, sin limitaciones, aquellas que ofrecen estos 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 aplicación "Finanzas" y divulgar la siguiente información en los metadatos de la aplicación:

- Los términos y condiciones del pago
- Todas las comisiones, incluidas las tarifas de suscripción, las comisiones por transacción y todas las demás comisiones relacionadas con la provisión del préstamo
- Un ejemplo representativo del costo total del préstamo, incluidas todas las comisiones aplicables
- Una política de privacidad que divulgue de manera exhaustiva el acceso, la recopilación, la utilización y el uso compartido de datos personales y sensibles de los usuarios, sujeta a las restricciones que se describen en esta política

Debemos poder establecer una conexión entre su cuenta de desarrollador y la documentación o las licencias proporcionadas que demuestren su capacidad para brindar servicios de préstamos personales. Es posible que se soliciten documentos o información adicionales para confirmar que su cuenta cumple con todas las leyes y reglamentaciones locales.

Se prohíbe que las aplicaciones de préstamos personales, las aplicaciones que tengan como fin principal facilitar el acceso a préstamos de este tipo (por ejemplo, facilitadoras o generadoras de clientes potenciales), las aplicaciones de líneas de crédito, las aplicaciones auxiliares de préstamos o créditos (calculadoras o guías de préstamos, etc.), y las aplicaciones de Acceso al Salario Ganado (EWA) accedan a datos sensibles, como fotos y contactos. Se prohíben los siguientes permisos:

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

Las aplicaciones que usan APIs o información sensible están sujetas a restricciones y requisitos adicionales. Consulte la política de Permisos para obtener información adicional.

Préstamos personales con TAE alta

En los Estados Unidos, no se permiten aplicaciones de préstamos personales en las que la tasa anual equivalente (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 implementa sobre las aplicaciones que ofrecen préstamos de forma directa, las que generan clientes potenciales y las que conectan a los consumidores con prestamistas externos.

Requisitos específicos de cada país

Las aplicaciones de préstamos personales diseñadas para los países mencionados deben satisfacer requisitos adicionales y proporcionar documentación complementaria como parte de la Declaración

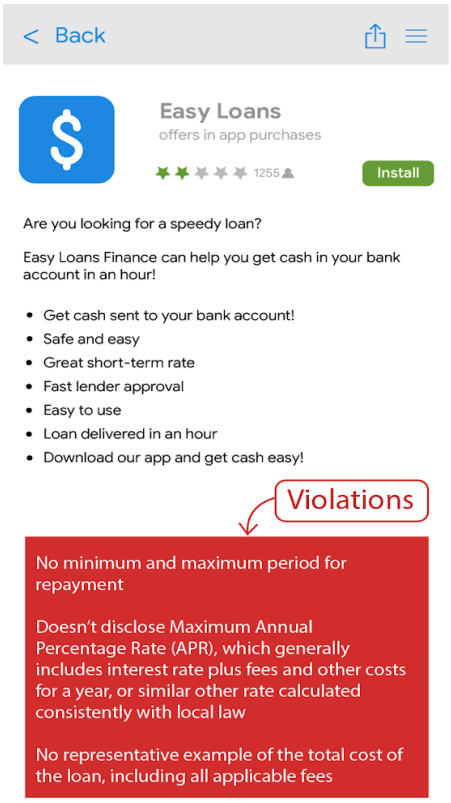
de funciones financieras en Play Console. Las aplicaciones que proporcionan préstamos de Acceso al Salario Ganado (EWA) están sujetas a estos requisitos en la medida aplicable en las jurisdicciones pertinentes. Usted deberá, a pedido de Google Play, proporcionar información o documentación adicional con relación a su cumplimiento de los requisitos regulatorios y de licencias aplicables.

1. **India**
   - 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 Entidades Financieras No Bancarias (NBFC) registradas, deberá reflejar esa información con exactitud en la declaración.
     - Además, los nombres de todos los bancos o NBFC registradas se deben divulgar de manera destacada en la descripción de la aplicación.
2. **Indonesia**
   - 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 Nº 77/POJK.01/2016 (además de las enmiendas que podrían implementarse ocasionalmente), debe enviar una copia de su licencia válida para que la revisemos.
3. **Filipinas**
   - 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, en la descripción de su aplicación 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).
   - Las aplicaciones involucradas en actividades de financiación colectiva basadas en préstamos, como préstamos entre pares (P2P), o según se define en virtud de las Reglas y Reglamentaciones que Rigen la Financiación Colectiva (Reglas de CF), deben procesar las transacciones a través de Intermediarios de CF registrados en la PSEC.
4. **Nigeria**
   - Los Prestamistas de Dinero Digital (DML) deben satisfacer y completar el MARCO PROVISIONAL LIMITADO DE REGULACIÓN Y REGISTRO, Y LAS PAUTAS PARA PRÉSTAMOS DIGITALES, 2022 (además de las enmiendas que podrían implementarse ocasionalmente), de la Comisión Federal de Competencia y Protección al Consumidor (FCCPC) de Nigeria, y obtener una carta de aprobación verificable de esa entidad.
   - Los Agregadores de Préstamos deben proporcionar la documentación o certificación correspondiente para los servicios de préstamos digitales, y los detalles de contacto de cada DML asociado.
5. **Kenia**
   - Los Proveedores de Crédito Digital (DCP) deben completar el proceso de registro de DCP y obtener una licencia del Banco Central de Kenia (CBK). Como parte de la declaración, debe proporcionar una copia de la licencia emitida por el CBK.
   - 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 DCP registrados, deberá reflejar esa información con exactitud en la declaración y proporcionar copias de las licencias de DCP de sus respectivos socios.
   - Por el momento, solo aceptamos declaraciones y licencias de entidades publicadas en el Directorio de Proveedores de Crédito Digital que se incluye en el sitio web oficial del CBK.
6. **Pakistán**

- Cada prestamista de Empresas Financieras No Bancarias (NBFC) puede publicar solo una Aplicación de Préstamos Digitales (DLA). Los desarrolladores que intenten publicar más de una DLA por NBFC corren el riesgo de que se cierre su cuenta de desarrollador y cualquier otra cuenta asociada.
- Debe enviar un comprobante de aprobación de la SECP para ofrecer o facilitar servicios de préstamos digitales en Pakistán. Además, no se permiten aplicaciones de préstamos a corto plazo; sin embargo, podrían considerarse excepciones poco frecuentes cuando las leyes y reglamentaciones de Pakistán lo permitan explícitamente.

7. **Tailandia**
   - Las aplicaciones de préstamos personales diseñadas para Tailandia con tasas de interés iguales o superiores al 15% deben obtener una licencia válida del Banco de Tailandia (BoT) o del Ministerio de Finanzas (MoF). Los desarrolladores deben proporcionar documentación que demuestre su capacidad para ofrecer o facilitar préstamos personales en Tailandia. Esta documentación debe incluir lo siguiente:
     - Una copia de su licencia emitida por el Banco de Tailandia para operar como organización de nanofinanzas o proveedor de préstamos personales
     - Una copia de su licencia comercial emitida por el Ministerio de Finanzas para operar como proveedor de préstamos Pico o Pico-plus

El siguiente es un ejemplo de incumplimiento común:



Juegos de apuestas, concursos y juegos con dinero real

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

Aplicaciones de Juegos de Apuestas

Conforme a las restricciones y el cumplimiento de todas las políticas de Google Play, se permiten las 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

Ocasionalmente y en determinadas regiones, es posible que llevemos a cabo pruebas piloto por tiempo limitado para ciertos tipos de juegos con dinero real. Para obtener detalles, consulte esta página del Centro de ayuda. La prueba piloto de Juegos de Máquinas de Pinzas en Línea en Japón finalizó el 11 de julio de 2023. A partir del 12 de julio de 2023, se podrán publicar en Google Play aplicaciones de Juegos de Máquinas de Pinzas en Línea a nivel mundial, sujetas a la legislación aplicable y a ciertos requisitos.

Programas de lealtad lúdicos

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

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

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

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

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

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

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

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

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

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

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

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

Ejemplos de incumplimientos

- Una app diseñada para usuarios menores de edad que muestra un anuncio que promociona servicios de juegos de apuestas
- Un juego de casino simulado que promociona casinos con dinero real o dirige a los usuarios hacia ellos

- Una app de seguimiento de probabilidades deportivas que contiene anuncios de juegos de apuestas integrados que se vinculan a un sitio de apuestas deportivas
- Apps que tienen anuncios de juegos de apuestas que no cumplen con nuestra política de Anuncios Engañosos, como anuncios que aparecen a los usuarios en forma de botones, íconos u otros elementos interactivos en la app

Apps de deportes de fantasía diarios (DFS)

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

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

Actividades ilegales

No permitimos aplicaciones que faciliten o promuevan actividades ilegales.

Los siguientes son ejemplos de incumplimientos comunes:

- 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

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 medidas firmes, efectivas y continuas de moderación de CGU que cumplan con lo siguiente:

- Deben requerir que los usuarios acepten las condiciones de uso o políticas del usuario de la aplicación antes de crear o subir CGU.
- Deben 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.
- Deben implementar la moderación del CGU de forma razonable y coherente con los tipos de CGU que aloja la aplicación. Esto incluye proporcionar un sistema dentro de la aplicación que permita denunciar y bloquear CGU y a usuarios censurables, y tomar medidas contra ellos cuando corresponda. Los esfuerzos de moderación pueden variar según las diferentes experiencias de CGU. Por ejemplo:
  - Las aplicaciones que presentan CGU que identifica a un conjunto específico de usuarios con herramientas como la verificación de usuarios y el registro sin conexión (por ejemplo, aplicaciones que se usan exclusivamente dentro de una escuela o una empresa en particular, etc.) deben proporcionar funciones que permitan denunciar contenido y a usuarios.
  - Las funciones de CGU que permitan la interacción 1:1 entre usuarios específicos (por ejemplo, mensajes directos, etiquetado, menciones, etc.) deben proporcionar funciones dentro de la aplicación que permitan bloquear a usuarios.
  - Las aplicaciones con las que se pueda acceder a CGU de acceso público, como aplicaciones de redes sociales y blogs, deben implementar funciones que permitan denunciar contenido y a usuarios, así como bloquear a usuarios.
  - 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 inaceptable de RA (por ejemplo, una imagen de RA sexualmente explícita) como la ubicación de anclaje de RA sensible (por ejemplo, contenido de RA anclado a un área restringida, como una base militar, o a una propiedad privada donde el anclaje de RA podría causarle problemas al propietario).
- Deben 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 situaciones de riesgo para menores no se consideran "imprevistos" y están prohibidos.

Las aplicaciones con 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 (por ejemplo, detrás de una opción intersticial de ofuscación o excluido de la vista de forma predeterminada, a menos que se inhabilite la función de "búsqueda segura").
- Los niños, según se define en la política de Familias, tienen explícitamente prohibido acceder a su aplicación mediante sistemas de control de edad como una pantalla neutral de comprobación de edad o un sistema adecuado en virtud de lo definido por 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 Clasificaciones 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Aplicaciones Médicas y de Salud

Si su aplicación ofrece funciones o información relacionadas con la salud como parte de su funcionalidad, o accede a datos de salud para poder ofrecer funciones no relacionadas con la salud, debe satisfacer las Políticas para Desarrolladores de Google Play existentes, incluida la de Privacidad, Engaño y Abuso de Dispositivos, además de los siguientes requisitos:

- **Declaración de Console:**
  - Todos los desarrolladores deben completar el Formulario de declaración de apps de salud en la página Contenido de la app (Política > Contenido de la app) de Play Console. Obtenga más información sobre cómo proporcionar información para el Formulario de declaración de apps de salud.
- **Política de Privacidad y Requisitos de Divulgación Destacada:**
  - Su aplicación debe publicar un vínculo a la política de privacidad en el campo designado de Play Console, así como un vínculo a la política de privacidad o el texto correspondiente dentro de la aplicación en sí. Asegúrese de que la política de privacidad esté disponible en una URL activa, accesible públicamente, sin geovallado (no en PDF) y que no se pueda editar (según la sección de Seguridad de los datos).
  - En la política de privacidad de su aplicación, junto con cualquier otro aviso de divulgación integrado en la aplicación, se debe explicar detalladamente cómo se recopilan, usan y comparten los datos personales o sensibles del usuario, y cómo se accede a ellos, sin limitarse a los datos divulgados en la sección de Seguridad de los datos que se menciona más arriba. La aplicación debe cumplir con todos los requisitos de divulgación destacada y consentimiento correspondientes para cualquier funcionalidad o datos regulados por los permisos peligrosos o de tiempo de ejecución .
  - No deben solicitarse permisos que no sean necesarios para que una aplicación de salud ejecute su funcionalidad principal, y los que no se usen deben eliminarse. Para conocer la lista de permisos que se consideran dentro del alcance de los datos sensibles relacionados con la salud, consulte ¿Qué permisos están dentro del alcance de la política sobre apps de salud?
  - Si su aplicación no es primordialmente de salud, pero tiene funciones relacionadas con este tema y accede a datos de salud, igualmente se encuadra dentro del alcance de la política sobre Aplicaciones de Salud. Debe quedar clara para el usuario la conexión entre la funcionalidad principal de la aplicación y la recopilación de datos relacionados con la salud (por ejemplo, proveedores de seguros, aplicaciones de juegos que recopilan datos de la actividad del usuario como una manera de avanzar en el juego, etc.). La política de privacidad de la aplicación debe reflejar este uso limitado.
- **Funcionalidades Médicas y de Salud:**
  - No permitimos aplicaciones con funcionalidades médicas o de salud que sean engañosas o posiblemente perjudiciales.

- Las aplicaciones que se conectan a hardware o dispositivos externos (p. ej., medidores de glucemia) para realizar su función médica deben divulgar claramente estos requisitos de hardware externo en su descripción. No deben dar a entender que pueden funcionar de manera independiente del hardware externo requerido.
- Las aplicaciones que usan sensores del dispositivo (por ejemplo, la cámara) para posibilitar funciones de salud deben indicar información clara sobre compatibilidad con el dispositivo en su descripción. Por ejemplo, las aplicaciones con funcionalidad de oximetría que usan únicamente sensores del dispositivo deben divulgar de forma adecuada qué modelos de dispositivos admiten dicha funcionalidad.
- Las aplicaciones que hayan recibido autorización o aprobación reglamentaria como dispositivos médicos deben proporcionar prueba de dicha aprobación cuando se les solicite. Las aplicaciones que no estén reguladas y aprobadas por una autoridad sanitaria pertinente deben incluir una renuncia de responsabilidad clara que indique que no son dispositivos médicos y no diagnostican, tratan, curan ni previenen ninguna afección.
- Las aplicaciones también deben recordar a los usuarios que consulten a un profesional de la salud para recibir asesoramiento médico, diagnóstico o tratamiento.

- **Requisitos adicionales:**
  Si su aplicación de salud cumple con las condiciones para una de las siguientes designaciones, debe satisfacer los requisitos correspondientes:
  - **Aplicaciones de salud Afiliadas al Gobierno:** Si tiene permiso del gobierno o una organización de cuidado de la salud reconocida para desarrollar y distribuir una aplicación en afiliación con ellos, debe enviar una prueba de elegibilidad por medio del Formulario de Aviso Anticipado.
  - **Aplicaciones de Rastreo de Contactos o Estado de Salud:** Si su aplicación es de rastreo de contactos o de supervisión del estado de salud, debe seleccionar "Prevención de Enfermedades y Salud Pública" en Play Console y proporcionar la información solicitada a través del formulario de aviso anticipado antes mencionado.
  - **Aplicaciones de Investigación con Seres Humanos:** Las aplicaciones que sirven para llevar a cabo investigaciones con seres humanos relacionadas con la salud deben seguir todas las reglas y reglamentaciones, incluida, sin limitaciones, la obtención del consentimiento informado de los participantes o, en el caso de menores, de sus madres, padres o tutores. Las aplicaciones para la investigación de la salud también deben obtener aprobación por parte de una Junta de Revisión Institucional (IRB) o comité de ética independiente equivalente, a menos que estén exentas de alguna manera. Se debe proporcionar el comprobante de esa aprobación cuando se solicite.

Para obtener más información sobre las aplicaciones médicas y de salud, consulte este artículo del Centro de ayuda.

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 .

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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

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

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 .

Contenido basado en Cadenas de Bloques

Ante la rápida evolución de la tecnología de cadenas de bloques, nuestro objetivo es ofrecer una plataforma innovadora donde los desarrolladores puedan perfeccionarse y crear experiencias más inmersivas y enriquecidas para los usuarios.

Para los efectos de esta política, consideramos que el contenido basado en cadenas de bloques son recursos digitales con asignación de tokens protegidos en una cadena de bloques. Si su aplicación

incluye contenido basado en cadenas de bloques, debe satisfacer estos requisitos.

Exchanges de Criptomonedas y Billeteras de Software

Las prácticas de compra, retención o intercambio de criptomonedas deben llevarse a cabo a través de servicios certificados en jurisdicciones reguladas.

Además, usted debe satisfacer la reglamentación aplicable de cualquier región o país al que se oriente su aplicación y evitar publicar la aplicación en los territorios donde sus productos o servicios estén prohibidos. Google Play puede solicitarle que proporcione información o documentación adicional relacionadas con su cumplimiento de los requisitos regulatorios y de licencias aplicables.

Criptominería

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

Requisitos de Transparencia para Distribuir Recursos Digitales con Asignación de Tokens

Si su aplicación vende Recursos Digitales con Asignación de Tokens o permite que los usuarios los obtengan, debe declarar esta característica en el formulario de declaración de Funciones Financieras disponible en la página Contenido de la app de Play Console.

Cuando cree un producto integrado en la aplicación, deberá indicar en los detalles del producto que este representa un Recurso Digital con Asignación de Tokens Para obtener más orientación, consulte el artículo Crea un producto integrado en la aplicación.

No se permite promocionar ni realzar la posibilidad de obtener ganancias potenciales a partir de actividades de juego o intercambio.

Requisitos Adicionales para la Ludificación de NFTs

Según exige la Política de Juegos, Concursos y Juegos de Apuestas con Dinero Real de Google Play, las aplicaciones de juegos de apuestas que integren recursos digitales con asignación de tokens, como NFTs, deberán completar el proceso de solicitud correspondiente.

En el caso de todas las demás aplicaciones que no cumplan con los requisitos de elegibilidad de las aplicaciones de juegos de apuestas y que no se incluyan en los Otros Pilotos de Juegos con Dinero Real, no se debe aceptar nada que tenga valor monetario a cambio de una oportunidad de obtener un NFT de valor desconocido. Los NFTs que compren los usuarios se deben poder consumir o usar en el juego para mejorar la experiencia de los jugadores o ayudarlos a progresar en el título. Los NFTs no se deben usar para hacer apuestas a cambio de la oportunidad de ganar premios con valor en moneda real (incluidos otros NFTs).

Los siguientes son ejemplos de incumplimientos comunes:

- Aplicaciones que venden paquetes de NFTs sin divulgar el contenido específico ni los valores de los NFTs
- Juegos sociales de casino en los que los jugadores pagan por jugar, como máquinas tragamonedas, que otorgan NFTs como recompensa

Contenido generado por IA

En vista de que hay cada vez más modelos de IA generativa disponibles para desarrolladores, seguramente considerará incorporar alguno de ellos en sus aplicaciones para aumentar la interacción y mejorar la experiencia del usuario. Google Play quiere garantizar que el contenido generado por IA sea seguro para todos los usuarios y que los comentarios de estos se tengan en cuenta para llevar a cabo una innovación responsable.

Contenido Generado por IA

El contenido generado por IA es aquel que se crea con modelos de IA generativa a partir de instrucciones de los usuarios. Estos son algunos ejemplos de contenido generado por IA:

- Chatbots de IA generativa de conversación texto a texto en los que una de las funciones principales de la aplicación es interactuar con el chatbot
- Imágenes o videos generados por IA a partir de instrucciones de texto, imágenes o voz

Para garantizar la seguridad de los usuarios y en virtud del Alcance de las Políticas de Google Play, las aplicaciones que generen contenido con IA deberán satisfacer las Políticas para Desarrolladores de Google Play existentes, incluidas aquellas que prohíben y evitan la generación de Contenido Restringido, como contenido que facilite el abuso o la explotación infantil, y contenido que dé lugar a un Comportamiento Engañoso.

Para obtener recursos relacionados con las prácticas recomendadas del sector para la protección de aplicaciones de IA generativa, consulte nuestro artículo del Centro de ayuda.

