Google Developer Policy - April 16, 2020

Vamos construir a fonte mais fidedigna do mundo de aplicações e jogos

A sua inovação é o que impulsiona o nosso sucesso partilhado, mas isso implica responsabilidade. Estas Políticas do Programa para programadores, juntamente com o Contrato de Distribuição para Programadores, garantem que, juntos, possamos continuar a fornecer as apps mais inovadoras e fidedignas do mundo a mais de mil milhões de pessoas através do Google Play. Explore as nossas políticas abaixo ou numa vista de impressão.

Conteúdo restrito

Pessoas do mundo inteiro utilizam o Google Play todos os dias para aceder a apps e jogos. Antes de enviar uma app, tenha em consideração se esta é adequada para o Google Play e se está em conformidade com as leis locais.

Negligência infantil

As apps que incluem conteúdo com sexualização de menores estão sujeitas a remoção imediata da Google Store. Não são permitidas apps que sejam atrativas para crianças e que contenham temas para adultos.

Se tivermos conhecimento de conteúdo com imagens de abuso sexual infantil, iremos denunciá-lo às autoridades competentes e eliminaremos as Contas Google das pessoas envolvidas na respetiva distribuição.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Conteúdos de natureza sexual

Não são permitidas apps que incluam ou promovam conteúdos de natureza sexual, como pornografia ou quaisquer conteúdos ou serviços que pretendam ser sexualmente gratificantes. Pode ser permitido conteúdo com nudez se o objetivo principal for educativo, documental, científico ou artístico, e não for despropositado.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Representações de nudez em que o sujeito está nu ou minimamente vestido e em que o vestuário não seja aceitável num contexto público adequado.
- Representações, animações ou ilustrações de atos sexuais ou de poses com conotação sexual.
- Conteúdo que represente brinquedos e fetiches sexuais.
- Conteúdo que seja provocador ou obsceno.
- Conteúdo que represente, descreva ou incentive a bestialidade.
- Apps que promovam entretenimento associado a sexo, serviços de acompanhantes ou outros serviços que possam ser interpretados como disponibilização de atos sexuais em troca de compensação.

Incitação ao ódio

Não são permitidas apps que promovam violência ou incitem ao ódio contra pessoas ou grupos de pessoas com base na raça, etnia, religião, deficiência, idade, nacionalidade, estatuto de veterano, orientação sexual, género, identidade de género ou qualquer outra caraterística associada a discriminação ou a marginalização sistémica.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Compilações de declarações destinadas a provar que um grupo protegido é desumano, inferior ou passível de ser alvo de ódio.
- Aplicações com teorias acerca de um grupo protegido com caraterísticas negativas (por exemplo, malicioso, corrupto, demoníaco, etc.) ou que declare de forma explícita ou implícita que o grupo é uma ameaça.
- Conteúdo ou discurso que tente encorajar outros a acreditar que as pessoas devem ser odiadas ou discriminadas por serem membros de um grupo protegido.

Violência

Não são permitidas apps que representem ou promovam violência gratuita ou outras atividades perigosas.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Representações ou descrições gráficas de violência realista ou de ameaças de violência contra pessoas ou animais.
- Apps que promovam lesões autoinfligidas, suicídio, distúrbios alimentares, jogos de asfixia ou outros atos suscetíveis de causarem lesões graves ou a morte.

Conteúdo terrorista

A Google não permite que organizações terroristas publiquem aplicações no Google Play seja para que fim for, incluindo recrutamento.

Também não são permitidas aplicações com conteúdo relacionado com terrorismo, nomeadamente conteúdo que promova atos terroristas, incite à violência ou festeje ataques terroristas. Se publicar conteúdos relacionados com terrorismo com um objetivo educativo, documental, científico ou artístico, tenha o cuidado de fornecer informações suficientes para que os utilizadores compreendam o contexto.

Acontecimentos sensíveis

Não são permitidas apps que não revelem sensibilidade razoável ou procurem tirar partido de desastres naturais, atrocidades, conflitos, morte ou outros eventos trágicos.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- A falta de sensibilidade relativamente à morte de uma pessoa real ou de um grupo de pessoas devido a suicídio, overdose, causas naturais, etc.
- Negar um evento trágico importante.
- Aparentar lucrar com um evento trágico sem qualquer vantagem percetível para as vítimas.

Bullying e assédio

Não são permitidas apps que incluam ou promovam ameaças, assédio ou bullying.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Bullying a vítimas de conflitos internacionais ou religiosos.
- Conteúdo que vise explorar outras pessoas, incluindo a extorsão, a chantagem, etc.
- Publicar conteúdo para humilhar alguém publicamente.
- Assediar as vítimas, ou os respetivos amigos e familiares, de um evento trágico.

Produtos perigosos

Não são permitidas apps que promovam a venda de explosivos, armas de fogo, munições ou determinados acessórios para armas de fogo.

- Os acessórios restritos incluem todos aqueles que permitem simular disparos automáticos numa arma de fogo ou converter uma arma de fogo numa arma de disparo automático (por exemplo, coronhas de amortecimento, disparadores de gatilho, reguladores de disparo automático de encaixe, conjuntos de conversão) e cartuchos ou cintos com mais de 30 balas.

Não são permitidas aplicações que disponibilizem instruções para o fabrico de explosivos, de armas de fogo, de munições, de acessórios para armas de fogo restritos ou de outras armas. Isto inclui instruções sobre como converter uma arma de fogo numa arma automática ou com capacidades de disparo automático simuladas.

Marijuana

Não são permitidas apps que promovam a venda de marijuana ou produtos de marijuana, independentemente da sua legalidade.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Permitir que os utilizadores encomendem marijuana através de uma funcionalidade de compras na app.
- Auxiliar os utilizadores na entrega ou recolha de marijuana.
- Facilitar a venda de produtos com THC.

Tabaco e álcool

Não são permitidas apps que promovam a venda de tabaco (incluindo cigarros eletrónicos) ou que incentivem o uso irresponsável de álcool ou tabaco.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Descrever ou encorajar o uso ou a venda de álcool ou tabaco a menores.
- Afirmar que o consumo de tabaco pode melhorar a vida social, sexual, profissional, intelectual ou atlética.
- Promover o consumo excessivo de álcool de forma favorável, incluindo a representação favorável do seu consumo excessivo, exagerado ou como forma de competição.

Serviços financeiros

Não são permitidas apps que exponham os utilizadores a produtos ou serviços financeiros enganadores ou prejudiciais.

Para efeitos da presente política, a Google define os produtos e os serviços financeiros como aqueles produtos e serviços relacionados com a gestão e o investimento de dinheiro e criptomoedas, incluindo aconselhamento personalizado.

Se a sua app contiver ou promover produtos e serviços financeiros, tem de agir em conformidade com os regulamentos estatais e locais de qualquer região ou país a que a sua app se destina. Por exemplo, inclua divulgações específicas requeridas pela legislação local.

Opções binárias

Não são permitidas apps que possibilitem aos utilizadores a negociação de opções binárias.

Criptomoedas

Não são permitidas apps para a mineração de criptomoedas em dispositivos. São permitidas apps que efetuam a gestão remota da mineração de criptomoedas.

Empréstimos pessoais

A Google define empréstimos pessoais como um empréstimo não recorrente de dinheiro por parte de uma pessoa, organização ou entidade a um consumidor individual, não destinado ao financiamento para aquisição de um ativo fixo ou para despesas de educação. Os consumidores de empréstimos pessoais necessitam de informações acerca da qualidade, das condições, das taxas, dos riscos e das vantagens dos produtos relacionados com empréstimos, para poderem tomar decisões informadas sobre contrair ou não o empréstimo.

> Exemplos: empréstimos pessoais, empréstimos de ordenado, empréstimos coletivos, empréstimos com garantia automóvel.
> Não incluído: hipotecas, crédito automóvel, empréstimos para estudantes, linhas de crédito rotativo (como cartões de crédito, linhas de crédito pessoal).

As apps para empréstimos pessoais têm de divulgar as seguintes informações nos metadados da app:

> O período mínimo e máximo para o reembolso.
> A Taxa Anual Efetiva (TAE) máxima, que geralmente inclui a taxa de juro, bem como taxas e outros custos durante um ano, ou qualquer outra taxa semelhante calculada em conformidade com a legislação local.
> Um exemplo representativo do custo total do empréstimo, incluindo todas as taxas aplicáveis.

Não são permitidas apps que promovam empréstimos pessoais que requeiram o pagamento na totalidade em 60 dias ou menos a contar da data de emissão do empréstimo (denominados "empréstimos pessoais a curto prazo"). A presente política aplica-se às apps que oferecem empréstimos diretamente, geram potenciais clientes e ligam os consumidores a credores de terceiros.

Empréstimos pessoais associados a uma TAE elevada

Nos Estados Unidos, não são permitidas apps para empréstimos pessoais em que a Taxa Anual Efetiva (TAE) seja igual ou superior a 36%. As apps para empréstimos pessoais nos Estados Unidos têm de apresentar a respetiva TAE máxima, calculada em conformidade com a Lei da Verdade em Empréstimos (TILA).

A presente política aplica-se às apps que oferecem empréstimos diretamente, geram potenciais clientes e ligam os consumidores a credores de terceiros.

Jogos de azar

Permitimos conteúdo, serviços e anúncios que facilitem jogos de azar online, desde que cumpram determinados requisitos. Também permitimos apps de daily fantasy sports que cumpram determinados requisitos.