Las aplicaciones que generen contenido mediante IA deberán contener funciones que permitan a los usuarios marcar contenido ofensivo o informar acerca de este a los desarrolladores sin la necesidad de salir de la aplicación. Los desarrolladores, a su vez, deberán usar los informes de los usuarios para ajustar la moderación y los filtros de contenido en sus aplicaciones.

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.

Los siguientes son ejemplos de incumplimientos comunes:

- Material gráfico para álbumes de música, videojuegos y libros
- Imágenes de comercialización de películas, televisión o videojuegos.

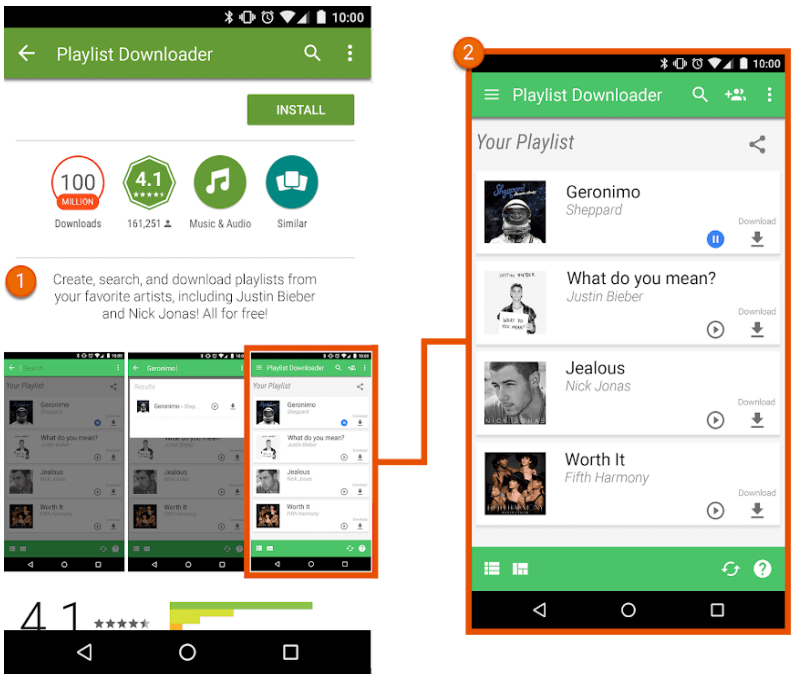
- Material gráfico o imágenes de libros de cómics, dibujos animados, películas, videos de música o televisión.
- Logotipos de equipos deportivos profesionales y universitarios.
- Fotos tomadas de la cuenta de medios sociales de una persona pública.
- Imágenes profesionales de personas públicas.
- Reproducciones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

Los siguientes son ejemplos de incumplimientos comunes:

- 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 transparente en la manera en que maneja los datos de los usuarios (por ejemplo, información recopilada sobre un usuario o de parte de este, incluida la información del dispositivo). Es decir, debe divulgar si su aplicación accede a los datos, y si los recopila, usa, maneja y comparte, además de limitar su uso a los fines divulgados que satisfagan las políticas. Tenga en cuenta que cualquier tipo de manejo de datos sensibles y personales de los usuarios también está sujeto a los requisitos adicionales que se incluyen en la sección "Datos Sensibles y Personales del Usuario" más adelante. Además de esta y las demás Políticas del Programa para Desarrolladores de Play, debe satisfacer en todo momento las leyes de privacidad y protección de datos aplicables en las jurisdicciones donde ofrezca sus productos o servicios. Por ejemplo, si ofrece sus servicios a usuarios de la Unión Europea, tenga en cuenta que la Autoridad Francesa de Protección de Datos (CNIL) adoptó una guía sobre prácticas recomendadas para la protección de datos personales en el entorno de dispositivos móviles que podría resultarle útil como referencia.

Si incluye código de terceros (por ejemplo, SDK) en su aplicación, debe garantizar que tanto ese código como las prácticas de los terceros en cuestión relacionadas con los datos de los usuarios de su aplicación satisfagan las Políticas del Programa para Desarrolladores de Google Play, que incluyen requisitos de uso y divulgación. Por ejemplo, debe garantizar que sus proveedores de SDKs no vendan los datos sensibles y personales de los usuarios recopilados en su aplicación. Este requisito se aplica independientemente de si los datos de los usuarios se transfieren después de enviarse a un servidor o a través de la incorporación de código de terceros en su aplicación.

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, los contactos, la ubicación del dispositivo, SMS y llamadas; datos de salud y de Health Connect; inventario de otras aplicaciones en el dispositivo, el micrófono y la cámara, y otros datos sensibles relacionados de uso o del dispositivo. Si su aplicación maneja datos sensibles y personales de los usuarios, asegúrese de hacer lo siguiente:

- Limite el acceso, la recopilación, el uso y el uso compartido de los datos sensibles y personales de los usuarios adquiridos desde la aplicación a los fines de la funcionalidad del servicio y de la aplicación que satisfagan las políticas y las expectativas razonables de los usuarios:

- Las aplicaciones que extiendan el uso de datos sensibles y personales de los usuarios a la publicación de anuncios deben satisfacer la Política de Anuncios de Google Play.
- También puede transferir datos a los proveedores de servicios cuando sea necesario o por motivos legales, tales como cumplir con una solicitud gubernamental válida o la legislación aplicable, o como parte de una fusión o adquisición, habiendo proporcionado una notificación legal adecuada a los usuarios.

- Maneje todos los datos sensibles y personales 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.
  - "Venta" significa el intercambio o la transferencia de datos sensibles y personales de los usuarios con un tercero a cambio de una contraprestación económica.
    - La transferencia de datos sensibles y personales de los usuarios iniciadas por estos (por ejemplo, cuando el usuario usa una función de la aplicación para transferir un archivo a un tercero o casos en los que elige usar una aplicación de estudio de investigación de propósito exclusivo) no se consideran ventas.

Requisito de Divulgación Destacada y Consentimiento

En los casos en que el acceso, la recopilación, el uso o el uso compartido de los datos sensibles y personales de los usuarios del producto o la función en cuestión puedan no caber dentro de las expectativas razonables de estas personas (por ejemplo, si la recopilación de datos se produce en segundo plano cuando el usuario no está interactuando con la aplicación), deberá cumplir con los siguientes requisitos:

Divulgación destacada: Debe proporcionar una divulgación integrada en la aplicación sobre su acceso, recopilación, uso y uso compartido de los datos. 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.

Consentimiento y permisos de tiempo de ejecución: Las solicitudes de consentimiento del usuario integradas en la aplicación y las solicitudes de permisos de tiempo de ejecución deben estar precedidas inmediatamente por una divulgación integrada en la aplicación que cumpla con el requisito de esta política. 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 (por ejemplo, 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.
- El usuario debe otorgar el consentimiento antes de que la aplicación pueda recopilar datos sensibles y personales, o acceder a ellos.

Las aplicaciones que utilicen otras bases legales como justificación para procesar datos sensibles y personales de los usuarios sin consentimiento, como el interés legítimo contemplado por el GDPR de la UE, deben cumplir con todos los requisitos legales aplicables y realizar las divulgaciones correspondientes a los usuarios, incluidas las divulgaciones integradas en la aplicación que se requieren para satisfacer esta política.

Para cumplir con los requisitos de la política, le recomendamos que aplique el siguiente ejemplo de formato de Divulgación Destacada cuando sea necesario:

- "[Esta aplicación] recopila, transmite, sincroniza o almacena [tipos de datos] para permitir ["función"], [en determinado caso]".
- *Por ejemplo, "Fitness Funds recopila datos de ubicación para permitir el seguimiento de entrenamientos, incluso cuando la aplicación está cerrada o no está en uso, y también se usa como medio para publicar 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".*

Si su aplicación integra código de terceros (por ejemplo, SDK) diseñado para recopilar datos sensibles y personales de los usuarios de forma predeterminada, deberá, en un plazo de 2 semanas a partir de recibir la solicitud de Google Play (o bien, si la solicitud de Google Play permite más tiempo, dentro del período correspondiente), proporcionar evidencia suficiente que demuestre que su aplicación cumple con los requisitos de Divulgación Destacada y Consentimiento de esta política, incluso en relación con el acceso, la recopilación, el uso y el uso compartido de los datos mediante código de terceros.

Los siguientes son ejemplos de incumplimientos comunes:

- 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 aplicación 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 aplicación 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 aplicación 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
- Una aplicación con un SDK que recopila datos sensibles y personales de los usuarios, y no trata esta información como sujeta a la Política de Datos del Usuario en cuestión y a los requisitos de divulgación destacada y consentimiento, acceso y manejo de datos (incluida la venta no permitida).

Consulte este artículo para obtener más información sobre el Requisito de Divulgación Destacada y Consentimiento.

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

Para cada aplicación, los desarrolladores deben completar una sección clara y precisa de Seguridad de los datos 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, sin limitarse a los datos divulgados en la sección de Seguridad de los datos. 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 la aplicación y luego 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.

Requisito de Eliminación de Cuentas

Si su aplicación permite que los usuarios creen una cuenta desde ella, también debe permitirles que soliciten que se elimine la cuenta. Los usuarios deben tener una opción fácilmente detectable para iniciar la eliminación de la cuenta de la aplicación dentro y fuera de ella (p. ej., si visitan su sitio web). Se debe ingresar un vínculo a este recurso web en el campo del formulario de la URL designada de Play Console.

Cuando elimine una cuenta de la aplicación en función de la solicitud de un usuario, también debe eliminar los datos del usuario asociados con esa cuenta de la aplicación. La desactivación, la inhabilitación o el bloqueo temporales de la cuenta de la aplicación no califican como eliminación de la cuenta. Si necesita retener ciertos datos por motivos legítimos, como la seguridad, la prevención de fraudes o el cumplimiento regulatorio, debe informar claramente a los usuarios sobre sus prácticas de retención de datos (por ejemplo, en su política de privacidad).

Para obtener más información sobre los requisitos de la política de eliminación de cuentas, revise este artículo del Centro de ayuda. Si desea obtener información adicional para actualizar su formulario de seguridad de los datos, visite este artículo.

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 .

Marcos de Privacidad de Datos UE-EE.UU., del Reino Unido y de Suiza

Si procesa o usa información personal compartida por Google que identifique de forma directa o indirecta a alguna persona física, o bien accede a ella, y esos datos se originaron en el Espacio Económico Europeo, el Reino Unido o Suiza (“Información Personal de la UE”), tenga en cuenta lo siguiente:

- Debe satisfacer todas las leyes, directivas, reglamentaciones y reglas aplicables de privacidad, protección de datos y seguridad de los datos.
- Debe procesar o usar la Información Personal de la UE, o acceder a estos datos, únicamente para fines acordes con el consentimiento otorgado por la persona física a la cual se refiere dicha

información.

- Debe implementar medidas organizativas y técnicas apropiadas para proteger la Información Personal de la UE frente a cualquier pérdida, uso inadecuado y acceso, divulgación, alteración o destrucción no autorizados o ilícitos.
- Debe proporcionar el mismo nivel de protección que requieren los Principios del Marco de Privacidad de Datos o el mecanismo de transferencia aplicable, tal como se describe en las Condiciones de Protección de Datos entre Responsables del Tratamiento de Datos de Google.

Debe supervisar con frecuencia que cumple con estas condiciones. Si en algún momento no puede cumplir con estas condiciones (o si existe un riesgo significativo de que no pueda satisfacerlas), debe notificárnoslo de inmediato por correo electrónico a data-protection-office@google.com y dejar de procesar Información Personal de la UE de inmediato, o bien tomar las medidas razonables y pertinentes para restablecer un nivel de protección adecuado.

Permisos y API que Acceden a Información Sensible

Las solicitudes de permisos y el uso de APIs que accedan a información sensible deben tener un sentido claro para los usuarios. Solo puede solicitar permisos y usar APIs 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 APIs que accedan a información sensible que otorgue acceso a los datos del usuario o del dispositivo para funciones o fines no divulgados, no implementados o no autorizados. No se permite vender los datos sensibles o personales que se obtengan mediante permisos o APIs que accedan a información sensible, ni compartirlos para facilitar una venta.

Solicite permisos y use APIs 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 de usuarios o dispositivos a los que se accede mediante Permisos Restringidos se consideran datos sensibles y personales de los usuarios. En este caso, se aplican los requisitos de la política de Datos del Usuario .
- Se debe respetar la decisión de los usuarios si rechazan una solicitud de Permisos Restringidos y no se debe manipular ni forzar a los usuarios para que den su consentimiento a ningún 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 (por ejemplo, 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 que infrinjan las políticas de software malicioso de Google Play (incluidas las relacionadas con 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` se restringe 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 (por ejemplo, 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 las funciones principales 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"), por ejemplo, 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.

Permiso Solicitar Paquetes de Instalación

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

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

Las funcionalidades permitidas incluyen las siguientes:

- Búsqueda o navegación web
- Servicios de comunicación que admitan archivos adjuntos
- Uso compartido, transferencia o administración de archivos

- Administración de dispositivos empresariales
- Copia de seguridad y restablecimiento
- Migración de Dispositivo o Transferencia Telefónica
- Aplicación Complementaria para sincronizar el teléfono con el dispositivo wearable o IoT (por ejemplo, reloj inteligente o smart TV)

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 promocionarse 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.

Permisos de Sensores Corporales

Los datos provenientes de sensores que miden parámetros físicos del cuerpo (como la frecuencia cardíaca, la saturación de oxígeno en sangre (SpO_2) y la temperatura cutánea) se consideran información personal y sensible de los usuarios**.** Las aplicaciones que solicitan acceso a ellos están sujetas a los requisitos que se describen en la política de Datos del Usuario y la política sobre Aplicaciones de salud. Esto se aplica a las solicitudes de los permisos `android.permission.BODY_SENSORS` y `android.permission.BODY_SENSORS _BACKGROUND` en todos los factores de forma, incluidos teléfonos, tablets y dispositivos Wear OS.

En Android 16 y versiones posteriores, el permiso amplio `BODY_SENSORS` está en proceso de transición hacia permisos `android.permissions.health.*` más detallados y que preservan más la privacidad para tipos de datos específicos (por ejemplo, `android.permission.health.READ_HEART_RATE` , `android.permission.health.READ_OXYGEN_SATURATION` y `android.permission.health.READ_SKIN_TEMPERATURE`).

Las aplicaciones orientadas a Android 16 o versiones posteriores deben usar estos permisos específicos para las APIs que antes requerían `BODY_SENSORS` . Consulte la página Cambios en el comportamiento: apps orientadas a Android 16 o versiones posteriores para obtener todos los detalles.

Todas las solicitudes de permisos para sensores corporales (tanto permisos heredados como los nuevos permisos detallados) pasarán por un proceso de revisión para garantizar que el uso previsto de estos datos personales y sensibles se ajuste a los casos de uso aprobados que aportan un beneficio directo a los usuarios. Estos casos se centran principalmente en funciones relacionadas con el seguimiento de la actividad física y el bienestar (por ejemplo, el monitoreo de entrenamientos en tiempo real), la supervisión médica o de afecciones específicas, la investigación sobre la salud (con las aprobaciones correspondientes) o la mejora de funciones de aplicaciones complementarias para wearables.

Para obtener una orientación completa sobre las políticas, incluidos los usos prohibidos, los casos de uso aceptables y los requisitos detallados, consulte Permisos de Android Health: Orientación y preguntas frecuentes.

Permisos para Health Connect de Android

Health Connect es una plataforma de Android que permite que las aplicaciones de salud y fitness almacenen y compartan los mismos datos en el dispositivo, dentro de un ecosistema unificado. También ofrece un lugar centralizado para que los usuarios controlen qué aplicaciones pueden leer y

escribir datos de salud y fitness, lo que incluye registros de salud. Los Registros de Salud pueden incluir historias clínicas, diagnósticos, tratamientos, medicamentos, resultados de laboratorio y otros datos clínicos obtenidos de instituciones o proveedores de atención médica, o a través de plataformas de salud compatibles de terceros.

Health Connect admite la lectura y escritura de una variedad de tipos de datos , desde pasos hasta temperatura corporal y datos de registros de salud.

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. Si su aplicación califica como aplicación de salud o tiene funciones relacionadas con la salud, y accede a datos de salud (incluidos los datos de Health Connect), también debe satisfacer la política sobre Aplicaciones de salud.

Consulte esta guía para desarrolladores de Android sobre cómo comenzar a usar Health Connect. Para solicitar acceso a los tipos de datos de Health Connect y ver otras preguntas frecuentes, consulte el artículo de orientación y preguntas frecuentes sobre los permisos de salud de Android.

Las aplicaciones que se distribuyen en Google Play deben cumplir con los siguientes requisitos de las políticas para leer o escribir datos en Health Connect.

Acceso y Uso Adecuados de Health Connect

Health Connect solo se puede usar de acuerdo con las políticas y los términos y condiciones aplicables, y para los casos de uso aprobados según se describe en esta política. Esto significa que solo puede solicitar acceso a los permisos cuando su aplicación o servicio cumpla con uno de los casos de uso aprobados.

Los casos de uso aprobados incluyen fitness y bienestar, recompensas, entrenamiento físico, bienestar corporativo, investigación y atención médica, y juegos. Las aplicaciones a las que se les otorgó acceso para estos casos de uso no deben extender su utilización a fines no permitidos o no divulgados.

Solo podrán solicitar acceso a los Permisos de Health Connect los servicios o las aplicaciones que tengan una o más funciones diseñadas para beneficiar la salud y el estado físico de los usuarios. Por ejemplo:

- Aplicaciones o servicios que les permitan a los usuarios **registrar, informar, supervisar o analizar directamente** su actividad física, sueño, bienestar mental, nutrición, mediciones de salud, descripciones físicas, registros de salud y otras descripciones y mediciones relacionadas con salud y fitness
- Aplicaciones o servicios que les permitan a los usuarios **almacenar su actividad física, sueño, bienestar mental, nutrición, mediciones de salud, descripciones físicas**, **registros de salud** y otras descripciones y mediciones relacionadas con salud y fitness en sus dispositivos, y compartir sus datos con otras aplicaciones integradas en los dispositivos que satisfagan estos casos de uso
- Aplicaciones o servicios que les permitan a los usuarios tratar afecciones crónicas, seguir tratamientos médicos o acceder a servicios de atención médica

Health Connect no deberá usarse incumpliendo esta política o cualquier otra política o términos y condiciones aplicables de Health Connect, lo que incluye los siguientes propósitos:

- No use Health Connect para desarrollar aplicaciones, entornos o actividades en los que se prevea de manera razonable que el uso o la falla de Health Connect podría provocar la muerte, lesiones personales, o bien daños a personas físicas, al medioambiente o a la propiedad (como la creación o la puesta en funcionamiento de instalaciones nucleares, controles de tráfico aéreo, sistemas de soporte vital o armamento). Tampoco deberá usar Health Connect para su incorporación en aplicaciones, entornos o actividades de las características mencionadas.
- No acceda a datos obtenidos a partir de Health Connect con aplicaciones sin interfaz gráfica. Las aplicaciones deben mostrar un ícono claramente identificable en la bandeja de aplicaciones, admitir

la configuración en el dispositivo, mostrar íconos de notificaciones, etcétera.

- No use Health Connect con aplicaciones que sincronicen datos entre plataformas o dispositivos incompatibles.
- No use Health Connect para conectarse a aplicaciones, servicios o funciones que estén dirigidas exclusivamente a niños.
- Tome medidas razonables y adecuadas para proteger todas las aplicaciones o sistemas que usen Health Connect contra el acceso, el uso, la destrucción, la pérdida, la alteración o la divulgación que no estén autorizados o no sean legales.

También es responsabilidad suya garantizar el cumplimiento de cualquier requisito legal o reglamentario que se aplique según su uso previsto de Health Connect y los datos de Health Connect. Por ejemplo, si usted es una entidad cubierta o un socio comercial sujeto a la Ley de Responsabilidad y Portabilidad de Seguros Médicos (HIPAA), debe satisfacer los requisitos aplicables para acceder a la información de Health Connect y usarla. Si usted es un desarrollador sujeto al Reglamento General de Protección de Datos (RGPD) para usuarios de la UE, debe cumplir las obligaciones respectivas en virtud del RGPD. Estas leyes y reglamentaciones pueden exigirle celebrar otros acuerdos (por ejemplo, un Acuerdo entre Socios Comerciales o de Tratamiento de Datos) con las entidades pertinentes involucradas en sus actividades de tratamiento de datos antes de poder divulgarles información. También es responsabilidad de los desarrolladores de aplicaciones determinar si sus actividades requieren la celebración de dichos acuerdos. Los desarrolladores deben proporcionarle a Google evidencia de tales acuerdos o del cumplimiento correspondiente si así se les solicitara.