Apps de jogos de azar

(Atualmente permitidas apenas no Reino Unido, na Irlanda e em França)

Permitimos conteúdos e serviços que facilitem jogos de azar online, desde que cumpram os seguintes requisitos:

- O programador tem de concluir o processo de candidatura com êxito para distribuir a app no Google Play;
- A app tem de cumprir todas as normas da indústria e as leis aplicáveis em todos os países nos quais é distribuída;
- O programador precisa de uma licença de jogos de azar válida para todos os países nos quais a aplicação é distribuída;
- A aplicação tem de impedir os utilizadores menores de idade de jogarem na aplicação;
- A app tem de impedir a utilização nos países não abrangidos pela licença de jogos de azar fornecida pelo programador;
- A app NÃO pode ser adquirida como uma app paga no Google Play, nem utilizar a Faturação em apps do Google Play;
- A transferência e a instalação da app têm de ser gratuitas a partir da Play Store;
- A app tem de incluir a classificação AA (Apenas adultos) ou equivalente da IARC; e
- A app e a ficha da app têm de apresentar claramente informações acerca de jogos de azar responsáveis.

Para todas as outras localizações, não são permitidos conteúdos ou serviços que promovam jogos de azar online, incluindo, entre outros, casinos online, apostas desportivas, lotarias e jogos de perícia que ofereçam prémios em dinheiro ou noutro valor real.

Anúncios de jogos de azar em apps distribuídas no Google Play

Permitimos anúncios que facilitem jogos de azar online, desde que cumpram os seguintes requisitos:

- A app e o anúncio (incluindo os anunciantes de jogos de azar) têm de cumprir todas as normas da indústria e as leis aplicáveis em todas as localizações nas quais o anúncio de jogos de azar é apresentado;
- O anúncio tem de cumprir os requisitos de licenciamento locais para todos os serviços e produtos relacionados com jogos de azar que estão a ser promovidos;
- A aplicação não deve apresentar um anúncio de jogos de azar a indivíduos com menos de 18 anos;
- A aplicação não pode estar inscrita no programa Concebido para Famílias;
- A aplicação não se pode destinar a indivíduos com menos de 18 anos;
- O anúncio tem de apresentar claramente informações acerca de jogos de azar responsáveis na página de destino, na própria ficha da aplicação anunciada ou na aplicação; e
- A app que está a apresentar um anúncio de jogos de azar não pode ser uma app de jogos de azar simulados (um jogo de entretenimento sem jogos de azar a dinheiro real).

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

A app "KIDS 123" com um anúncio a promover serviços de jogos de azar.

Apps de daily fantasy sports (DFS)

São permitidas apps de daily fantasy sports (DFS), desde que cumpram os seguintes requisitos:

A app só pode permitir o acesso e ser distribuída nos Estados Unidos; as apps de DFS destinadas a jurisdições fora dos EUA têm de definir a elegibilidade através do processo relativo a Apps de jogos de azar a dinheiro real;
O programador tem de concluir com êxito o processo de candidatura a DFS e ser aceite para distribuir a app no Google Play.
A app tem de cumprir todas as normas da indústria e as leis aplicáveis em qualquer estado ou território dos EUA em que é distribuída;
O programador precisa de uma licença válida para cada estado ou território dos EUA em que seja obrigatória uma licença para aplicações diárias de desportos fictícios;
A aplicação tem de impedir os utilizadores menores de participarem em transações monetárias na aplicação;
A aplicação tem de impedir a utilização em estados ou territórios dos EUA para os quais o programador não possui uma licença obrigatória para aplicações diárias de desportos fictícios;
A app tem de impedir a utilização em estados ou territórios dos EUA onde as apps de daily fantasy sports não são legais;
A app NÃO pode ser adquirida como uma app paga no Google Play, nem utilizar a Faturação em apps do Google Play;
A transferência e a instalação da app têm de ser gratuitas a partir da Play Store;
A app tem de incluir a classificação AA (Apenas adultos) ou equivalente da IARC; e
A app e a ficha da app têm de apresentar claramente informações acerca de jogos de azar responsáveis.

Atividades ilegais

Não são permitidas apps que facilitem ou promovam atividades ilegais.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Facilitar a venda ou a compra de drogas ilegais ou de medicamentos sem receita.
Descrever ou encorajar a utilização ou a venda de drogas, de álcool ou de tabaco por menores.
Instruções para plantação ou fabrico de drogas ilegais.

Conteúdo gerado pelo utilizador

Conteúdo gerado pelo utilizador (UGC) refere-se a conteúdo que resulta da contribuição de utilizadores para uma app e que está visível ou acessível, pelo menos, a um subconjunto de utilizadores da app. Conteúdo censurável refere-se a conteúdo que viola as nossas políticas.

As aplicações que incluam ou apresentem UGC têm de:

- exigir que os utilizadores aceitem os termos de utilização e/ou a política do utilizador da aplicação para poderem criar ou carregar UGC;
- definir, em consonância com o espírito das Políticas do Programa para Programadores do Google Play, UGC que seja censurável e proibir esse UGC através dos termos de utilização e/ou da política do utilizador da aplicação;
- Implementar uma moderação de UGC sólida, eficaz e contínua, na medida do que for razoável e consistente com o(s) tipo(s) de UGC alojado(s) pela app;
- Proporcionar um sistema integrado na app intuitivo para denúncia e remoção de UGC censurável;
    - No caso de apps de stream em direto, o UGC problemático tem de ser removido o mais aproximadamente possível do tempo real;
- Remover ou bloquear utilizadores ofensivos que violem os termos de utilização e/ou a política do utilizador da app;
- Fornecer salvaguardas para evitar a rentabilização na app ao encorajar um comportamento censurável por parte dos utilizadores.

As apps cujo principal objetivo consiste em apresentar UGC censurável serão removidas do Google Play. De igual modo, as apps que acabem por ser utilizadas, essencialmente, para alojar UGC censurável ou que fiquem conhecidas entre os utilizadores como sendo um local onde esse tipo de conteúdo prolifera, serão também removidas do Google Play.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Promover conteúdo sexualmente explícito gerado pelo utilizador, incluindo a implementação de funcionalidades pagas que encorajem principalmente a partilha de conteúdo censurável.
- Apps com conteúdo gerado pelo utilizador (UGC) que não tenham salvaguardas suficientes contra ameaças, assédio ou bullying, especialmente em relação a menores.
- Publicações, comentários ou fotos numa app que se destinem principalmente a assediar ou a discriminar outra pessoa para abuso, ataque malicioso ou ridicularização.
- Apps que ignoram constantemente as reclamações dos utilizadores relativas a conteúdo censurável.

Substâncias não aprovadas

O Google Play não permite apps que promovam ou vendam substâncias não aprovadas, independentemente de quaisquer queixas relacionadas com a respetiva legalidade. Exemplos:

Todos os artigos desta lista não exaustiva de produtos farmacêuticos e suplementos proibidos
Produtos que contenham éfedra.
Produtos que contenham gonadotrofina coriónica humana (hCG) relacionados com perda ou controlo de peso, ou quando promovidos em conjunto com esteroides anabolizantes.
Suplementos fitoterápicos e dietéticos com ingredientes ativos farmacêuticos ou perigosos.
Afirmações falsas ou enganadoras sobre saúde, incluindo a afirmação de que um produto é tão eficaz como medicamentos sujeitos a receita médica ou substâncias regulamentadas.
Produtos não aprovados pelas entidades oficiais comercializados de uma forma que insinue que são seguros ou eficazes para utilização na prevenção, na cura ou no tratamento de determinada doença ou determinado problema de saúde.
Produtos que tenham sido sujeitos a qualquer ação ou notificação governamental ou regulamentar.
Produtos com nomes que possam causar confusão por serem demasiado semelhantes a um produto farmacêutico, a uma substância regulamentada ou a um suplemento não aprovado.

Para obter informações adicionais sobre fármacos e suplementos não aprovados ou enganadores monitorizados pela Google, visite www.legitscript.com.

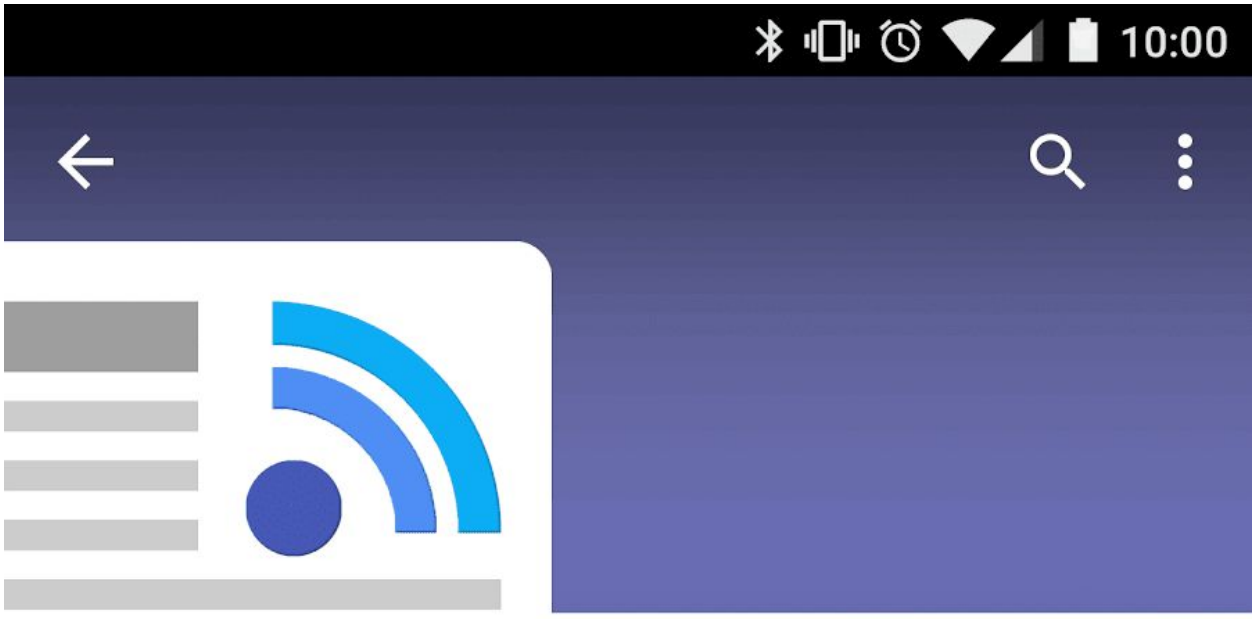
Roubo de identidade e propriedade intelectual