A excepción de lo que se detalla explícitamente en las etiquetas o la información que proporciona Google para sus productos o servicios específicos, Google no recomienda el uso ni garantiza la precisión de los datos incluidos en Health Connect para cualquier uso o propósito, y, en particular, para usos médicos o relacionados con la salud o la investigación. Google renuncia a toda responsabilidad asociada con el uso de datos obtenidos con Health Connect.

Uso Limitado

Cuando use Health Connect, el acceso a los datos y el uso que haga de ellos deben cumplir con limitaciones específicas:

- El uso de los datos se debe limitar a proporcionar o mejorar el caso de uso apropiado o las funciones visibles en la interfaz de usuario de la aplicación.
- Los datos de los usuarios se pueden transferir a terceros únicamente con el consentimiento explícito de los usuarios: con fines de seguridad (por ejemplo, para investigar un abuso), para satisfacer las leyes o reglamentaciones aplicables, o como parte de fusiones o adquisiciones.
- A menos que se haya obtenido el consentimiento explícito de los usuarios, el acceso de personas físicas a datos de los usuarios solo se permitirá para fines de seguridad, para satisfacer las leyes o cuando se agregan datos para operaciones internas de acuerdo con los requisitos legales.
- **Está prohibido cualquier otro uso, transferencia o venta de datos de Health Connect, lo que incluye lo siguiente:**
  - Transferir o vender datos del usuario a terceros como plataformas publicitarias, agentes de datos o cualquier revendedor de información
  - Transferir, vender o usar datos de los usuarios para publicar anuncios, lo que incluye publicidad personalizada o basada en intereses
  - Transferir, vender o usar datos de los usuarios para determinar la solvencia crediticia o con fines de préstamos
  - Transferir, vender o usar datos de los usuarios con cualquier producto o servicio que podría considerarse como un dispositivo médico, a menos que la aplicación de dispositivo médico satisfaga todas las reglamentaciones aplicables, lo que incluye haber obtenido las aprobaciones o los permisos necesarios de los órganos reguladores pertinentes (p. ej., la FDA de EE.UU.) para el uso previsto de los datos de Health Connect, y que el usuario haya otorgado su consentimiento explícito para tal uso

- Transferir, vender o usar datos de los usuarios para cualquier fin o de cualquier manera que involucre Información de Salud Protegida (según se define en la HIPAA), a menos que el usuario inicie tales operaciones y estas satisfagan las reglamentaciones de la HIPAA

Alcance Mínimo

Solo debe solicitar acceso a los permisos que son necesarios para implementar los servicios o las funciones de sus productos. Dichas solicitudes de acceso deben ser específicas para los datos que son necesarios y limitarse a ellos.

Control y Aviso Precisos y Transparentes

Health Connect maneja datos de salud y fitness, que incluyen información personal y sensible. Los desarrolladores deben divulgar información clara y accesible sobre sus prácticas de datos a través de una política de privacidad integral. En ella deben incluir lo siguiente:

- Una representación precisa de la identidad de la aplicación o el servicio que solicita acceso a los datos del usuario
- Información clara y precisa que explique los tipos de datos a los que se accede y que se solicitan o recopilan, los cuales deben estar relacionados con una función para el usuario o una recomendación ofrecida en la app en cuestión
- Una explicación sobre cómo se usarán o compartirán los datos: si solicita datos por un motivo, pero estos también se usarán para un propósito secundario, debe divulgar todos los casos de uso a los usuarios
- Documentación de ayuda para los usuarios que indique cómo pueden administrar sus datos y borrarlos de la aplicación, y qué ocurre con los datos cuando se desactiva o borra una cuenta
- Información sobre sus prácticas de manejo seguro de los datos sensibles y personales de los usuarios, lo que incluye transmitirlos con criptografía moderna (por ejemplo, a través de HTTPS)

Si desea obtener más información sobre los requisitos para las aplicaciones que se conectan a Health Connect, consulte este artículo del Centro de ayuda.

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)

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 .

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 .

Permiso de Intent de Pantalla Completa

En el caso de las aplicaciones que se orientan a Android 14 (nivel de API 34) y versiones superiores, `USE_FULL_SCREEN_INTENT` es un permiso especial de acceso para aplicaciones . Solo se permitirá automáticamente que las aplicaciones usen el permiso `USE_FULL_SCREEN_INTENT` si su funcionalidad principal está dentro de una de las siguientes categorías que requieren enviar notificaciones de alta prioridad:

- establecer una alarma
- recibir llamadas telefónicas o videollamadas

Las aplicaciones que soliciten este permiso están sujetas a revisión, y a las que no cumplan con los criterios indicados arriba no se les otorgará automáticamente este permiso. En esos casos, las aplicaciones deberán pedirle permiso al usuario para usar `USE_FULL_SCREEN_INTENT`.

No olvide que todo uso del permiso `USE_FULL_SCREEN_INTENT` debe satisfacer las Políticas para Desarrolladores de Google Play, incluidas las políticas de Software No Deseado para Dispositivos Móviles, Abuso de Dispositivos y Redes, y Anuncios. No se permite que las notificaciones de intents de pantalla completa interfieran con los dispositivos de los usuarios de maneras no autorizadas ni que los afecten negativamente o accedan a ellos. Las aplicaciones tampoco deben interferir con otras aplicaciones ni con la usabilidad del dispositivo.

Obtenga más información sobre el permiso `USE_FULL_SCREEN_INTENT` en nuestro Centro de ayuda.

API de Age Signals y datos del usuario

En esta política, se definen las condiciones para el uso de la API de Age Signals , que proporciona acceso a datos personales y sensibles sobre la edad del usuario y el consentimiento parental.

Solo puedes usar los datos a los que accedes a través de la API de Age Signals con el único propósito de cumplir con las obligaciones legales y reglamentarias aplicables, como proporcionar experiencias adecuadas para la edad en tu app.

Está estrictamente prohibido usar estos datos para los siguientes fines, incluidos, sin limitaciones, los que se enumeran a continuación:

- Fines publicitarios, de marketing o de personalización, incluida la publicación de anuncios segmentados
- Inteligencia empresarial, análisis de datos o creación de perfiles de usuarios
- Vender, compartir o transferir los datos a terceros por cualquier motivo, excepto cuando la ley lo exija estrictamente

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.

Los siguientes son ejemplos de incumplimientos comunes:

Ejemplos de incumplimientos comunes de la política de Abuso de Redes y Dispositivos:

- Aplicaciones que bloquean la exhibición de anuncios de otra aplicación o interfieren con ella
- Aplicaciones para hacer trampa en juegos que afectan la experiencia de juego en otras aplicaciones
- Aplicaciones que facilitan o proporcionan instrucciones para hackear servicios, software o hardware, o para evadir protecciones de seguridad
- Aplicaciones que acceden o usan un servicio o una API de forma tal que infrinjan las condiciones del servicio
- Aplicaciones que no son aptas para incluirse en la lista de entidades permitidas y que intentan omitir la administración de energía del sistema
- Aplicaciones que facilitan servicios de proxy a terceros (solo deben hacerlo aquellas con esa finalidad principal para el usuario)

- Aplicaciones o código de terceros (por ejemplo, SDKs) que descargan código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play
- Aplicaciones 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 (por ejemplo, SDKs) que contengan WebViews con la interfaz de JavaScript y carguen contenido web que no sea de confianza (por ejemplo, URLs http://) o URLs sin verificar provenientes de fuentes no confiables (por ejemplo, URLs obtenidas con intents que no sean de confianza)
- Aplicaciones que usan el permiso de intent de pantalla completa para forzar la interacción de los usuarios con notificaciones o anuncios invasivos
- Aplicaciones que eluden las protecciones de la zona de pruebas de Android para derivar la actividad o la identidad de los usuarios de otras aplicaciones

Uso del Servicio en Primer Plano

El permiso Servicio en Primer Plano garantiza el uso adecuado de los servicios en primer plano para el usuario. En el caso de las aplicaciones que se orientan a Android 14 y versiones posteriores, debe especificar un tipo de servicio en primer plano para cada uno de estos servicios que se use en su aplicación y declarar el permiso de servicio en primer plano que sea adecuado para ese tipo. Por ejemplo, si el caso de uso de su aplicación requiere ubicación geográfica con un mapa, debe declarar el permiso FOREGROUND_SERVICE_LOCATION en el manifiesto de su aplicación.

Solo se permite que las aplicaciones declaren un permiso de servicio en primer plano si su uso cumple con las siguientes condiciones:

- Proporciona una función que es beneficiosa para el usuario y pertinente para la funcionalidad principal de la aplicación.
- El servicio es perceptible para el usuario o él es quien lo inicia (por ejemplo, el audio de la reproducción de una canción, la transmisión de contenido multimedia a otro dispositivo, una notificación clara y precisa para el usuario, la solicitud de un usuario para subir una foto a la nube).
- El usuario puede cancelar el servicio o detenerlo.
- El sistema no puede interrumpirlo ni aplazarlo sin provocar una experiencia del usuario negativa o que la función esperada por el usuario no funcione según lo previsto (por ejemplo, las llamadas telefónicas se deben comenzar de inmediato y el sistema no puede aplazarlas).
- El servicio se ejecuta solo durante el tiempo necesario para completar la tarea.

Los siguientes casos de uso de servicios en primer plano están exentos de los criterios que se mencionan más arriba:

- tipos de servicios en primer plano systemExempted o shortService
- tipo de servicio en primer plano dataSync solo cuando se usan funciones de Play Asset Delivery

El uso del servicio en primer plano se explica con más detalle aquí.

Tareas de Transferencia de Datos Iniciadas por el Usuario

Solo se permite que las aplicaciones usen la API de user-initiated data transfer jobs si el uso cumple con las siguientes condiciones:

- El usuario es quien lo inicia.
- Está destinado a tareas de transferencia de datos de red.
- Dura el tiempo necesario para completar la transferencia de datos.

El uso de las APIs de User-Initiated Data Transfer se explica con más detalle aquí.

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.

Aplicaciones que Ejecutan Contenedores de Android en el Dispositivo

Las aplicaciones de contenedor de Android integrado en los dispositivos proporcionan entornos que estimulan la totalidad o partes de un SO Android subyacente. Es posible que la experiencia en estos entornos no refleje el kit completo de funciones de seguridad de Android , por lo que los desarrolladores pueden elegir agregar un parámetro de manifiesto de entorno seguro para comunicarles a los contenedores de Android integrados en los dispositivos que no deben operar en su entorno de Android simulado.

Parámetro de Manifiesto de Entorno Seguro

REQUIRE_SECURE_ENV es un parámetro que se puede declarar en el manifiesto de una aplicación para indicar que esta no debe ejecutarse en aplicaciones de contenedor de Android integrado en los dispositivos. Por fines de seguridad y privacidad, las aplicaciones que proporcionan contenedores de Android integrados en los dispositivos deben respetar todas las aplicaciones que declaren este parámetro y cumplir con lo siguiente:

- Deben comprobar si los manifiestos de las aplicaciones que pretendan cargar en su contenedor de Android en el dispositivo contienen este parámetro.
- No deben cargar las aplicaciones que declararon este parámetro en su contenedor de Android en el dispositivo.
- No deben funcionar como proxy interceptando o llamando a APIs en el dispositivo para que parezca que están instaladas en el contenedor.
- No deben facilitar ni crear soluciones alternativas para evitar el parámetro (como cargar una versión antigua de la aplicación para omitir el parámetro REQUIRE_SECURE_ENV de la aplicación actual).

Obtenga más información sobre esta política en nuestro Centro de ayuda.

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.

Los siguientes son ejemplos de incumplimientos comunes:

- Aplicaciones que tergiversen o no describan de forma precisa y clara su funcionalidad:
  - Una aplicación que afirme ser un juego de carreras en la descripción y en las capturas de pantalla, pero que en realidad sea un juego de habilidad mental con bloques 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, etcétera
- 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 o que esté relacionado con los resultados electorales
- Aplicaciones que afirmen falsamente mantener algún vínculo con una entidad gubernamental o proporcionar o facilitar servicios gubernamentales para los cuales no estén debidamente autorizadas
- Aplicaciones que afirmen 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) Aplicaciones que afirmen 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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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 permitimos aplicaciones que promuevan o ayuden a crear información o afirmaciones falsas o engañosas recurriendo a imágenes, audio, videos o texto para ese fin. No permitimos aplicaciones

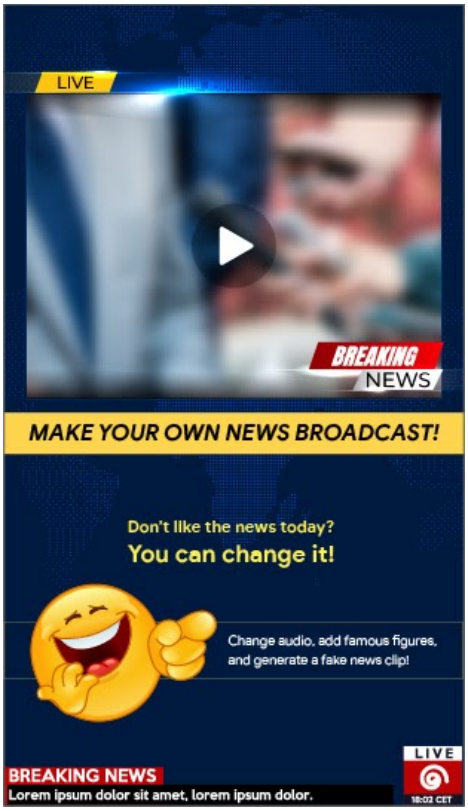
diseñadas para promover o perpetuar imágenes, videos o textos comprobablemente engañosos, que puedan provocar daños con relación a sucesos delicados, política, problemas sociales u otros asuntos de interés público.

Se pueden contemplar excepciones para asuntos de interés público, imágenes claramente artificiales, contenido multimedia manipulado con renuncias de responsabilidad para el usuario o marcas de agua, o sátiras o parodias evidentes.

El contenido multimedia manipulado debe satisfacer las Políticas para Desarrolladores de Google Play existentes, lo que incluye prohibir el contenido no permitido en virtud de las políticas de contenido restringido.

Los siguientes son ejemplos de incumplimientos comunes:

- Aplicaciones que usen figuras públicas o contenido multimedia a partir de un suceso delicado para publicitar sus capacidades de alteración del contenido multimedia dentro de la ficha de Play Store de una aplicación
- Aplicaciones que modifiquen clips con contenido multimedia para imitar un programa de noticias incluyendo nombres o logotipos de medios de comunicación reales sin renuncias de responsabilidad ni marcas de agua claras
- Aplicaciones que tengan como único fin crear contenido multimedia engañoso



(1) Esta aplicación 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.

Comportamiento Transparente

La funcionalidad de su aplicación debe estar razonablemente clara para los usuarios. La aplicación no debe incluir funciones ocultas, latentes ni no documentadas. No se permite implementar técnicas para evadir las revisiones de aplicaciones. Se puede exigir que las aplicaciones proporcionen detalles adicionales para garantizar la seguridad de los usuarios, la integridad del sistema y el cumplimiento de las políticas.

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

---

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.

Si necesita asesoramiento técnico para satisfacer el requisito de nivel de API objetivo, consulte la guía de migración .

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

Política de Datos del Usuario

Debe ser transparente en la manera en que maneja los datos de los usuarios (por ejemplo, información recopilada sobre un usuario o de parte de este, incluida la información del dispositivo). Es decir, debe divulgar si su aplicación accede a los datos, así como cuándo los recopila, usa, maneja y comparte, además de limitar su uso a los fines divulgados que satisfagan las políticas.

Si incluye código de terceros (por ejemplo, un SDK) en su aplicación, debe garantizar que tanto ese código como las prácticas de los terceros en cuestiones relacionadas con los datos de los usuarios de su aplicación satisfagan las Políticas del Programa para Desarrolladores de Google Play, que incluyen requisitos de uso y divulgación. Por ejemplo, debe garantizar que sus proveedores de SDKs no vendan los datos sensibles y personales de los usuarios recopilados en su aplicación. Este requisito se aplica independientemente de si los datos de los usuarios se transfieren después de enviarse a un servidor o mediante la incorporación de código de terceros en su aplicación.

Datos Sensibles y Personales del Usuario

- Limite el acceso, la recopilación, la utilización y el uso compartido de los datos de usuario sensibles y personales que se adquieran desde la aplicación a los fines de la funcionalidad del servicio y de la aplicación, así como del cumplimiento de las políticas según las expectativas razonables de los usuarios:
  - Las aplicaciones que extiendan el uso de datos sensibles y personales de los usuarios a la publicación de anuncios deben satisfacer la política de Anuncios de Google Play.
- Maneje todos los datos sensibles y personales 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 restringidos por los permisos de Android.

Venta de Datos Sensibles y Personales del Usuario

No venda datos sensibles ni personales de los usuarios.

- "Venta" significa el intercambio o la transferencia de datos sensibles y personales de los usuarios a un tercero a cambio de una contraprestación económica.
  - La transferencia de datos sensibles y personales de los usuarios iniciadas por estos (por ejemplo, cuando el usuario usa una función de la aplicación para transferir un archivo a un tercero o casos en los que elige usar una aplicación de estudio de investigación de propósito exclusivo) no se consideran ventas.

Requisitos de Divulgación Destacada y Consentimiento

En los casos en donde el acceso, la recopilación, la utilización o el uso compartido de los datos sensibles y personales de los usuarios del producto o la función en cuestión puedan no caber dentro de las expectativas razonables de esas personas, deberá cumplir con los requisitos de divulgación destacada y consentimiento de la política de Datos del Usuario.

Si su aplicación integra código de terceros (por ejemplo, un SDK) diseñado para recopilar datos sensibles y personales de los usuarios de forma predeterminada, deberá, en un plazo de 2 semanas a partir de recibir la solicitud de Google Play (o bien, si la solicitud de Google Play permite más tiempo, dentro del período correspondiente), proporcionar evidencia suficiente que demuestre que su aplicación cumple con los requisitos de Divulgación Destacada y Consentimiento de esta política, incluso en relación con el acceso, la recopilación, la utilización y el uso compartido de los datos mediante código de terceros.

Recuerde asegurarse de que el uso que haga del código de terceros (por ejemplo, un SDK) no provoque que su aplicación infrinja la política de Datos del Usuario.

Consulte este artículo del Centro de Ayuda para obtener más información sobre el requisito de Divulgación Destacada y Consentimiento.

Ejemplos de infracciones provocadas por SDKs

- Una aplicación con un SDK que recopila datos sensibles y personales de los usuarios, y no trata esta información como sujeta a la política de Datos del Usuario en cuestión y a los requisitos de divulgación destacada y consentimiento, acceso y manejo de datos (incluida la venta no permitida)
- Una aplicación que integra un SDK que recopila datos sensibles y personales de los usuarios de forma predeterminada sin cumplir con los requisitos de esta política relacionados con la divulgación destacada y el consentimiento del usuario
- Una aplicación con un SDK que declara recopilar datos sensibles y personales de los usuarios solo para proporcionar una funcionalidad antifraude y antiabuso de la aplicación, pero en realidad el SDK también comparte los datos que recopila con terceros para fines de estadísticas o publicidad
- Una aplicación que incluye un SDK que transmite información de los paquetes instalados de los usuarios sin cumplir los lineamientos sobre divulgación destacada ni los de la política de privacidad
  - Consulte también la política de Software No Deseado para Dispositivos Móviles

Requisitos Adicionales para el Acceso a los Datos Sensibles y Personales

La tabla que se incluye a continuación describe los requisitos para determinadas actividades.

Actividad	Requisito
Su aplicación recopila o vincula identificadores de dispositivos persistentes (por ejemplo, IMEI, IMSI, número de serie de SIM, etcétera)	Los identificadores de dispositivos persistentes no pueden vincularse a otros datos personales y sensibles de los usuarios, ni a identificadores de dispositivos que se pueden restablecer, excepto para los siguientes fines: • Telefonía vinculada a una identidad de SIM (por ejemplo, llamadas por Wi-Fi vinculadas a la cuenta de un 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.
Su aplicación se orienta a niños.	Su aplicación solo puede incluir SDKs que tengan autocertificación para usarse en servicios dirigidos a niños. Consulte el Programa del SDK de Anuncios con Autocertificación para Familias para conocer los requisitos y el texto completo de la política.