Quando os programadores copiam o trabalho de alguém ou enganam os utilizadores, isso prejudica os utilizadores e a comunidade de programadores. Não utilize o trabalho de outras pessoas de forma enganadora ou desleal.

Roubo de identidade

Não são permitidas apps que utilizem o nome, o logótipo, o título ou a marca de outra entidade ou app de forma que possa enganar os utilizadores. Não tente insinuar um patrocínio ou uma relação com outra entidade onde tal não exista. O roubo de identidade pode ocorrer mesmo quando não haja intenção de enganar, pelo que deve ter cuidado ao mencionar quaisquer marcas que não lhe pertençam. Isto aplica-se mesmo se a marca ainda não estiver presente no Google Play.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Programadores que sugerem falsamente afiliação com outra entidade:



RSS News Aggregator

Google Developer

Everyone

INSTALL

100 MILLION
Downloads

4.1
161,251

News & Magazines

Similar

All the best news, aggregated in one spot!

WHAT'S NEW

- Push notifications now enabled.
- Customize your feed based on your current location!

① O nome de programador listado para esta aplicação sugere uma relação oficial com a Google, embora tal relação não exista.
Ícones e títulos de aplicação que sejam tão semelhantes aos de produtos ou de serviços existentes que podem enganar os utilizadores:

✓	 Google Maps	 Google+	 YouTube	 Twitter
✗	 Google Maps Navigator	 Google+ Sharify	 YouTube Aggregator	 TwitterPro

Aplicações que reivindicam falsamente ser a aplicação oficial de uma entidade estabelecida. Títulos como "Justin Bieber Oficial" não são permitidos sem as autorizações ou os direitos necessários.
Apps que violam as Diretrizes da imagem corporativa do Android.

Propriedade intelectual

Não são permitidas contas de programador ou apps que infrinjam os direitos de propriedade intelectual de terceiros (incluindo marcas comerciais, direitos de autor, patentes, segredos comerciais e outros direitos de propriedade). Também não são permitidas apps que encorajem ou induzam à infração de direitos de propriedade intelectual.

Responderemos a avisos claros de alegada violação de direitos de autor. Para mais informações ou para apresentar um pedido DMCA, visite os nossos procedimentos de direitos de autor.

Para apresentar uma acusação relativamente à venda ou à promoção da venda de produtos contrafeitos numa app, envie um aviso de contrafação.

Se for proprietário de uma marca comercial e considerar que há uma app no Google Play que infringe os seus direitos de marca comercial, recomendamos que contacte diretamente o programador para resolver a sua preocupação. Se não conseguir chegar a uma resolução em conjunto com o programador, envie uma reclamação por violação da marca comercial através deste formulário.

Se possuir documentação escrita que comprove a sua autorização para utilizar a propriedade intelectual de terceiros na sua app ou Ficha da loja (por exemplo, nomes, logótipos e recursos

gráficos de marcas), contacte a equipa do Google Play antes do envio para garantir que a sua app não é rejeitada devido a uma violação de propriedade intelectual.

Utilização não autorizada de conteúdo protegido por direitos de autor

Não são permitidas apps que infrinjam direitos de autor. Modificar conteúdo protegido por direitos de autor pode conduzir também a uma violação. Os programadores podem ter de fornecer comprovativos dos seus direitos para utilizarem conteúdos protegidos por direitos de autor.

Tenha cuidado ao utilizar conteúdo protegido por direitos de autor para demonstrar a funcionalidade da sua app. Em geral, a abordagem mais segura é criar algo original.