Ejemplos de infracciones provocadas por SDKs

- Una aplicación que usa un SDK que vincula el número de IMEI y la ubicación
- Una aplicación con un SDK que conecta el ID de Publicidad de Android (AAID) a identificadores de dispositivos persistentes para cualquier fin publicitario o estadístico
  Una aplicación que usa un SDK que conecta el AAID y la dirección de correo electrónico para fines estadísticos

Sección de Seguridad de los datos

Para cada aplicación, los desarrolladores deben completar una sección clara y precisa de Seguridad de los datos en la que se detalle la utilización, la recopilación y el uso compartido de datos de los usuarios. Esto incluye los datos recopilados y manejados mediante bibliotecas o SDKs de terceros que se usen en sus aplicaciones. 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 del Centro de Ayuda para obtener información adicional sobre cómo completar la sección de Seguridad de los datos.

Consulte la política de Datos del Usuario en su totalidad.

Política sobre Permisos y APIs que Acceden a Información Sensible

Las solicitudes de permisos y el uso de APIs que accedan a información sensible deben tener un sentido claro para los usuarios. Solo puedes solicitar permisos y usar APIs que accedan a información sensible cuando estos sean necesarios para implementar funciones o servicios existentes en tu aplicación que se promuevan en la ficha de Google Play. Se prohíbe el uso de permisos o APIs que accedan a información sensible que otorgue acceso a los datos del usuario o del dispositivo para funciones o fines no divulgados, no implementados o no autorizados. No se permite vender los datos sensibles o personales que se obtengan mediante permisos o APIs que accedan a información sensible, ni compartirlos para facilitar una venta.

Consulte la política de Permisos y APIs que Acceden a Información Sensible en su totalidad.

Ejemplos de infracciones provocadas por SDKs

- Su aplicación incluye un SDK que solicita la ubicación en segundo plano para un fin no permitido o no divulgado.
- Su aplicación incluye un SDK que transmite el IMEI derivado del permiso de Android read_phone_state sin el consentimiento del usuario.

Política de 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. Se incluyen, entre otros, Aplicaciones Potencialmente Dañinas (APD), objetos binarios o

modificaciones de framework, que a su vez se organizan en categorías como troyanos, suplantación de identidad (phishing) y aplicaciones de software espía. (Actualizamos esta lista de manera continua con nuevas categorías).

Los requisitos de esta política también se aplican al código de terceros (por ejemplo, un SDK) que usted incluya en su aplicación.

Consulte la política de Software Malicioso en su totalidad.

Ejemplos de infracciones provocadas por SDKs

- Aplicaciones que incluyen bibliotecas de SDKs de proveedores que distribuyen software malicioso
- Aplicaciones que no cumplen con el modelo de permisos de Android o que roban credenciales (p. ej., tokens de OAuth) de otras aplicaciones
- Apps que abusan de las funciones para evitar que las desinstalen o las detengan
- Aplicaciones que inhabilitan SELinux
- Aplicaciones que incluyen un SDK que infringe el modelo de permisos de Android debido a que gana privilegios elevados mediante el acceso de los datos del dispositivo para un fin no divulgado
- Aplicaciones que incluyen un SDK con código que engaña a los usuarios para que se suscriban a contenido o lo compren a través de la facturación del operador de telefonía celular

Uso de SDKs en Aplicaciones

Si incluye un SDK en su aplicación, es responsable de garantizar que las prácticas y el código de terceros no provoquen una infracción de las Políticas del Programa para Desarrolladores de Google Play. Es importante estar al tanto de cómo los SDKs de su aplicación manejan los datos de los usuarios, además de asegurarse de conocer qué permisos usan, qué datos recopilan y por qué.

Requisitos para los SDKs

Por lo general, los desarrolladores de aplicaciones usan código de terceros (por ejemplo, un SDK) para integrar la funcionalidad y los servicios clave en sus aplicaciones. Cuando incluya un SDK en su aplicación, debe asegurarse de poder mantener la seguridad de sus usuarios y aplicaciones en contra de cualquier tipo de vulnerabilidad. En esta sección, mostramos cómo algunos de nuestros requisitos de privacidad y seguridad se aplican en el contexto de los SDKs y están diseñados para ayudar a los desarrolladores a integrar de manera segura los SDKs en sus aplicaciones.

Si incluye un SDK en su aplicación, es responsable de garantizar que las prácticas y el código de terceros no provoquen una infracción de las Políticas del Programa para Desarrolladores de Google Play. Es importante estar al tanto de cómo los SDKs de su aplicación manejan los datos de los usuarios, además de asegurarse de conocer qué permisos usan, qué datos recopilan y por qué. Recuerde que la forma de recopilar y manejar los datos de los usuarios de un SDK debe alinearse con el cumplimiento de su aplicación con las políticas relacionadas al uso de esos datos.

Para asegurarse de que su uso del SDK no infrinja los requisitos de las políticas, lea y comprenda las siguientes políticas en su totalidad. A continuación, se incluyen algunos de los requisitos existentes relacionados con los SDKs:

Las aplicaciones de elevación de privilegios que otorgan a los dispositivos permisos de administrador sin que el usuario conceda el permiso se clasifican como aplicaciones con permisos de administrador.

Software espía

El software espía es una aplicación, un código o un comportamiento malicioso que recopila, exfiltra o comparte los datos de un usuario o dispositivo de una manera no relacionada con la funcionalidad permitida por las políticas.

También puede considerarse que un código o comportamiento malicioso constituye software espía si se puede interpretar que dicho código o comportamiento espía al usuario o exfiltra datos sin la notificación o el consentimiento correspondientes.

Consulte la política completa de Software Espía.

Algunos ejemplos de incumplimientos de software espía causados por SDKs incluyen, sin limitaciones, los siguientes:

- Aplicaciones que usan un SDK que transmite datos de grabaciones de audio o llamadas cuando estos no se relacionan con las funciones de la aplicación que satisfacen las políticas
- Aplicaciones con código externo malicioso (por ejemplo, un SDK) que transmite datos hacia fuera del dispositivo de una manera que el usuario no espera o sin una notificación o el consentimiento correspondientes del usuario

Política de Software No Deseado para Dispositivos Móviles

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.

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 sensibles y personales del usuario. Los usos de los datos del usuario deben cumplir con todas las Políticas de Datos del Usuario pertinentes, cuando corresponda, y se deben tomar todas las precauciones necesarias para protegerlos.

Ejemplos de incumplimiento:

- Recopilación de Datos (consulta software espía)
- Abuso de Permisos Restringidos

Consulte la política de Software No Deseado para Dispositivos Móviles en su totalidad.

Política de Abuso de Redes y Dispositivos

No permitimos 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 (APIs) o servicios (incluidos, sin limitaciones, a otras aplicaciones del dispositivo, cualquier servicio de Google o red de proveedor autorizada).

Las aplicaciones o códigos de terceros (p. ej., SDKs) 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 Aplicaciones a fin de obtener información sobre los problemas de seguridad más recientes que se marcaron para los desarrolladores.

Consulte la política de Abuso de Redes y Dispositivos en su totalidad.

Ejemplos de infracciones provocadas por SDKs

- Aplicaciones que facilitan servicios de proxy a terceros (solo deben hacerlo aquellas con esa finalidad principal para el usuario)

- Aplicaciones que incluyen un SDK que descarga código ejecutable, como archivos dex o código nativo, de una fuente que no sea Google Play
- Aplicaciones con un SDK que contiene WebViews con la interfaz de JavaScript y carga contenido web que no es de confianza (por ejemplo, URLs http://) o URLs sin verificar provenientes de fuentes no confiables (por ejemplo, URLs obtenidas con intents que no son de confianza)
- Aplicaciones que incluyen un SDK que contiene código usado para actualizar su propio APK
- Aplicaciones que incluyen un SDK que expone a los usuarios a una vulnerabilidad de seguridad por descargar archivos a través de una conexión no segura
- Aplicaciones con un SDK que usa código para descargar o instalar aplicaciones de fuentes desconocidas por fuera de Google Play
- Aplicaciones que incluyen un SDK que usa servicios en primer plano sin un caso de uso adecuado
- Aplicaciones que incluyen un SDK que usa servicios en primer plano por un motivo que satisface las políticas, pero que no está declarado en el manifiesto de la aplicación

Política de 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 cambio en la configuración del dispositivo debe realizarse con el conocimiento y el consentimiento del usuario, y este debe poder revertirlo.

Consulte la política completa de Comportamiento Engañoso.

Comportamiento Transparente

La funcionalidad de su aplicación debe estar razonablemente clara para los usuarios. La aplicación no debe incluir funciones ocultas, latentes ni no documentadas. No se permite implementar técnicas para evadir las revisiones de aplicaciones. Se puede exigir que las aplicaciones proporcionen detalles adicionales para garantizar la seguridad de los usuarios, la integridad del sistema y el cumplimiento de las políticas.

Ejemplo de un incumplimiento provocado por el SDK

- Su aplicación incluye un SDK que usa técnicas para evadir revisiones de aplicaciones.

¿Qué Políticas para Desarrolladores de Google Play se asocian por lo general con las infracciones provocadas por SDKs?

Para ayudarlo a asegurarse de que el código de terceros que usa su aplicación satisfaga las Políticas del Programa para Desarrolladores de Google Play, consulte las siguientes políticas en su totalidad:

- Política de Datos del Usuario
- Permisos y APIs que Acceden a Información Sensible
- Política de Abuso de Redes y Dispositivos
- Software Malicioso
- Software No Deseado para Dispositivos Móviles
- Programa del SDK de Anuncios con Autocertificación para Familias
- Política de Anuncios
- Comportamiento engañoso
- Políticas del Programa para Desarrolladores de Google Play

Aunque estas políticas son las más comunes, es importante que recuerde que un código de SDK erróneo puede provocar que su aplicación infrinja alguna otra política a la que no se haya hecho referencia aquí. Recuerde revisar y estar al tanto de todas las políticas en su totalidad, ya que es su

responsabilidad como desarrollador de aplicaciones asegurarse de que los SKDs manejen sus datos de aplicaciones de una manera que satisfaga las políticas.

Para obtener más información, visite nuestro 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. Se incluyen, entre otros, Aplicaciones Potencialmente Dañinas (APD), objetos binarios o modificaciones de framework, que a su vez se organizan en categorías como troyanos, suplantación de identidad (phishing) y aplicaciones de software espía. (Actualizamos esta lista de manera continua con nuevas categorías).

Los requisitos de esta política también se aplican al código de terceros (por ejemplo, un SDK) que usted incluya en su aplicación.

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 de SMS, fraude telefónico y fraude de cargos telefónicos.

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

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

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

Fraude de cargos telefónicos
Se trata de código que engaña al usuario para que se suscriba a contenido o lo compre a través de la facturación del operador de telefonía celular.

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

Stalkerware

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.

Para obtener más información, consulte el artículo del Centro de ayuda Uso del parámetro IsMonitoringTool .

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

El software espía es una aplicación, un código o un comportamiento malicioso que recopila, exfiltra o comparte los datos de un usuario o dispositivo de una manera no relacionada con la funcionalidad permitida por las políticas.

También puede considerarse que un código o comportamiento malicioso constituye software espía si se puede interpretar que dicho código o comportamiento espía al usuario o exfiltra datos sin la

notificación o consentimiento correspondientes.

Por ejemplo, los incumplimientos relacionados con el software espía pueden incluir, entre otros:

- Grabaciones de audio o de llamadas realizadas al teléfono
- Robo de datos de las aplicaciones
- Una aplicación con código malicioso de terceros (por ejemplo, un SDK) que transmita datos hacia fuera del dispositivo de una manera que el usuario no espera o sin una notificación o el consentimiento correspondientes del usuario.

Todas las aplicaciones deben satisfacer también todas las Políticas del Programa para Desarrolladores de Google Play, incluidas las políticas de datos del usuario y del dispositivo, como las de Software no Deseado para Dispositivos Móviles, Datos del Usuario, Permisos y APIs que Acceden a Información Sensible y Requisitos de SDK.

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.

Riskware

Una aplicación que usa una variedad de técnicas de evasión para presentarle al usuario funciones falsas o diferentes a las esperadas. Estas aplicaciones se hacen pasar por legítimas o por juegos con aspecto inofensivo ante las tiendas de aplicaciones y los usuarios, y usan técnicas tales como la ofuscación, la carga de código dinámico o el encubrimiento para ocultar contenido potencialmente dañino.

El riskware es similar a otras categorías de APD, en especial los troyanos, y su principal diferencia son las técnicas que se usan para ofuscar la actividad maliciosa.

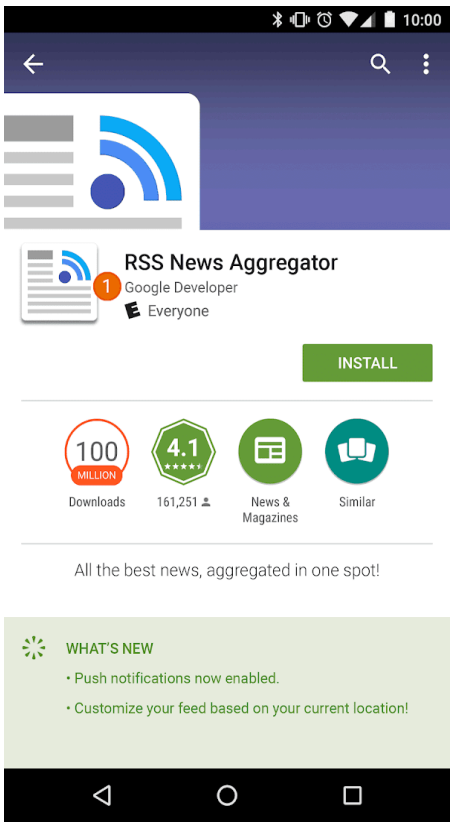
Suplantación de Identidad

No permitimos apps que confundan a los usuarios mediante la suplantación de 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.

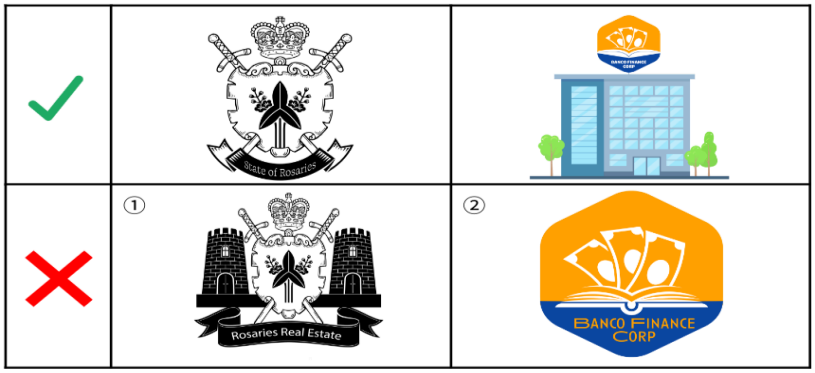
Los siguientes son ejemplos de incumplimientos comunes:

- 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 comercial 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 la Marca de Android

Si quiere conocer preguntas frecuentes sobre la política de Suplantación de Identidad, consulte este artículo del Centro de ayuda.

Software no Deseado para Dispositivos Móviles

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

Cómo proteger la privacidad y los datos del usuario

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

Todas las aplicaciones deben satisfacer todas las Políticas del Programa para Desarrolladores de Google Play, incluidas las políticas de datos del usuario y del dispositivo, por ejemplo, las de Datos del Usuario, Permisos y APIs que Acceden a Información Sensible, Software Espía y Requisitos para los SDKs.

- No solicite a los usuarios que desactiven las protecciones de seguridad del dispositivo, como Google Play Protect, ni los engañe para que lo hagan. Por ejemplo, no debe ofrecer a los usuarios funciones adicionales de la aplicación ni recompensas a cambio de que desactiven Google Play Protect.

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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

---

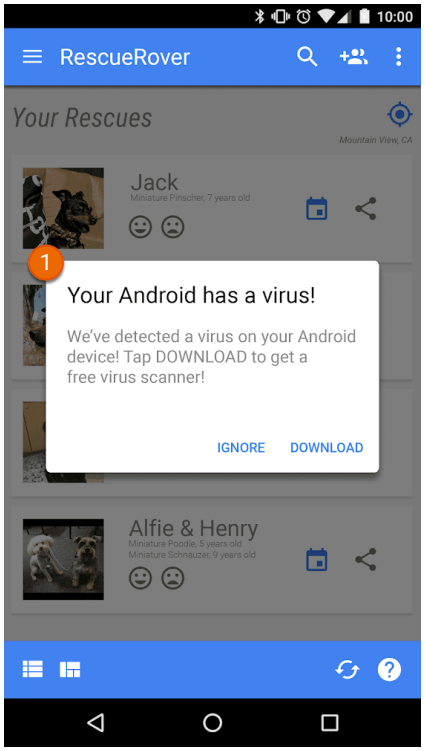
Uso no autorizado o imitación de las funciones del sistema

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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.

Ingeniería social

No se permiten aplicaciones que simulen ser otras con la intención de engañar a los usuarios para que lleven a cabo acciones que tenían pensado realizar en la aplicación de confianza original.

Monetización y anuncios

Google Play admite varias estrategias de monetización en beneficio de los desarrolladores y usuarios, como la distribución paga, los productos integrados en la 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, incluidas las funciones de la aplicación y el contenido o los bienes digitales (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, el Artículo 8 o el Artículo 9.

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

- artículos (como monedas virtuales, vidas adicionales, tiempo de juego adicional, elementos complementarios, personajes y avatares)
- servicios mediante suscripción (como los relacionados con entrenamiento físico, juegos, citas, educación, música, videos, actualizaciones de servicios y otros tipos de contenido)
- funciones 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. pagos que tienen 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 Aplicaciones 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 Pagos de Google

   Nota: En algunos mercados, ofrecemos Google Pay para las aplicaciones 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, el Artículo 8 y el Artículo 9, 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, 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 aplicación relacionadas con el contenido que se puede comprar
   - Vistas web, botones, vínculos, mensajes, anuncios y otros llamados a la acción en la aplicación
   - Flujos de la interfaz de usuario en la aplicación, incluidos los flujos de creación de cuentas o de registro, que dirigen a los usuarios de una aplicación 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 aplicación solo pueden usarse dentro del título (juego o aplicación) 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 aplicaciones, o sobre cualquier función o suscripción integrada que se pueda comprar. Los precios integrados en la aplicación 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 aplicación 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, incluidas, sin limitaciones, las "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 que requieran o acepten pagos de los usuarios ubicados en estos países o regiones para acceder a compras directas desde las aplicaciones pueden ofrecer a los usuarios un sistema alternativo de facturación en la aplicación, junto con el sistema de facturación de Google Play, para esas transacciones si los desarrolladores completan correctamente el formulario de declaración de facturación para cada programa respectivo y aceptan los requisitos del programa y las condiciones adicionales que allí se incluyen.

9. Los desarrolladores de aplicaciones distribuidas por Play pueden dirigir a los usuarios del Espacio Económico Europeo (EEE) fuera de la aplicación, por ejemplo, para promocionar ofertas de funciones y servicios digitales integrados en la aplicación. Los desarrolladores que dirijan a los usuarios del EEE fuera de la aplicación deben completar correctamente el formulario de declaración del programa y aceptar los requisitos del programa y las condiciones adicionales que allí se incluyen.

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

Anuncios

Con el fin de mantener una experiencia de calidad, tomamos en cuenta el público, la experiencia del usuario, el comportamiento y el contenido de sus anuncios, así como la seguridad y la privacidad. Consideramos los anuncios y las ofertas asociadas como parte de su aplicación; por lo tanto, también deben cumplir con todas las demás políticas de Google Play. También tenemos requisitos adicionales para los anuncios si monetiza una aplicación que se orienta a niños en Google Play.

También puede leer más información acerca de nuestras políticas sobre la Ficha de Play Store y Promociones de Aplicaciones aquí, incluida la forma en que abordamos las prácticas de promoción engañosa.

Contenido de los Anuncios

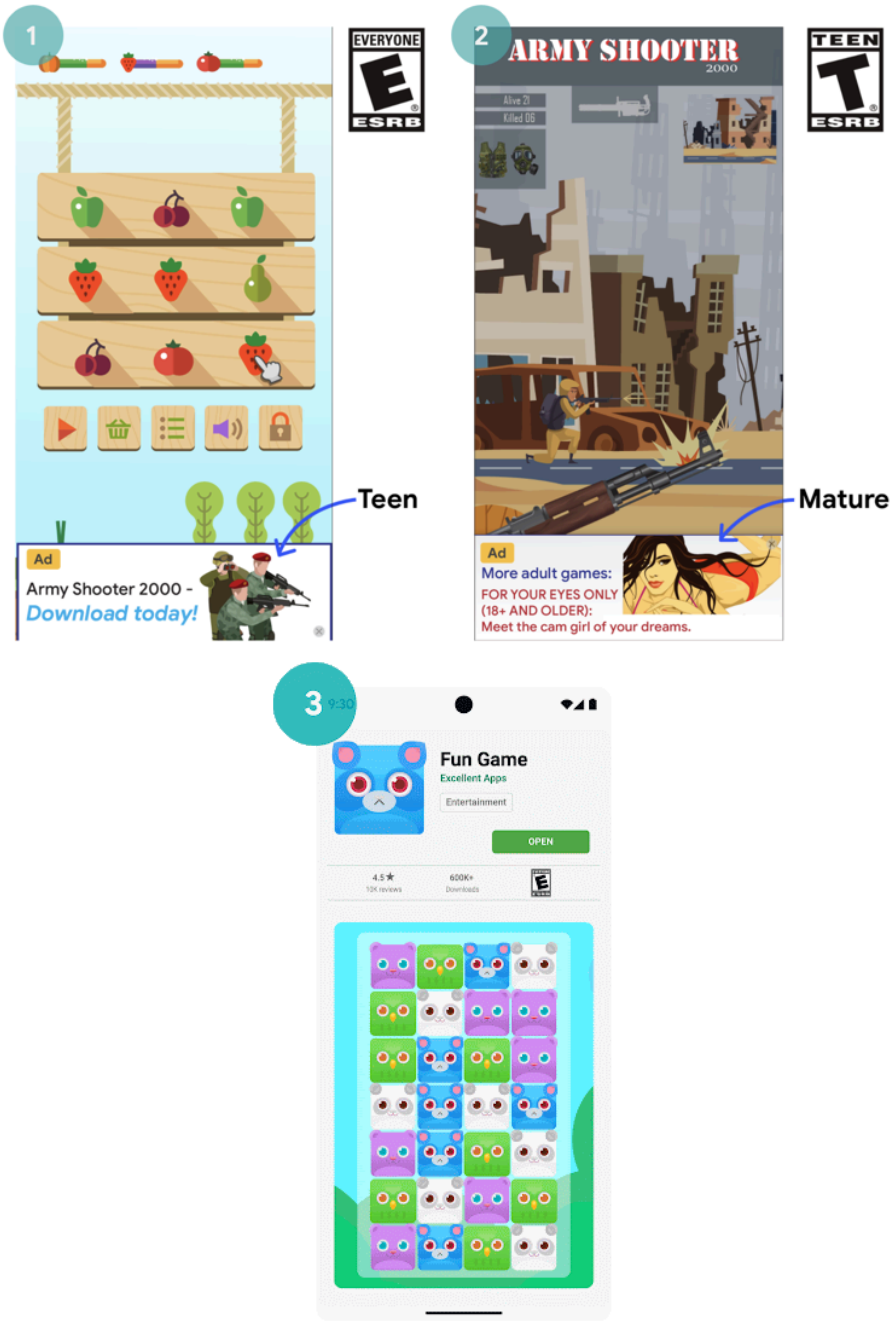
Los anuncios y las ofertas asociadas son parte de su aplicación, y deben cumplir con nuestras políticas de Contenido Restringido. Si su aplicación es de juegos de apuestas, se aplican requisitos adicionales.

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.

Los siguientes son ejemplos de incumplimientos comunes:

- Anuncios que son inadecuados para la clasificación del contenido de la aplicación



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)

Requisitos de los Anuncios para Familias

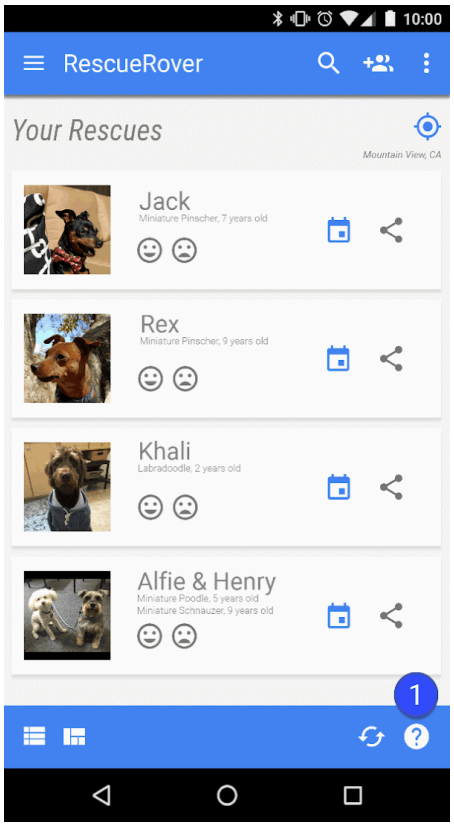
Si monetiza una aplicación que se orienta a niños en Google Play, es importante que esta cumpla con los Requisitos de la Política de Monetización y Anuncios para Familias.

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 con claridad a qué aplicación corresponde cada anuncio.

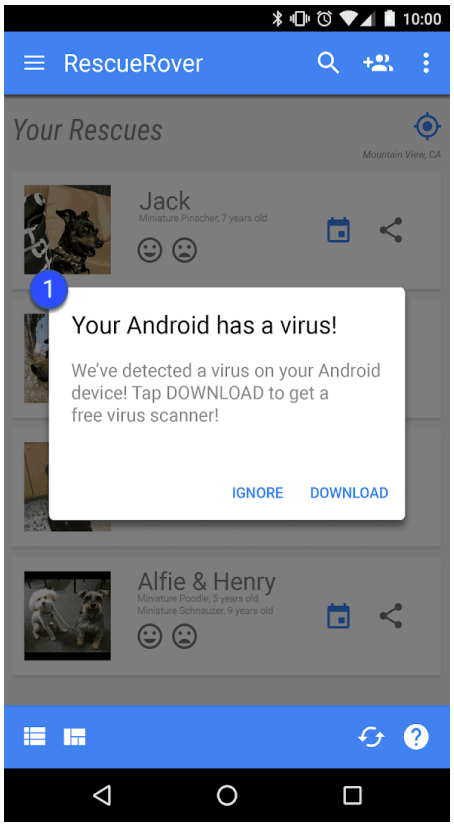
Los siguientes son ejemplos de incumplimientos comunes:

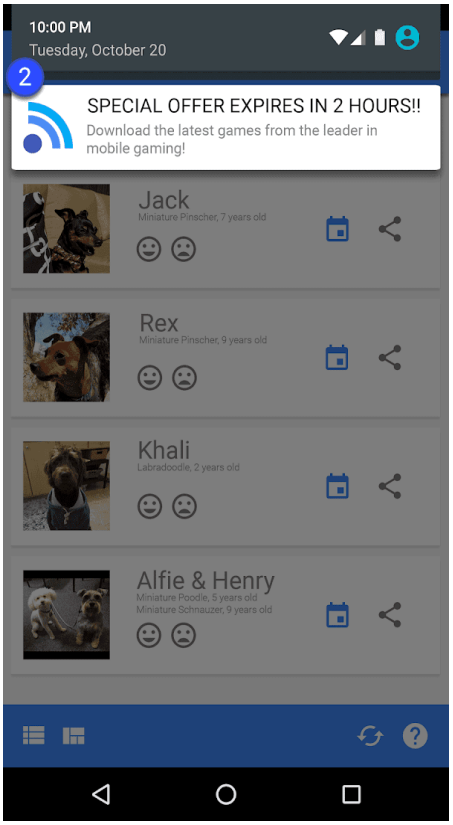
- Anuncios que imitan la IU de una aplicación:



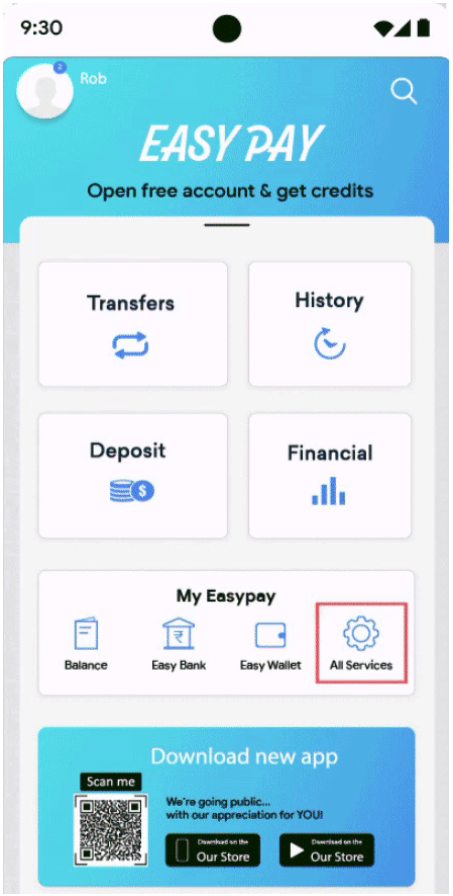
① El ícono de signo de interrogación en esta aplicación es un anuncio que lleva al usuario a una página de destino externa.

- Anuncios que imitan una notificación del sistema:





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



① El ejemplo anterior muestra la sección de una función que imita a otras funciones, pero que solamente dirige al usuario a uno o varios anuncios.

Anuncios Invasivos

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

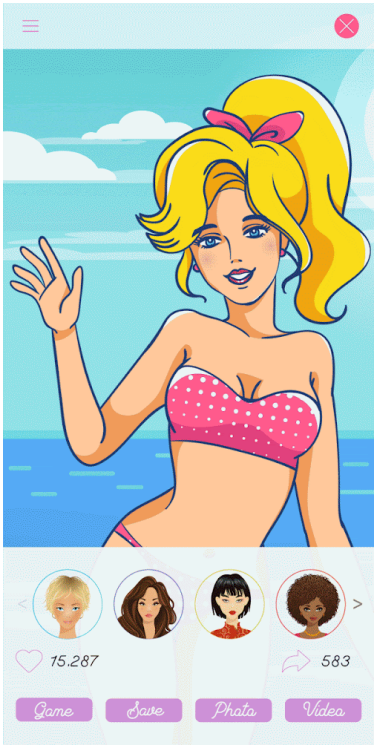
Su aplicación no puede obligar al usuario a hacer clic en un anuncio ni a enviar información personal con fines publicitarios antes de que pueda usar la aplicación por completo. Los anuncios solo se pueden mostrar dentro de la aplicación que los publica y no deben interferir con otras aplicaciones, anuncios o el funcionamiento del dispositivo, lo que incluye el sistema o los botones y puertos. Entre estos aspectos, se incluyen las superposiciones, las funciones complementarias y las unidades de anuncios con widgets. Si su aplicación muestra anuncios que interfieren con el uso normal, estos deben poder descartarse fácilmente sin penalización.

Los siguientes son ejemplos de incumplimientos comunes:

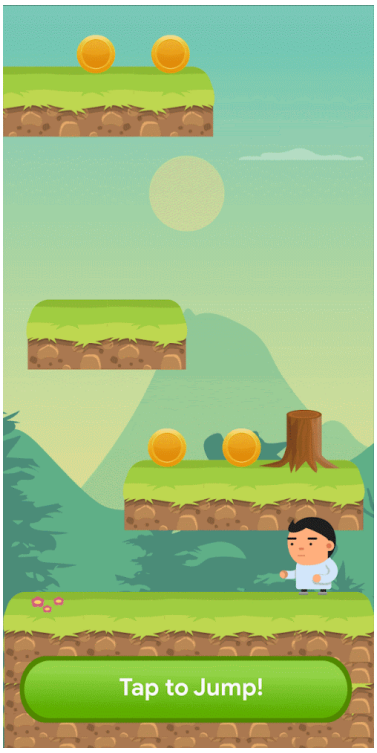
- Anuncios que ocupan toda la pantalla o interfieren con el uso normal, y que no ofrecen una manera clara de descartar el anuncio:

① Este anuncio no tiene un botón para descartar.

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

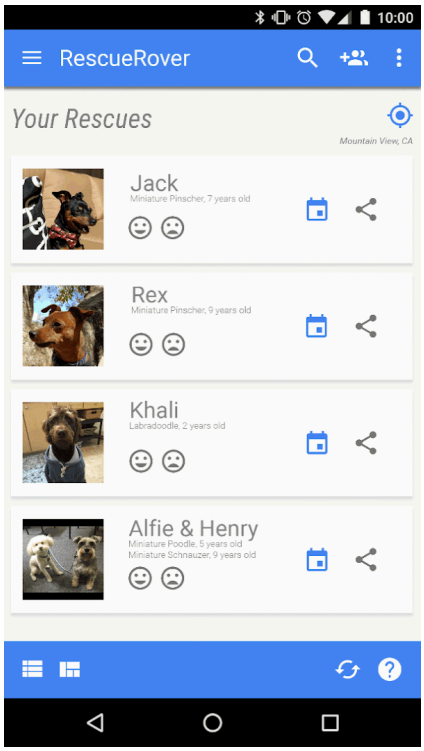


① Este anuncio usa un botón para descartar falso.



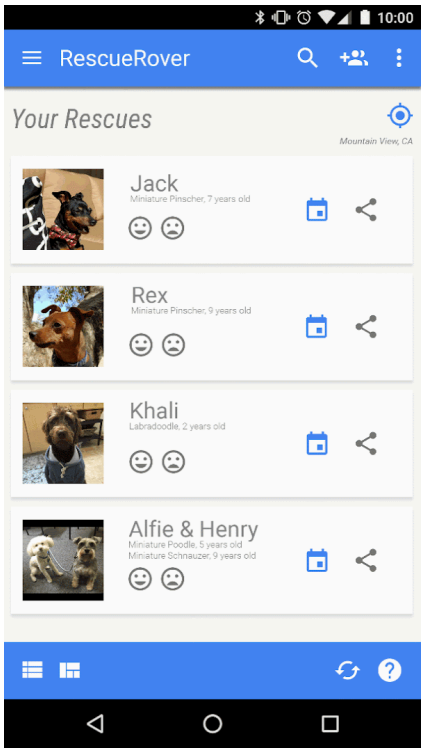
② Este anuncio aparece de repente en un área donde el usuario está acostumbrado a presionar para obtener funciones en la aplicación.

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



① El usuario navega a la pantalla principal desde esta aplicación, y aparece un anuncio en esa pantalla de manera repentina.

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



① El usuario intenta salir de la aplicación y navegar a la pantalla principal, pero un anuncio interrumpe el flujo esperado.

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.

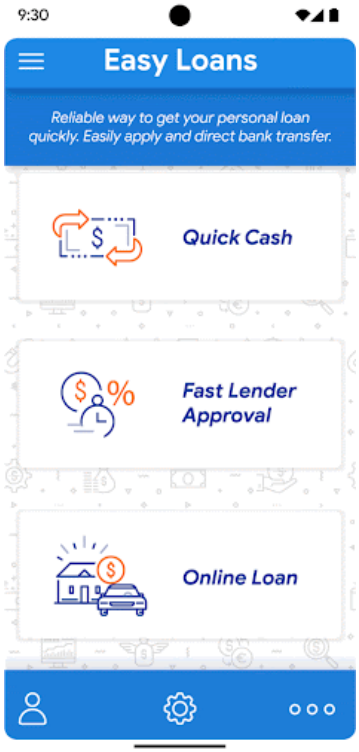
Esta política no se aplica a los anuncios recompensados que estén habilitados de forma explícita por los usuarios (por ejemplo, un anuncio que los desarrolladores ofrezcan mirar explícitamente a los usuarios a cambio de desbloquear una característica o contenido específico del juego). Esta política tampoco 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 .

Los siguientes son ejemplos de incumplimientos comunes:

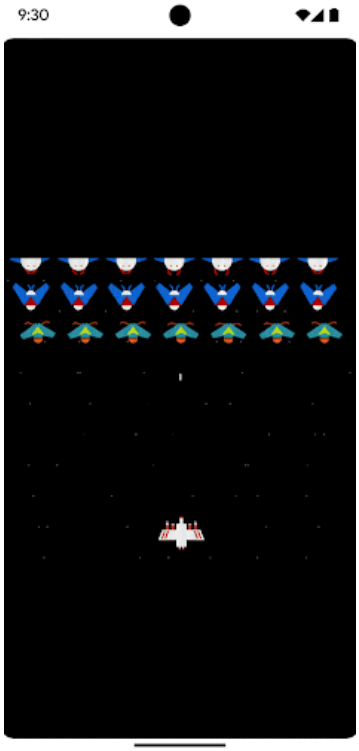
- Anuncios inesperados que aparecen durante el juego o al comienzo de un segmento de contenido (por ejemplo, después de que un usuario hizo clic y antes de que la acción prevista del clic en el botón haya surtido efecto); Estos anuncios son inesperados para los usuarios, ya que ellos esperan comenzar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



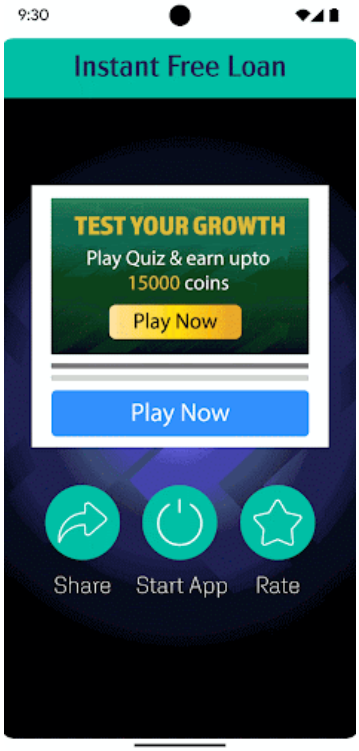
① Aparece un anuncio intersticial durante el juego, el cual no les ofrece a los usuarios la opción de omitirlo en el transcurso de 15 segundos.

Apps creadas para la publicación de anuncios

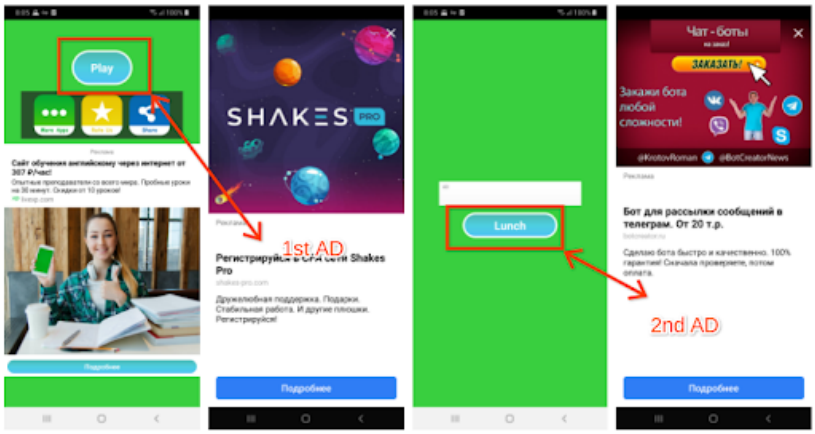
No permitimos aplicaciones que muestren anuncios intersticiales de forma reiterada para distraer a los usuarios y evitar que interactúen con una aplicación y realicen tareas en ella.

Los siguientes son ejemplos de incumplimientos comunes:

- 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



① 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.



② 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.

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.

Fraude Publicitario

Se prohíbe estrictamente el fraude publicitario. Para obtener más información, consulte nuestra política de Fraude Publicitario.

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.

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.

Para obtener más información, consulte nuestra política de Datos del Usuario.

Suscripciones

Como desarrollador, no debe generar confusión en los usuarios acerca de los servicios mediante suscripción o el contenido que ofrece en su aplicación. Es fundamental que se comunique con claridad en todas las promociones integradas en las aplicaciones, pantallas de presentación y pantallas de selección de planes de suscripción. No permitimos aplicaciones que lleven a los usuarios a tener experiencias de compra engañosas o manipuladoras (lo que incluye suscripciones o compras directas desde las aplicaciones). Si proporciona beneficios de suscripción, estos deben ser veraces y precisos, y no deben tergiversar ningún aspecto de la suscripción correspondiente.

Debe brindar una explicación transparente sobre la oferta. Esto incluye divulgar de forma clara y explícita las condiciones de su oferta, el costo de la suscripción, la frecuencia del ciclo de facturación, las condiciones de renovación automática, si se requiere una suscripción para usar la aplicación y cualquier otra información importante sobre la suscripción. Los usuarios no deben tener que realizar ninguna acción adicional para revisar la información.