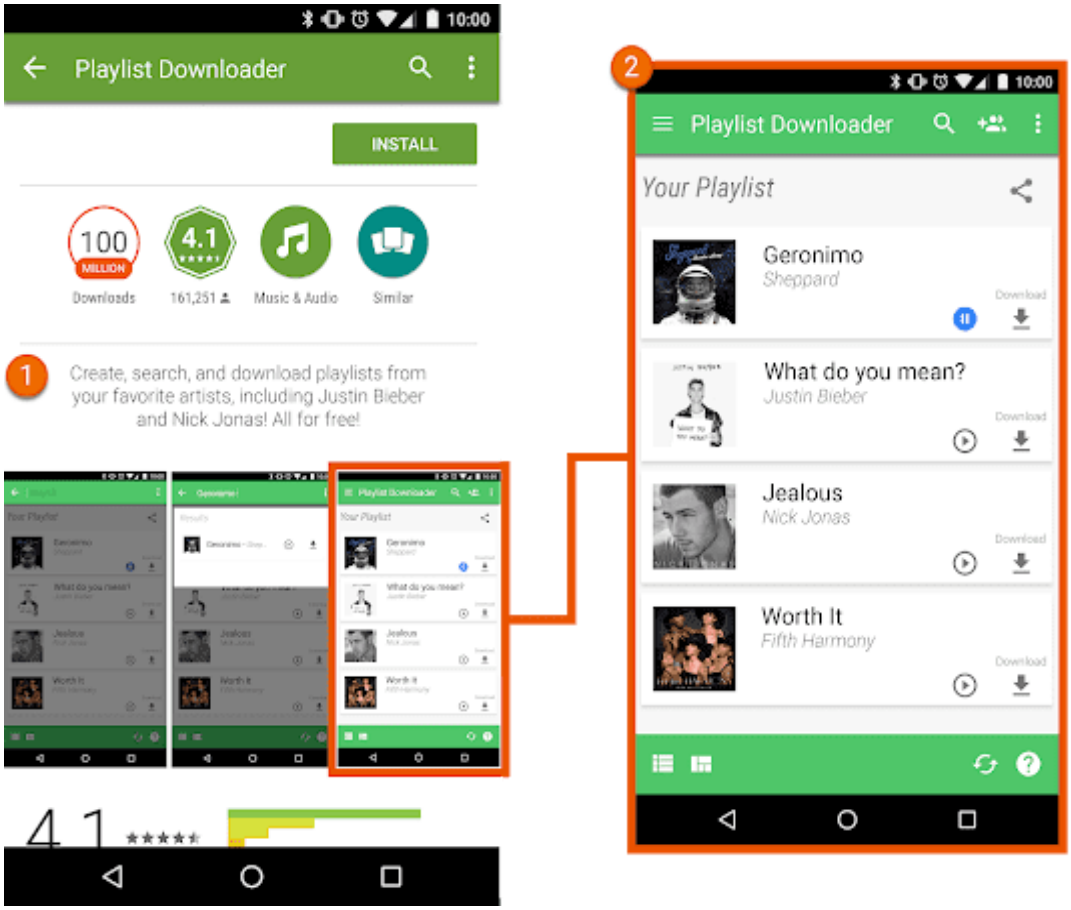
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Capas de álbuns de música, de videojogos e de livros.
- Imagens de marketing de filmes, de televisão ou de videojogos.
- Ilustrações ou imagens de livros de banda desenhada, de desenhos animados, de vídeos de música ou de televisão.
- Logótipos de equipas desportivas profissionais e universitárias.
- Fotos retiradas de contas de redes sociais de figuras públicas.
- Imagens profissionais de figuras públicas.
- Reproduções ou "arte dos fãs" indistinguíveis do trabalho original protegidas por direitos de autor.
- Aplicações com mesas de som que reproduzem clipes de áudio de conteúdo protegido por direitos de autor.
- Reproduções ou traduções completas de livros que não sejam de domínio público.

Encorajamento à violação de direitos de autor

Não são permitidas apps que induzam ou encorajem a violação de direitos de autor. Antes de publicar a sua app, verifique se esta está de alguma forma a encorajar a violação de direitos de autor e obtenha aconselhamento jurídico se necessário.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Apps de streaming que permitam aos utilizadores transferir uma cópia local de conteúdo protegido por direitos de autor sem autorização.
- Aplicações que encorajam os utilizadores a transmitir em fluxo contínuo e a transferir trabalhos protegidos por direitos de autor, incluindo música e vídeo, em violação da lei de direitos de autor aplicável:



① A descrição nesta ficha da app encoraja os utilizadores a transferir conteúdo protegido por direitos de autor sem autorização.
② A captura de ecrã na ficha da app encoraja os utilizadores a transferir conteúdo protegido por direitos de autor sem autorização.

Violação de marca comercial

Não são permitidas apps que violem marcas comerciais de terceiros. Uma marca comercial é uma palavra, um símbolo ou uma combinação de ambos que identifica a origem de um bem ou de um serviço. Uma vez adquirida, uma marca comercial confere ao proprietário direitos exclusivos para a respetiva utilização no que respeita a determinados bens ou serviços.