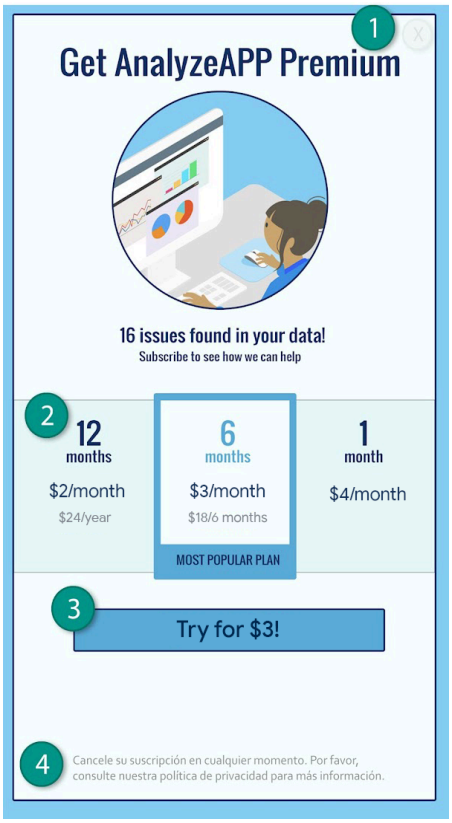
Las suscripciones deben brindar valor sostenido o recurrente a los usuarios durante su vigencia y no pueden usarse para ofrecerles beneficios únicos (por ejemplo, SKU que brindan monedas/créditos acumulados en una app o potenciadores de juegos de un solo uso). Su suscripción puede ofrecer bonificaciones de incentivo o promocionales, pero deben ser complementarias al valor sostenido o recurrente que se proporciona durante su vigencia**.** Los productos que no ofrezcan valor sostenido ni recurrente deben brindarse como productos integrados en la aplicación, y no como productos de suscripción.

No engañe a los usuarios ni haga pasar los beneficios únicos como suscripciones. Estas prácticas incluyen la modificación de una suscripción para convertirla en una oferta única (por ejemplo, cancelar la suscripción, darla de baja o minimizar el valor recurrente) después de que el usuario la compra.

Los siguientes son ejemplos de incumplimientos comunes:

- 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
- Suscripciones que no ofrecen valor sostenido ni recurrente (por ejemplo, ofrecer 1,000 gemas el primer mes y, luego, reducir el beneficio a 1 gema en los meses subsiguientes)
- Exigirle a un usuario que se registre para obtener una suscripción de renovación automática a fin de proporcionar un beneficio único y cancelar su suscripción sin que lo solicite después de la compra

Ejemplo 1:



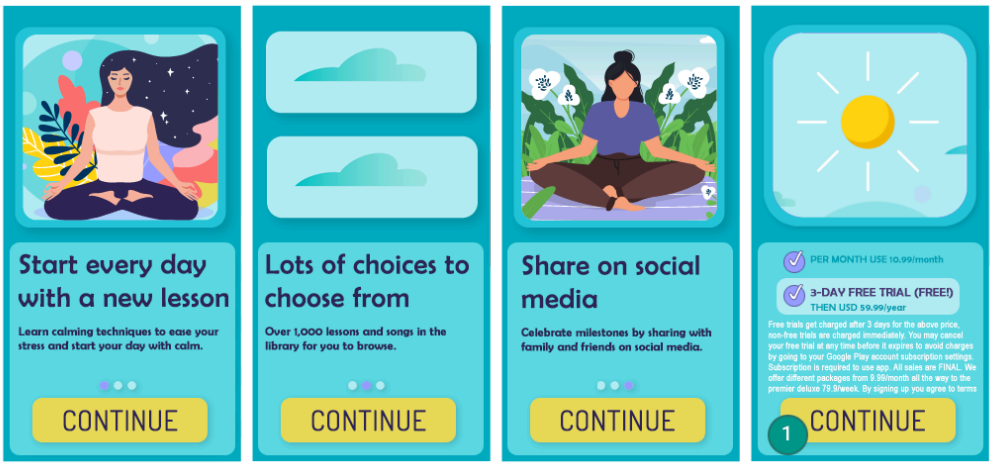
① Falta el botón para descartar o no se ve claramente, y los usuarios podrían no entender que pueden acceder a la función sin aceptar la oferta de suscripción.

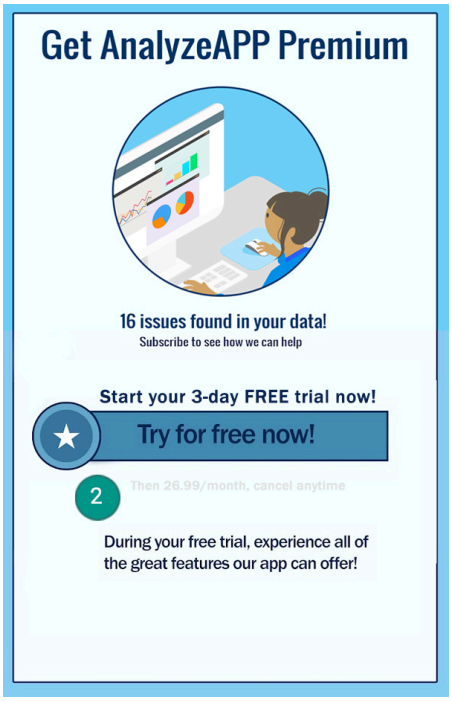
② La oferta muestra los precios en términos de costo mensual desglosado de manera más prominente que el importe que deberán pagar efectivamente los usuarios, quienes podrían no entender que se les cobrará un precio para seis meses en el momento de la suscripción.

③ La oferta solo muestra el precio de lanzamiento, por lo que los usuarios podrían no comprender cuál es el importe que se les cobrará automáticamente cuando finalice el período de lanzamiento.

④ La oferta no cumple con las políticas porque se presenta en un idioma y una moneda que no están localizados para el país del usuario, a diferencia de los términos y condiciones. Esto podría impedir que el usuario entienda completamente los detalles de la oferta.

Ejemplo 2:





① El usuario selecciona sin darse cuenta el botón “Continuar” final que activa la suscripción luego de hacer clics recurrentes en el mismo botón.

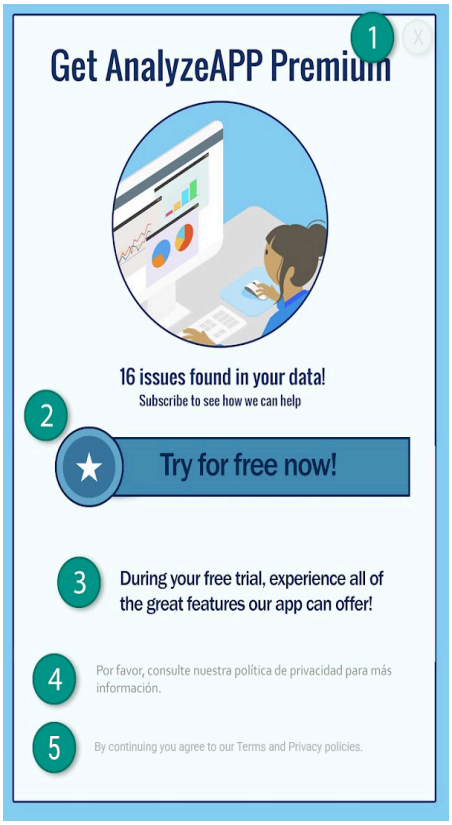
② El importe que se les cobra a los usuarios al final de la prueba es difícil de leer, y eso puede hacerles creer que el plan es gratuito.

Pruebas gratuitas y ofertas de lanzamiento

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

Los siguientes son ejemplos de incumplimientos comunes:

- 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 Falta el botón para descartar o no se ve claramente, y los usuarios podrían no entender que pueden acceder a la función sin aceptar la oferta de suscripción.

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

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

④ La oferta no cumple con las políticas porque se presenta en un idioma y una moneda que no están localizados para el país del usuario, a diferencia de los términos y condiciones. Esto podría impedir que el usuario entienda completamente los detalles de la oferta.

⑤ La oferta no explica de manera clara cómo cancelar la prueba gratuita para los usuarios que no deseen continuar con una suscripción pagada después de que finalice el período de prueba.

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:

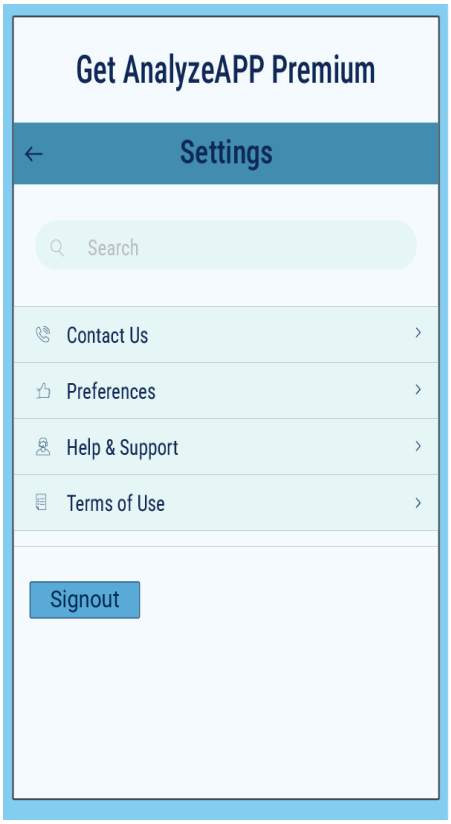
- Un vínculo al Centro de Suscripciones de Google Play (en el caso de las suscripciones que usen el sistema de facturación de Google Play) y/o
- Un acceso directo al proceso de cancelación

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. Es posible que los usuarios de algunos países

tengan la opción de cancelar su suscripción de forma inmediata y recibir un reembolso prorrateado, de acuerdo con la legislación aplicable.

Como proveedor de contenido o acceso, debe implementar una política de reembolso más flexible directamente con los usuarios. Es su responsabilidad notificarles sobre los cambios en las políticas de suscripción, cancelación y reembolsos, y garantizar que las políticas satisfagan la legislación vigente.

Los siguientes son ejemplos de incumplimientos comunes:



En la aplicación falta un vínculo para administrar y cancelar suscripciones en la configuración de la cuenta o una página equivalente.

Programa del SDK de Anuncios con Autocertificación para Familias

Si publica anuncios en su aplicación y esta tiene como público objetivo únicamente a niños según se describe en la Política de Familias , solo debe usar versiones de SDK de anuncios que cumplan con la autocertificación que se estipula en las políticas de Google Play, incluidos los requisitos del Programa del SDK de Anuncios con Autocertificación para Familias que se indican a continuación.

Si el público objetivo de su aplicación incluye tanto niños como usuarios mayores, debe asegurarse de que los anuncios que se muestren a niños provengan exclusivamente de una de estas versiones de SDK de anuncios con autocertificación (por ejemplo, mediante el uso de pantallas neutrales de comprobación de edad).

Tenga en cuenta que es su responsabilidad asegurarse de que todas las versiones de SDK que implemente en su aplicación, incluidas las versiones de SDK de Anuncios con Autocertificación, satisfagan todas las políticas, leyes locales y reglamentaciones aplicables. 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 en qué consisten los comportamientos y el contenido de 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 en 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 y el suministro de una aplicación de prueba.
- 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.

Puede obtener más información sobre el uso de marcas de agua en creatividades de anuncios y cómo proporcionar una aplicación de prueba aquí.

A continuación 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 y consultar qué versiones específicas de esos SDK de anuncios cuentan con la autocertificación para usarse en aplicaciones 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.

Los siguientes son 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
- Texto o imágenes en el título, el ícono o el nombre del desarrollador de la aplicación que indiquen la clasificación o el rendimiento en la tienda, el precio o información sobre promociones, o que sugieran relaciones con programas existentes de Google Play

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

Metadatos

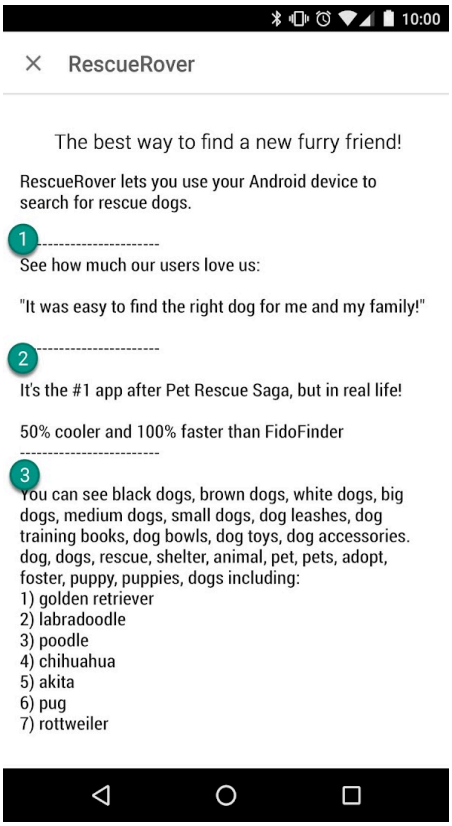
Los usuarios confían en las descripciones de las aplicaciones para comprender su funcionalidad y propósito. No permitimos aplicaciones con metadatos engañosos, no descriptivos, irrelevantes, excesivos, inapropiados ni con formato inadecuado, incluidos, sin limitaciones, la descripción de la aplicación, el nombre del desarrollador, el título, el ícono, las capturas de pantalla y las imágenes promocionales. Los desarrolladores deben proporcionar una descripción clara y bien escrita 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 o instalación cuando la aplicación no está relacionada con la descarga de contenido. El título de la aplicación debe tener 30 caracteres o menos. No se deben usar imágenes ni texto en el título, el ícono o el nombre del desarrollador de la aplicación que indiquen la clasificación o el rendimiento en la tienda, el precio o información sobre promociones, o que sugieran relaciones con programas existentes de Google Play

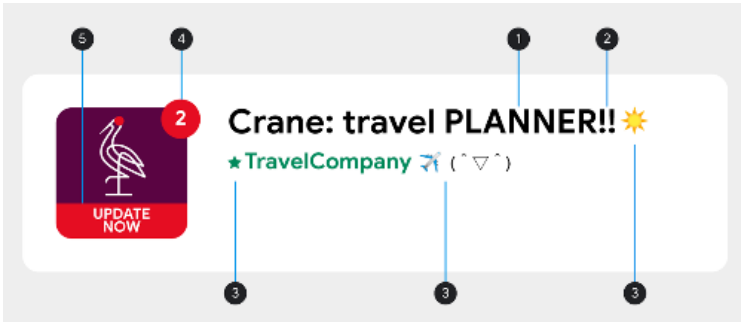
Además de los requisitos que se mencionan aquí, es posible que, según las Políticas para Desarrolladores de Google Play, se le exija que proporcione información adicional sobre los

metadatos.

Los siguientes son ejemplos de incumplimientos comunes:

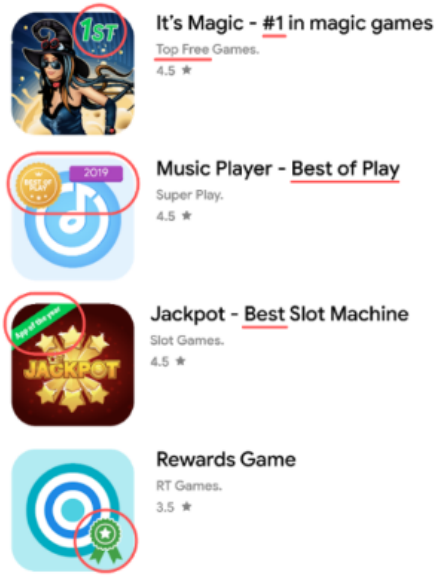


① Testimonios de usuarios anónimos o sin la atribución correspondiente
② Comparación de datos de aplicaciones o marcas
③ Bloques de palabras y listas de palabras horizontales o verticales

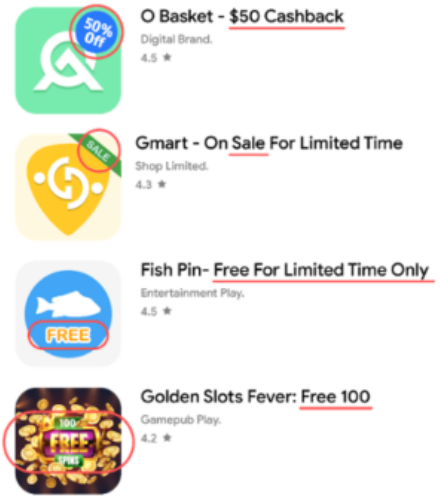


① SOLO MAYÚSCULAS, aunque no sean parte del nombre de la marca
② Secuencias de caracteres especiales que son irrelevantes para la aplicación
③ Uso de emojis, emoticones (incluidos los kaomojis) y caracteres especiales
④ Símbolos engañosos
⑤ Texto engañoso

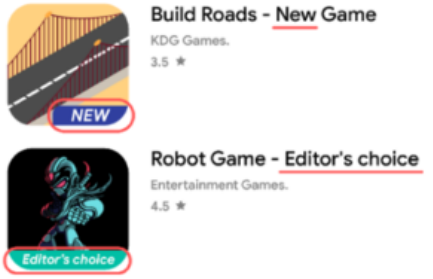
- Imágenes o texto que indiquen la calificación o el rendimiento en Play Store, como "App del año", "Núm. 1", "La mejor de Google Play en 20XX", "Popular", íconos de premios, etcétera



- 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



Los siguientes son ejemplos de textos, imágenes o videos inapropiados para una ficha de Play Store:

- Imágenes o videos con contenido de carácter sexual (no incluya imágenes con contenido provocativo, como pechos, nalgas, genitales o cualquier contenido anatómico vulgarizado, tanto real como ilustrado).
- Usar lenguaje profano, vulgar o de otra manera inapropiado para el público general en la ficha de Play Store de su aplicación
- Violencia gráfica representada de manera explícita en íconos de aplicaciones, videos o imágenes promocionales

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

A continuación, se detallan algunas prácticas recomendadas:

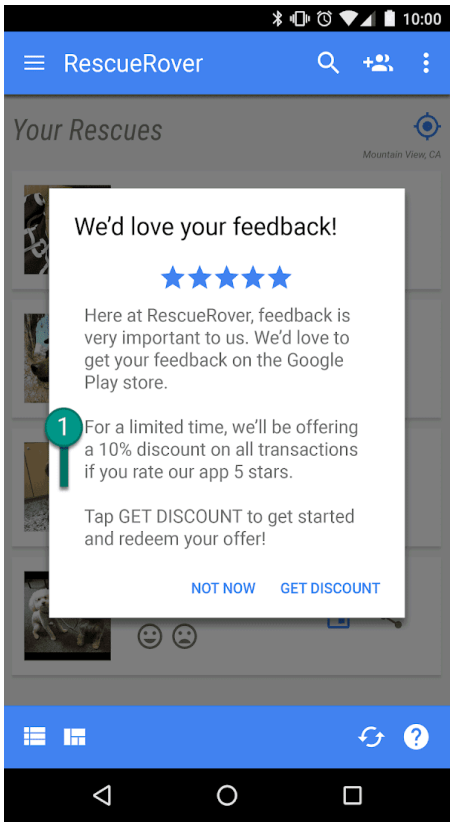
- Destaque lo mejor de la aplicación. Comparta hechos interesantes para que los usuarios entiendan qué tiene de especial.
- Asegúrese de que el título y la descripción de la app describan su funcionalidad de forma precisa.
- Evite el uso de palabras clave o referencias que sean repetitivas o que no estén 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, Entre otros aspectos, esto incluye el aumento de la cantidad de opiniones, instalaciones o calificaciones de productos a través de medios ilegítimos, como calificaciones y opiniones fraudulentas o que se hayan incentivado, o el aliento a los usuarios a instalar otras aplicaciones como la funcionalidad principal de la aplicación.

Los siguientes son ejemplos de incumplimientos comunes:

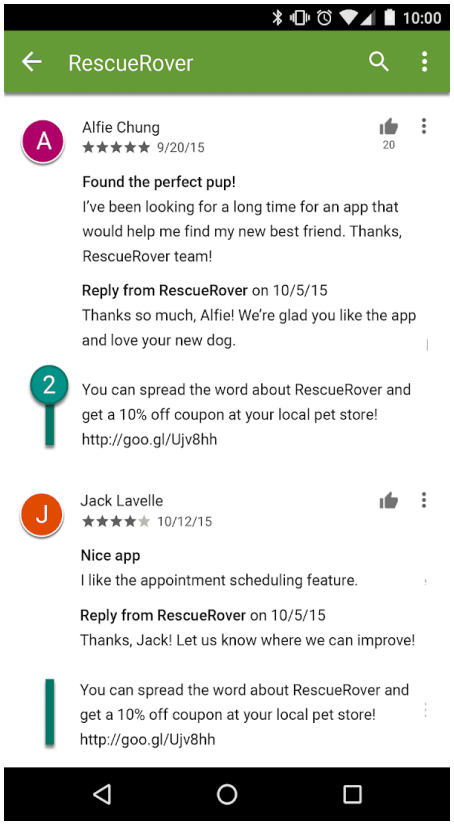
- Solicitarles a los usuarios que califiquen una app a cambio de un incentivo:



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

- Enviar de forma reiterada calificaciones cuyos autores se hagan pasar por usuarios para influenciar la posición de una aplicación en Google Play

- Enviar o motivar a los usuarios a que envíen opiniones que incluyan contenido inapropiado, como afiliados, cupones, códigos de juegos, direcciones de correo electrónico o vínculos a otras 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 confían en que son auténticas y relevantes. A continuación, se detallan algunas de las prácticas recomendadas a la hora de responder la reseña 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.

Clasificaciones del contenido

La Coalición Internacional de Calificación 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 pertinentes a nivel local. Las autoridades regionales de la IARC mantienen lineamientos que se usan para determinar el nivel de madurez del contenido en una aplicación. No permitimos aplicaciones que no tengan clasificación de contenido en Google Play. Tenga en cuenta que los anuncios que se muestren en la aplicación no pueden incluir contenido para un público más maduro que el del contenido principal de la propia aplicación. Consulte la política Anuncios inapropiados para obtener más información.

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 se muestre "Sin clasificación", 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 de contenido, debe completar un nuevo cuestionario en Play Console.

La clasificación del contenido que se asigne a su aplicación es específica para el contenido de esta y no incluye otras funciones ni prácticas, por ejemplo, anuncios o acuerdos con los usuarios. Es su responsabilidad informar a los usuarios de cualquier consideración adicional relativa a la edad, como prácticas de privacidad específicas de la edad.

Visite el Centro de ayuda para obtener más información sobre el cuestionario, conocer las diferentes autoridades de clasificación en las diferentes regiones y aprender a 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.

Noticias y revistas

Todas las aplicaciones de Noticias y Revistas deben autodeclararse como tales en Google Play Console.

Una aplicación de noticias y revistas es la que cumple con una o más de estas condiciones:

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

Para obtener más orientación sobre qué se considera una aplicación de "Noticias" o de "Revista", consulte los Requisitos para las apps de noticias y contenido relacionado.

Además, las aplicaciones de Noticias y Revistas deben hacer lo siguiente:

- Proporcionar la fuente de los artículos de noticias y revistas, incluidos, sin limitaciones, el editor o autor original de cada uno de ellos
- Actualizar su contenido de forma regular (no deben tener contenido estático)
- Ofrecerles a los usuarios acceso claro y sencillo a información de contacto actualizada de las personas a cargo de la aplicación

- Ofrecerles a los usuarios información clara sobre las fuentes de publicación del contenido de terceros (como cuando se proporcionan a través de apps de agregadores de noticias y revistas)
- Ofrecerles a los usuarios una vista previa del contenido integrado en la aplicación antes de que lo compren (si se requiere membresía o suscripción)
- No tener como objetivo principal el marketing de afiliación o los ingresos publicitarios

Spam, Funcionalidad y Experiencia del Usuario

Las aplicaciones deben brindarles a los usuarios un nivel básico de funcionalidad y contenido adecuados para ofrecer una experiencia del usuario atractiva. Las aplicaciones que fallan, que muestran un comportamiento incoherente con la experiencia del usuario funcional o que solo sirven para enviar spam a los usuarios o a Google Play no contribuyen para ampliar el 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.

El siguiente es un ejemplo de incumplimiento común:

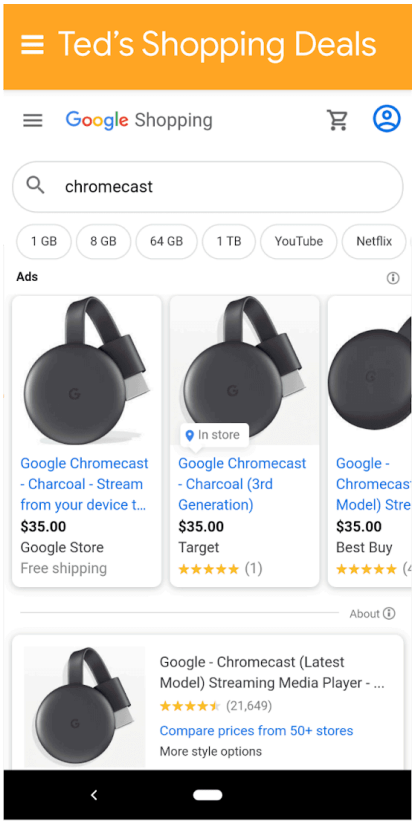
- Cuando el usuario presiona el botón "Compartir", la app envía mensajes en nombre suyo sin darle la posibilidad de confirmar el contenido y los destinatarios:

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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:



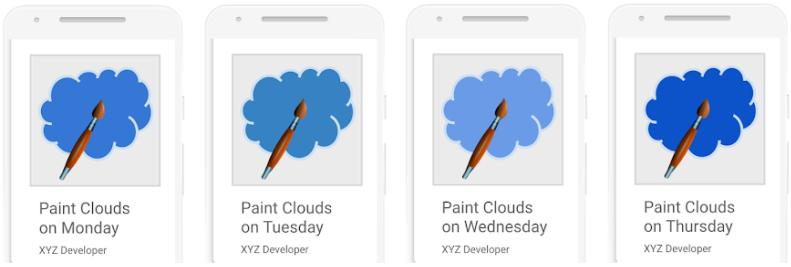
① Esta app se llama "Ofertas de compras de Ted" y solo proporciona una vista web de Google Shopping.

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.

Los siguientes son ejemplos de incumplimientos comunes:

- 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)



Funcionalidad, Contenido y Experiencia del Usuario

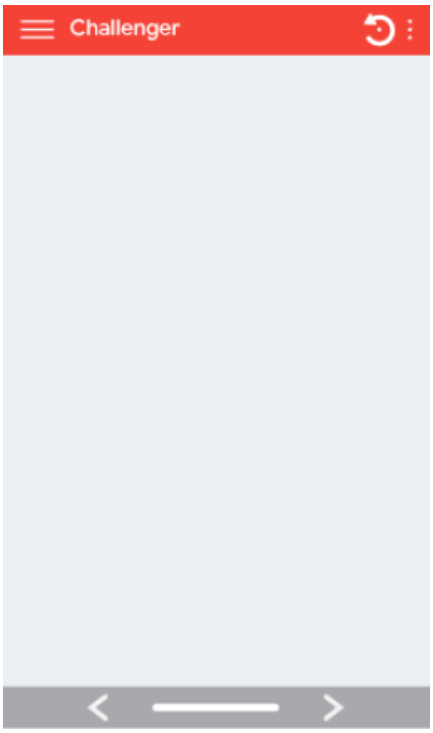
Las aplicaciones deben proporcionar una experiencia del usuario estable, interesante y responsiva. No se permiten en Google Play aplicaciones que fallan, no tienen el nivel básico de utilidad adecuada como aplicaciones para dispositivos móviles, no tienen contenido atractivo o presentan comportamientos que no son coherentes con una experiencia del usuario interesante y funcional.

Contenido y Funcionalidades Limitados

No permitimos aplicaciones que solo tengan contenido y funcionalidades limitados.

El siguiente es un ejemplo de incumplimiento común:

- Aplicaciones que son estáticas sin funcionalidades específicas (por ejemplo, aplicaciones de archivos PDF o de texto únicamente)
- Aplicaciones con muy poco contenido y que no proporcionan una experiencia del usuario interesante, por ejemplo, aplicaciones de un único fondo de pantalla
- Aplicaciones que no tienen ninguna función o que están diseñadas para no realizar ninguna acción



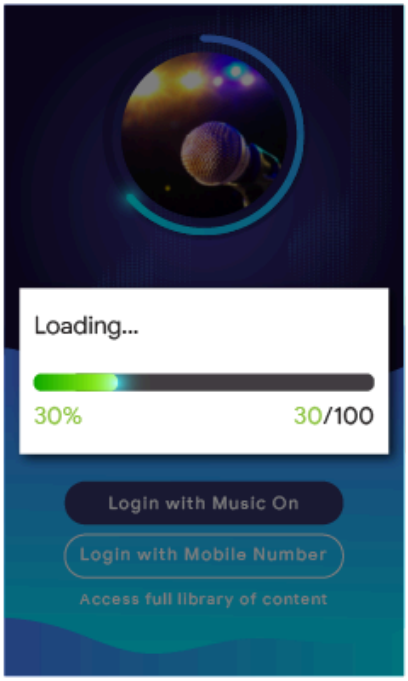
Funcionalidad dañada

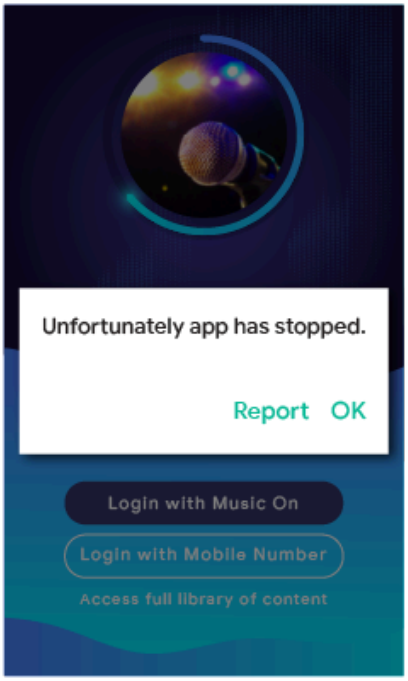
No permitimos las aplicaciones que fallan, se cierran de manera forzada, se bloquean o funcionan de manera anormal.

Los siguientes son ejemplos de incumplimientos comunes:

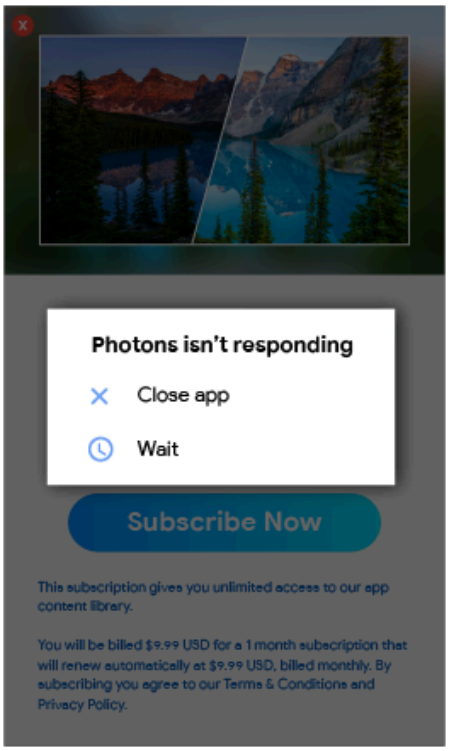
- Apps que **no se instalan**

- 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 .

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.

Políticas de Familias de Google Play

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

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

En todas las aplicaciones que satisfagan las políticas de Familias de Google Play se puede habilitar la opción de que las califiquen para el programa con Contenido Aprobado por Profesores, pero no podemos garantizar que su aplicación se incluirá en el mencionado programa.

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.

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 dar lugar a la eliminación o suspensión de la aplicación.

1. **Contenido de la aplicación:** El contenido de la aplicación al que pueden acceder los 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 allí (regiones limitadas), pero seguirá sin estar disponible en otras regiones.
2. **Funciones de la aplicación:** 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 sin permiso del administrador o el propietario del sitio web.
3. **Respuestas en Play Console:** Debe responder con precisión las preguntas relacionadas con su aplicación en Play Console y actualizar esas respuestas para que reflejen con exactitud cualquier

cambio que realice en ella. Esto incluye, sin limitaciones, proporcionar respuestas precisas sobre su aplicación en la sección Público Objetivo y Contenido, la sección de Seguridad de los datos y el Cuestionario de Clasificación del Contenido de la IARC.

4. **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 recopile a través de APIs o SDKs 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 garantizar que su aplicación implemente las prácticas de datos que se mencionan a continuación:
   - Las aplicaciones que se dirijan únicamente a niños no deben transmitir el identificador de publicidad de Android (AAID), números de serie de SIM, Build Serial, BSSID, MAC, SSID, IMEI ni IMSI.
     - Las aplicaciones que se dirijan únicamente a niños no deben solicitar el permiso de AD_ID cuando el nivel de API objetivo sea Android 33 o una versión posterior.
   - 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 dirijan 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 que no sean compatibles con CDM.

5. **APIs y SDKs:** Debe asegurarse de que su aplicación implemente todas las APIs y SDKs de forma adecuada.
   - Las aplicaciones que se dirijan únicamente a niños no deben contener APIs ni SDKs cuyo uso no esté aprobado para servicios dirigidos principalmente a niños.
     - Por ejemplo, un Servicio de API que use tecnología de OAuth para fines de autenticación y autorización cuyas condiciones del servicio establezcan que no está aprobado para usarlo en servicios dirigidos a niños.
   - Las aplicaciones orientadas tanto a niños como a públicos mayores no deben implementar APIs ni SDKs 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 contenido de la aplicación desde una API o un SDK que no esté aprobado para su uso en servicios dirigidos a niños.

6. **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 (por ejemplo, estar atento al entorno)
   - La aplicación no debe requerir el uso de un dispositivo no recomendado para niños (por ejemplo, Daydream, Oculus)

7. **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 (es decir, con el uso de PIN, contraseñas, fechas de nacimiento, verificación por correo electrónico, ID con 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 dirigirse a niños. Entre algunos ejemplos, se incluyen aplicaciones con el estilo de Chatroulette, aplicaciones de citas, salas de chat abiertas enfocadas en niños, etcétera.

8. **Cumplimiento legal:** Debe asegurarse de que la aplicación, incluidos todos los SDKs o APIs que esta llame o use, cumpla con 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.

Los siguientes son ejemplos de incumplimientos comunes:

- Apps que promueven juegos para niños en sus fichas de Play Store, pero cuyo contenido solo es apropiado para adultos
- Apps que implementan APIs 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
- Aplicaciones con vínculos a sitios web que presentan contenido que infringe las políticas del Programa para Desarrolladores de Google Play
- Aplicaciones que muestran anuncios para adultos (p. ej., contenido violento, sexual o de juegos de apuestas) a niños

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 los anuncios

Si la aplicación muestra anuncios a niños o usuarios de edades desconocidas, debe respetar los siguientes lineamientos:

- Solo se deben usar los SDK de anuncios con autocertificación para Familias de Google Play a fin de mostrar anuncios a esos usuarios.
- Asegúrese 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).
- Asegúrese de que los anuncios que se muestren a esos usuarios presenten contenido apropiado para niños.
- Asegúrese de que los anuncios que se muestren a esos usuarios sigan los requisitos de formato de los anuncios para Familias.
- Garantice el cumplimiento de todas las reglamentaciones legales aplicables y los estándares de la industria relacionados con la publicidad dirigida a niños.

Requisitos de formato de los anuncios

Los elementos monetizados y los anuncios que muestre su aplicación no deben incluir contenido engañoso ni estar diseñados de manera tal que los usuarios menores de edad que usen la aplicación hagan clic en ellos de forma involuntaria.

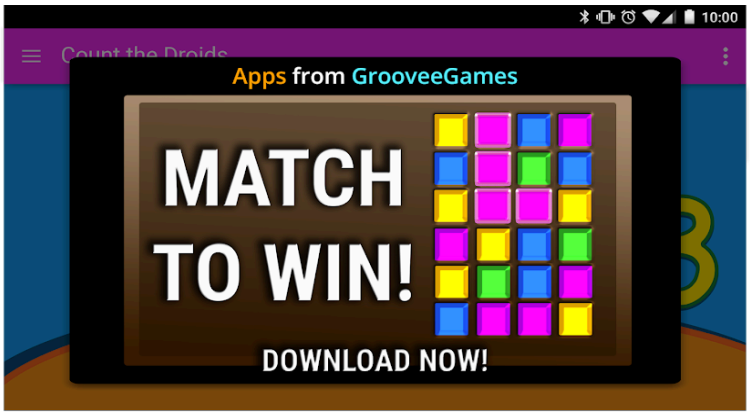
Si los niños son el único público objetivo de su aplicación, se prohíben los elementos que se detallan a continuación. Si los públicos objetivo de su aplicación incluyen niños y públicos mayores, se prohíben los elementos que se detallan a continuación cuando se muestren anuncios a niños o usuarios con edades desconocidas:

- 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 (por ejemplo, Paneles publicitarios)
- Monetización y publicidad que interfiera con el uso normal de la aplicación o la mecánica habitual del juego, incluidos los anuncios recompensados o de habilitación que no se puedan cerrar después de 5 segundos
- Los elementos de monetización y publicidad cuyos componentes no interfieran con el uso normal de la aplicación o la mecánica habitual del juego pueden persistir durante más de 5 segundos (por ejemplo, contenido de video con anuncios integrados)
- Monetización y publicidad con anuncios intersticiales que se muestren inmediatamente después de que se abre la aplicación
- Varias posiciones de anuncios en una página (por ejemplo, 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 y publicidad cuyos componentes no se distingan fácilmente del contenido de la aplicación, como offerwalls y otras experiencias de anuncios interactivos
- Tácticas impactantes o de manipulación emocional para alentar las reproducciones de anuncios o las compras directas desde la aplicación
- Anuncios engañosos que obligan al usuario a hacer clic con un botón para descartar que activan otro anuncio o que hacen que los anuncios aparezcan repentinamente en áreas de la aplicación donde el usuario suele presionar para usar otra función
- Falta de distinción entre el uso de monedas virtuales de juego y dinero real para hacer compras directas desde la aplicación

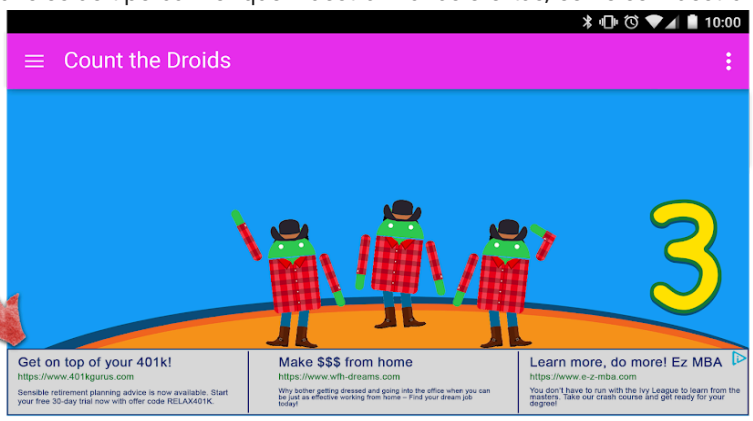
Los siguientes son ejemplos de incumplimientos comunes:

- 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:

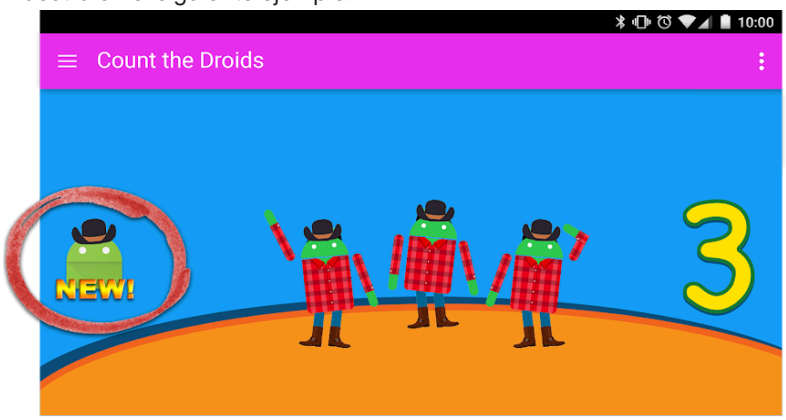
- Monetización y publicidad que ocupan la mayor parte de la pantalla del dispositivo sin brindarle al usuario una manera clara de descartarlos, como se muestra en el siguiente ejemplo:



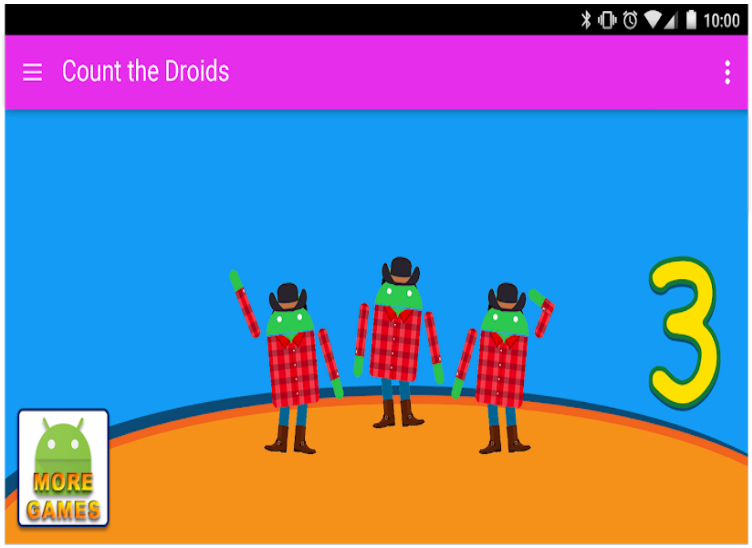
- Anuncios de tipo banner que muestran varias ofertas, como se muestra en el siguiente ejemplo:



- 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.