A violação de marca comercial é a utilização indevida ou não autorizada de uma marca comercial idêntica ou semelhante de tal forma que pode provocar confusão em relação à origem desse produto. Se a sua app utiliza marcas comerciais de terceiros de forma a que seja provável que cause confusão, pode ser suspensa.

Contrafação

Não são permitidas apps que vendam ou promovam a venda de produtos contrafeitos. Os artigos contrafeitos contêm uma marca comercial ou um logótipo idêntico ou quase indistinto da marca comercial de outra empresa. Estes produtos imitam as caraterísticas da marca do produto, numa tentativa de se fazerem passar por um produto genuíno do proprietário da marca.

Privacidade, segurança e logro

Estamos empenhados em proteger a privacidade do utilizador e em fornecer um ambiente seguro e protegido para os nossos utilizadores. São estritamente proibidas apps enganadoras, maliciosas ou que abusem ou utilizem indevidamente qualquer rede, dispositivo ou dados pessoais.

Dados do utilizador

Tem de ser transparente no modo como processa os dados do utilizador (por exemplo, as informações recolhidas sobre ou de um utilizador, incluindo as informações do dispositivo). Isso significa divulgar o acesso, a recolha, a utilização e a partilha dos dados da sua app e limitar a utilização dos dados às finalidades divulgadas. Além disso, se a sua app processar dados pessoais ou confidenciais do utilizador, consulte os requisitos adicionais na secção "Informações pessoais e confidenciais" abaixo. Estes requisitos do Google Play são adicionais a quaisquer requisitos estabelecidos por leis de privacidade e proteção de dados aplicáveis.

Informações pessoais e confidenciais

Os dados pessoais e confidenciais do utilizador incluem, entre outros, informações de identificação pessoal, informações de pagamento e financeiras, informações de autenticação, agenda telefónica, contactos, localização do dispositivo, SMS e dados relacionados com chamadas, microfone, câmara, bem como outros dados de utilização ou confidenciais do dispositivo. Se a sua app processar dados do utilizador confidenciais, tem de:

- Limitar o acesso, a recolha, a utilização e a partilha de dados pessoais ou confidenciais adquiridos pela app a finalidades relacionadas diretamente com o fornecimento e o melhoramento das funcionalidades da app (por exemplo, a funcionalidade antecipada do utilizador documentada e promovida na descrição da app na Play Store). As apps que estendam a utilização destes dados para publicar anúncios têm de agir em conformidade com a nossa Política de Anúncios.
- Publicar uma política de privacidade no campo designado na Play Console e na própria app. A política de privacidade deve, em conjunto com quaisquer divulgações na app, divulgar de modo abrangente a forma como a app recolhe, utiliza, partilha e acede aos dados do utilizador. A política de privacidade tem de divulgar os tipos de dados

pessoais ou confidenciais que a app utiliza, recolhe ou aos quais acede e com que tipos de partes são partilhados os dados pessoais ou confidenciais do utilizador.
Processar todos os dados pessoais ou confidenciais do utilizador de forma segura, incluindo a transmissão através de criptografia moderna (por exemplo, por HTTPS).
Utilizar um pedido de autorizações de tempo de execução sempre que estiver disponível, antes de aceder a dados bloqueados por autorizações do Android.
Não vender dados pessoais ou confidenciais do utilizador.

Divulgação proeminente e requisito de consentimento

Nos casos em que os utilizadores possam não considerar, de forma razoável, conforme determinado pelo Play na discrição exclusiva, que os respetivos dados pessoais ou confidenciais são necessários para fornecer ou melhorar as funcionalidades ou os serviços em conformidade com a política da app, tem de cumprir os seguintes requisitos:

Tem de fornecer uma divulgação na app do acesso, recolha, utilização e partilha de dados. A divulgação na app:

Tem de estar dentro da própria app e não apenas na descrição da app ou num Website;
Deve ser apresentada durante a utilização normal da app e não deve requerer que o utilizador navegue até um menu ou às definições;
Tem de descrever os dados a aceder ou a recolher;
Tem de explicar como é que os dados serão utilizados e/ou partilhados;
Não pode ser colocada apenas numa política de privacidade ou nos termos de utilização; e
Não pode ser incluída com outras divulgações não relacionadas com a recolha de dados pessoais ou confidenciais.