SDK de Anuncios

Si publica anuncios en su aplicación y su público objetivo solo incluye niños, debe usar únicamente las versiones de 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 versiones de SDK de anuncios con autocertificación de Google Play.

Visite la página de la política del Programa del SDK de Anuncios con Autocertificación para Familias a fin de obtener más detalles sobre estos requisitos y consulte aquí para ver la lista actual de versiones de SDK de anuncios con Autocertificación para Familias.

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 publicidad, contenido comercial y compras directas desde la aplicación. Comuníquese con sus proveedores de SDK de anuncios para obtener más información acerca de sus políticas de contenido y prácticas publicitarias.

Política del SDK de Anuncios con Autocertificación para Familias

Google Play se compromete a ofrecer una experiencia segura para niños y familias. Un elemento clave de ese compromiso es ayudar a garantizar que los niños solo vean anuncios adecuados para su edad y que sus datos se manejen de manera apropiada. Para ayudarnos a alcanzar ese objetivo, requerimos que los SDK de anuncios y las plataformas de mediación cuenten con una autocertificación de que son apropiados para niños y satisfacen las Políticas del Programa para Desarrolladores de Google Play y las Políticas de Familias de Google Play , incluidos los Requisitos del Programa del SDK de Anuncios con Autocertificación para Familias .

El Programa del SDK de Anuncios con Autocertificación para Familias de Google es una forma importante en la que los desarrolladores pueden identificar qué SDK de anuncios o plataformas de mediación cuentan con la autocertificación de que son apropiados para usarse en aplicaciones diseñadas específicamente para niños.

La tergiversación de cualquier información relacionada con su SDK, incluida la que consta en la solicitud del formulario de interés , puede tener como resultado la eliminación o suspensión de su SDK del Programa del SDK de Anuncios con Autocertificación para Familias, por lo que es fundamental proporcionar la información correcta.

Requisitos de la política

Si su SDK o plataforma de mediación publican aplicaciones que son parte del Programa para Familias de Google Play, usted debe satisfacer todas las Políticas para Desarrolladores de Google Play, incluidos los requisitos que se incluyen a continuación. El incumplimiento de alguno de los requisitos de las políticas podría causar su eliminación o suspensión del Programa del SDK de Anuncios con Autocertificación para Familias.

Es su responsabilidad asegurarse de que su SDK o plataforma de mediación satisfaga los requisitos, por lo que debe asegurarse de revisar las Políticas del Programa para Desarrolladores de Google Play, las Políticas de Familias de Google Play y los Requisitos del Programa del SDK de Anuncios con Autocertificación para Familias.

1. **Contenido del anuncio:** El contenido de sus anuncios al que puedan acceder niños debe ser apropiado para ellos.
   - Usted debe (i) definir el significado de comportamientos y contenido del anuncio reprochables, y (ii) prohibirlos en sus condiciones o políticas. Las definiciones deben satisfacer las Políticas del Programa para Desarrolladores de Google Play.
   - Asimismo, usted debe crear un método para clasificar sus creatividades de anuncios según 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 que proporciona Google a los SDK una vez que los desarrolladores completan el formulario de interés .

- Usted debe garantizar que, cuando se usen ofertas en tiempo real para mostrar anuncios a los niños, las creatividades se hayan revisado y satisfagan los requisitos que se indicaron anteriormente.
- Además, debe contar con un mecanismo para identificar visualmente las creatividades que provienen de su inventario (por ejemplo, una marca de agua en la creatividad del anuncio con un logotipo visual de su empresa o alguna funcionalidad similar).

2. **Formato del anuncio:** Usted debe garantizar que todos los anuncios que se muestren a usuarios menores de edad sigan los requisitos de formato de los anuncios para Familias y permitir que los desarrolladores seleccionen formatos de anuncios que satisfagan la Política de Familias de Google Play.
   - La publicidad no debe incluir contenido engañoso ni estar diseñada de manera tal que los usuarios menores de edad puedan hacer clic en ella de forma involuntaria. No se permiten los anuncios engañosos que obligan al usuario a hacer clic con un botón para descartar que activan otro anuncio o que hacen que los anuncios aparezcan repentinamente en áreas de la aplicación donde el usuario suele presionar para usar otra función.
   - No se permite la publicidad invasiva, incluida la que ocupe toda la pantalla o interfiera con el uso normal y no proporcione un medio claro para descartar el anuncio (por ejemplo, Paneles publicitarios).
   - La publicidad que interfiere con el uso normal de la aplicación o la mecánica habitual del juego, incluidos los anuncios recompensados o de habilitación, debe poder cerrarse después de 5 segundos.
   - No se permite la colocación de varios anuncios en una misma página. Por ejemplo, no se permiten los anuncios de banner que publiquen varias ofertas en una posición o que muestren más de un anuncio de banner o video.
   - La publicidad debe distinguirse del contenido de la aplicación de forma clara. No se permiten los Offerwalls ni las experiencias de anuncios interactivos que los usuarios menores de edad no puedan identificar claramente como publicidad.
   - La publicidad no debe usar tácticas impactantes ni de manipulación emocional para alentar las reproducciones de anuncios.
3. **IBA/Remarketing:** Usted debe garantizar que los anuncios que se muestran a usuarios menores de edad no involucren publicidad basada en intereses (segmentada para usuarios individuales que cumplen con ciertas características en función de su comportamiento de exploración en línea) ni de remarketing (segmentada para usuarios individuales en función de interacciones previas con una aplicación o un sitio web).
4. **Prácticas de datos:** Usted, el proveedor del SDK, debe ser transparente en la manera en que maneja los datos de los usuarios (por ejemplo, información recopilada sobre un usuario o de parte de este, incluida la información del dispositivo). Es decir, debe divulgar si su SDK accede a los datos, así como cuando los recopila, usa y comparte, además de limitar su uso a los fines divulgados. Estos requisitos de Google Play se agregan a las condiciones prescritas por las leyes aplicables en materia de privacidad y protección de datos. Usted debe divulgar cuando recopila cualquier información personal y sensible de niños, incluidos, sin limitaciones, los datos del dispositivo, del sensor de la cámara y el micrófono, y de uso de anuncios, así como cualquier información de autenticación y el ID de Android.
   - Debe permitir que los desarrolladores soliciten el tratamiento de contenido dirigido a niños, ya sea por solicitud o por aplicación, para fines de publicación de anuncios. 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 SDKs de anuncios inhabiliten los anuncios personalizados, la publicidad basada en intereses y el remarketing como parte del contenido dirigido a niños.

- Usted debe garantizar que, cuando se usen ofertas en tiempo real para mostrar anuncios a niños, se propaguen los indicadores de privacidad a los ofertantes.
- No debe transmitir AAID, números de serie de SIM, Build Serial, BSSID, MAC, SSID, IMEI ni IMSI de niños o usuarios de edades desconocidas.

5. **Plataformas de Mediación:** A la hora de publicar anuncios para niños, usted debe hacer lo siguiente:
   - Use únicamente SDKs 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.
6. **Autocertificación y Cumplimiento:** Usted debe proporcionarle a Google suficiente información, como la que se indica en el formulario de interés , para verificar el cumplimiento de la política del SDK de anuncios con todos los requisitos de autocertificación, incluido, sin limitación, lo siguiente:
   - Debe proporcionar una versión en inglés de las Condiciones del Servicio, la Política de Privacidad y la Guía de Integración para Publicadores de su SDK o Plataforma de Mediación.
   - Debe enviar una aplicación de prueba de muestra que use la versión más reciente del SDK de anuncios que satisfaga los requisitos. La aplicación de prueba de muestra debe ser un APK de Android completamente compilado y ejecutable que use todas las funciones del SDK. Requisitos para las aplicaciones de prueba:
     - Debe enviarse como un APK de Android totalmente compilado y ejecutable, diseñado para ejecutarse en un factor de forma de teléfono.
     - Debe usar la versión más reciente o próxima a publicarse del SDK de anuncios que cumpla con las políticas de Google Play.
     - Debe usar todas las funciones de su SDK de anuncios, incluida la opción de llamar al SDK de anuncios para recuperar y mostrar publicidad.
     - Debe tener acceso completo a todos los inventarios de anuncios publicados o en proceso de publicación en la red mediante creatividades solicitadas a través de la aplicación de prueba.
     - No debe restringirse por ubicación geográfica.
     - Si su inventario se segmenta para un público mixto, la aplicación de prueba debe ser capaz de diferenciar entre las solicitudes de creatividades de anuncios del inventario completo y del inventario adecuado para niños o todas las edades.
     - No se debe restringir a anuncios específicos dentro del inventario, a menos que se controle mediante la pantalla neutral de comprobación de edad.
7. Usted debe responder de manera oportuna ante cualquier solicitud de información subsiguiente y autocertificar que todos los lanzamientos de nuevas versiones satisfagan las Políticas del Programa para Desarrolladores de Google Play más recientes, incluidos los Requisitos de la Política de Familias.
8. **Cumplimiento legal:** 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.
   - Usted debe garantizar que su SDK o plataforma de mediación cumpla con 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.

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

Consulte la página del Programa del SDK de Anuncios con Autocertificación para Familias si desea obtener más detalles sobre sus requisitos.

Aplicación

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 aplicaciones al momento de la instalación. También analiza su dispositivo periódicamente. Si detecta una aplicación potencialmente dañina, es posible que haga lo siguiente:

- Enviarle una notificación. Para quitar la aplicación, presione la notificación y, luego, Desinstalar
- Inhabilitar la aplicación hasta que la desinstale
- Quitar la aplicación automáticamente. En la mayoría de los casos, si se detecta una aplicación dañina, recibirá una notificación que te indicará que se quitó

Cómo funciona la protección contra software malicioso

Para brindarle 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 su dispositivo
- Las URL potencialmente dañinas

- El sistema operativo y las aplicaciones instalados en su dispositivo mediante Google Play o alguna otra fuente

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

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

Cómo funcionan las alertas de privacidad

Google Play Protect lo alertará cuando se quite alguna aplicación de Google Play Store, dado que esta podría acceder a su información personal, y tendrá la opción de desinstalarla.

Proceso de aplicación de las políticas

Cuando revisamos el contenido o las cuentas para determinar si son ilegales o incumplen nuestras políticas, tenemos en cuenta información de distinta índole a la hora de tomar una decisión, lo que incluye metadatos de las aplicaciones (por ejemplo, su título o descripción), la experiencia en la aplicación, la información de la cuenta (como el historial de incumplimientos de políticas), todos los códigos de terceros en las aplicaciones y otros detalles que se proporcionan a través de mecanismos de generación de informes (si corresponde) y revisiones de iniciativa propia. Tenga en cuenta que usted es responsable de garantizar que todos los códigos de terceros (por ejemplo, un SDK) que se utilicen en su aplicación, así como las prácticas de terceros con respecto a ella, satisfagan todas las políticas del Programa para Desarrolladores de Google Play.

Si su aplicación o su cuenta de desarrollador incumplen alguna de nuestras políticas, tomaremos las medidas correspondientes que se detallan a continuación. Además, le enviaremos por correo electrónico información relevante sobre las medidas que tomamos, junto con instrucciones sobre cómo apelar si considera que se tomaron medidas por error.

Es posible que los avisos administrativos o de eliminación no indiquen cada uno de los incumplimientos presentes en su cuenta, aplicación o catálogo completo de aplicaciones. Los desarrolladores son responsables de abordar los problemas de incumplimiento y de llevar a cabo la diligencia debida adicional que se requiera para garantizar que sus aplicaciones o cuentas restantes cumplan por completo con las políticas. Si no resuelve los incumplimientos en su cuenta y todas sus aplicaciones, es posible que se apliquen más acciones de cumplimiento de políticas.

Los incumplimientos graves o repetidos (como software malicioso, fraude o aplicaciones que perjudiquen el dispositivo o al usuario) de estas políticas o del Acuerdo de Distribución para Desarrolladores (DDA) darán lugar al cierre de cuentas de Desarrollador de Google Play individuales o relacionadas.

Acciones de aplicación de las políticas

Las diferentes acciones de cumplimiento de políticas pueden tener diversos efectos en sus aplicaciones. Usamos una combinación de evaluaciones automatizadas y manuales para revisar las aplicaciones y el contenido que se incluye en ellas y, de ese modo, detectar y evaluar el contenido que incumple nuestras políticas y es dañino para los usuarios y el ecosistema de Google Play en general. El uso de modelos automatizados nos permite detectar más incumplimientos y evaluar los problemas potenciales más rápido, lo cual ayuda a mantener un entorno seguro para todos en Google Play. Nuestros modelos automatizados pueden quitar el contenido que incumple las políticas o, en los casos en que se necesita una determinación más detallada, marcarlos para una revisión adicional por parte de operadores y analistas capacitados que llevan a cabo evaluaciones de contenido; por ejemplo,

cuando se requiere comprender el contexto del contenido específico. Una vez que se obtienen, los resultados de estas revisiones manuales se emplean para generar datos de entrenamiento con el objeto de mejorar aún más nuestros modelos de aprendizaje automático.

En la siguiente sección, se describen las diversas acciones que Google Play puede realizar y el impacto sobre su aplicación o cuenta de desarrollador de Google Play.

A menos que se indique lo contrario en una comunicación de cumplimiento de políticas, estas acciones afectan a todas las regiones. Por ejemplo, si se suspende su aplicación, dejará de estar disponible en todas las regiones. Además, a menos que se indique lo contrario, las acciones permanecerán vigentes a menos que usted las apele y que se conceda tal apelación.

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

- Se eliminarán de Google Play la aplicación y sus versiones anteriores, y ya no estarán disponibles para que los usuarios la descarguen.
- Dado que se elimina la aplicación, los usuarios no podrán ver su ficha de Play Store. Esta información se restablecerá una vez que envíe una actualización de la aplicación 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 su cuenta de Desarrollador de Google Play, pero, si se producen varias, esta podría suspenderse.

Nota: No intente volver a publicar una aplicación que se eliminó hasta que haya corregido todos los incumplimientos de políticas.

Suspensión

- Se eliminarán de Google Play la aplicación y sus versiones anteriores, y ya no estarán disponibles para que los usuarios las descarguen.
- La suspensión puede ocurrir como resultado de incumplimientos graves o reiterados de las políticas, así como de eliminaciones o rechazos repetidos de aplicaciones.
- Dado que se suspenderá la aplicación, los usuarios no podrán ver su ficha de Play Store.
- Ya no podrá usar el APK ni el paquete de aplicación de una aplicación suspendida.
- Los usuarios no podrán realizar compras directas desde la aplicación ni utilizar funciones de facturación integrada en la aplicación.
- Las suspensiones cuentan como faltas que hacen que su cuenta de Desarrollador de Google Play deje de estar en regla. Si recibe múltiples faltas, es posible que se cierren las cuentas de Desarrollador de Google Play individuales y relacionadas.

Visibilidad limitada

- La visibilidad de su aplicación en Google Play está restringida. Su aplicación seguirá 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 aplicación no afecta la posición de su cuenta de Desarrollador de Google Play.
- El estado de Visibilidad Limitada de la aplicación no afecta la capacidad de los usuarios de ver su ficha de Play Store existente.

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.

Estado de Cuenta Restringida

- Cuando su cuenta de desarrollador se encuentre en estado restringido, se eliminarán de Google Play todas las aplicaciones de su catálogo, y no podrá publicar nuevas aplicaciones ni volver a publicar las existentes. De todos modos, tendrá acceso a Play Console.
- Dado que se eliminan todas las aplicaciones, los usuarios no podrán ver la ficha de Play Store de su aplicación ni su perfil de desarrollador.
- Los usuarios actuales no podrán realizar compras directas desde la aplicación ni utilizar funciones de facturación integrada en su aplicación.
- De todos modos, podrá usar Play Console para proporcionarle más información a Google Play y enmendar la información de su cuenta.
- Podrá volver a publicar sus aplicaciones una vez que haya corregido todos los incumplimientos de políticas.

Rescisión de la cuenta

- Si se cierra su cuenta de desarrollador, se eliminarán de Google Play todas las aplicaciones de su catálogo, y usted ya no podrá publicar aplicaciones 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 al cierre de su cuenta de Play Console.
- Dado que las aplicaciones de la cuenta cerrada se eliminan, los usuarios no podrán ver la ficha de Play Store de sus aplicaciones ni su perfil de desarrollador.
- Los usuarios actuales no podrán realizar compras directas desde las aplicaciones ni utilizar funciones de facturación integrada en sus aplicaciones.

Nota: También se cerrará cualquier cuenta nueva que intente abrir (sin que se reembolse la tarifa de registro del desarrollador), así que no intente registrarse para obtener una nueva cuenta de Play Console mientras se encuentre cerrada una de sus 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. Para evitar casos de abuso, cerramos las cuentas que están inactivas o que no se utilizan ni tienen interacciones frecuentes, por ejemplo, para publicar y actualizar aplicaciones, acceder a estadísticas o administrar fichas de Play Store.

El cierre de una cuenta inactiva hará que la cuenta se cierre. Esto significa que ya no podrá acceder a informes, estadísticas ni otra información dentro de Play Console a menos que se restablezca su cuenta inactiva. No se le devolverá el valor de la tarifa de registro, dado que no es reembolsable. Antes de cerrar su cuenta 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 realizar publicaciones en Google Play.

Cómo administrar y denunciar incumplimientos de políticas

Apelación a una acción de aplicación de políticas

Restableceremos la app si decidimos que se cometió un error y que esta 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 o haz clic aquí 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

Para garantizar la seguridad de nuestro dinámico ecosistema de aplicaciones, Google Play exige que todos los desarrolladores completen los requisitos de Play Console, incluidos los perfiles que se vinculen con su cuenta de desarrollador de Play Console. Se mostrará información verificada en Google Play para ayudar a los usuarios a forjar confianza y seguridad con relación a los desarrolladores. Obtenga más detalles sobre la información que se muestra en Google Play.

Google Play ofrece dos tipos de cuentas de desarrollador: Personal y Organización. Para lograr una experiencia de integración fluida, es fundamental seleccionar el tipo correcto de cuenta de desarrollador y completar las verificaciones necesarias. Obtenga más información para elegir un tipo de cuenta de desarrollador.

Cuando creen su cuenta de Play Console, los desarrolladores deberán registrarse como Organización si ofrecen los siguientes servicios:

- Productos y servicios financieros, incluidos, sin limitaciones, servicios bancarios, préstamos, operaciones bursátiles, fondos de inversión, exchanges de criptomonedas y billeteras de software de criptomonedas; obtenga más información acerca de la política sobre Servicios Financieros

- Aplicaciones de salud, como aplicaciones Médicas y de Investigación con Seres Humanos; obtenga más información sobre las categorías de aplicaciones de Salud
- Aplicaciones aprobadas para usar la clase VpnService ; obtenga más información sobre la política de Servicio de VPN
- Aplicaciones gubernamentales, incluidas aquellas desarrolladas por un organismo gubernamental o en nombre de él

Una vez que seleccione un tipo de cuenta, debe hacer lo siguiente:

- Proporcionar con precisión la información de su cuenta de desarrollador, incluidos los detalles que se indican a continuación:
  - Dirección y nombre legales
  - Número DUNS si se registra como una organización
  - Dirección de correo electrónico y número de teléfono de contacto
  - Dirección de correo electrónico y número de teléfono del desarrollador como se muestran en Google Play cuando corresponda
  - Formas de pago cuando corresponda
  - Perfil de pagos de Google vinculado a su cuenta de desarrollador
- Si se registra como una organización, asegurarse de que la información de su cuenta de desarrollador esté actualizada y sea coherente con los detalles almacenados en su perfil de Dun & Bradstreet

Antes de enviar su aplicación, debe hacer lo siguiente:

- Proporcionar con exactitud toda la información y los metadatos de su aplicación
- 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 Google Play revise la aplicación (específicamente, las credenciales de acceso, el código QR, etcétera)

Como siempre, debe asegurarse de que su aplicación proporcione una experiencia del usuario estable, interesante y responsiva; verifique que todos los elementos de su aplicación, incluidos los servicios de estadísticas, las redes de publicidad y los SDKs 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