A divulgação na app tem de acompanhar e preceder de imediato um pedido de consentimento do utilizador e, quando disponível, uma autorização de tempo de execução associada. Não pode aceder ou recolher quaisquer dados pessoais ou confidenciais até haver consentimento do utilizador. O pedido de autorização da aplicação:

Tem de apresentar a caixa de diálogo de consentimento de forma clara e inequívoca;
Tem de requerer uma ação afirmativa do utilizador (por exemplo, tocar para aceitar, selecionar uma caixa de verificação);
Não deve interpretar a navegação para fora da divulgação (incluindo tocar para sair ou premir o botão Anterior ou página inicial) como consentimento; e
Não deve utilizar mensagens com opção para ignorar automaticamente ou com validade.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Uma app que aceda ao inventário de apps instaladas de um utilizador e não trate estes dados como dados pessoais ou confidenciais do utilizador sujeitos aos requisitos da política de privacidade, da transmissão segura e da divulgação clara.
Uma app que aceda aos dados do telemóvel ou da agenda telefónica de um utilizador e não trate estes dados como dados pessoais ou confidenciais do utilizador sujeitos aos requisitos da política de privacidade, da transmissão segura e da divulgação clara.
Uma app que grave o ecrã do utilizador e não trate estes dados como dados pessoais ou confidenciais sujeitos a esta política.
Uma app que recolha a localização do dispositivo e não divulgue a respetiva utilização de modo abrangente em conformidade com os requisitos acima.

Restrições de acesso a dados confidenciais

Para além dos requisitos acima, a tabela abaixo descreve os requisitos para atividades específicas.

Atividade	Requisito
A sua app processa informações financeiras ou de pagamento, ou números de identificação governamental	A sua aplicação nunca pode divulgar publicamente quaisquer dados pessoais ou confidenciais do utilizador relacionados com atividades financeiras, ou de pagamento ou quaisquer números de identificação governamental.
A sua app processa informações de contacto ou da agenda telefónica que não são públicas	Não permitimos a publicação ou a divulgação não autorizada de contactos não públicos das pessoas.
A sua app inclui uma funcionalidade antivírus ou de segurança, por exemplo, antivírus, proteção contra software malicioso ou funcionalidades relacionadas com a segurança	A sua app tem de publicar uma política de privacidade que, juntamente com quaisquer divulgações na app, explique quais são os dados do utilizador que a app recolhe e transmite, como são utilizados e com quem são partilhados.

EU-U.S. Privacy Shield (Escudo de Proteção da Privacidade UE-EUA)

Se aceder, utilizar ou processar informações pessoais disponibilizadas pela Google que identifiquem, direta ou indiretamente, uma pessoa e que tenham origem na União Europeia ou Suíça ("Informações pessoais da UE"), deve:

Cumprir todas as leis, diretivas, normas e regras aplicáveis em matéria de privacidade, segurança de dados e proteção de dados;
Aceder, utilizar ou processar as Informações pessoais da UE apenas para fins compatíveis com a autorização obtida junto da pessoa a quem as referidas informações dizem respeito;

Implementar medidas organizacionais e técnicas adequadas para proteger as Informações pessoais da UE contra perda, utilização indevida e acesso, divulgação, alteração e destruição não autorizada ou ilegal; e
Assegurar o mesmo nível de proteção exigido pelos Princípios do Privacy Shield (Escudo de Proteção da Privacidade).

Deve monitorizar regularmente a conformidade com estas condições. Se, num dado momento, não puder agir em conformidade com estas condições (ou se houver um risco significativo de incumprimento das mesmas), deve comunicar-nos imediatamente essa informação por email para data-protection-office@google.com e interromper de imediato o processamento das Informações pessoais da UE ou tomar as medidas razoáveis e adequadas para repor um nível de proteção adequado.

Autorizações

Os pedidos de autorização devem ser compreensíveis pelos utilizadores. Apenas pode solicitar as autorizações necessárias para implementar as funcionalidades ou os serviços atuais na sua app que sejam promovidos na sua Ficha da loja da Play Store. Não pode utilizar autorizações que dão acesso aos dados do utilizador ou do dispositivo para funcionalidades ou finalidades não divulgadas, não implementadas ou não autorizadas. Nunca pode vender os dados pessoais ou confidenciais acedidos através de autorizações.

Solicite autorizações para aceder aos dados em contexto (através da autenticação progressiva) de forma que os utilizadores compreendam os motivos pelos quais a sua aplicação está a solicitar a autorização. Utilize os dados apenas para as finalidades autorizadas pelo utilizador. Se mais tarde pretender utilizar os dados para outras finalidades, tem de perguntar aos utilizadores e assegurar que concordam com as utilizações adicionais.

Autorizações restritas

Para além do exposto acima, as autorizações restritas são autorizações designadas como Assinatura ou Perigosas na nossa documentação para programadores e estão sujeitas aos seguintes requisitos e restrições adicionais:

Os dados confidenciais do utilizador ou do dispositivo acedidos através de Autorizações restritas só poderão ser transferidos a terceiros se tal for necessário para fornecer ou melhorar as funcionalidades ou os serviços atuais na app a partir da qual os dados foram recolhidos. Também poderá transferir os dados consoante o necessário para agir em conformidade com a lei aplicável ou como parte de um processo de fusão, aquisição ou venda de ativos, mediante o aviso legalmente adequado aos utilizadores. Todas as outras transferências ou vendas dos dados dos utilizadores são proibidas.
Respeite as decisões dos utilizadores caso recusem um pedido de Autorização restrita. Os utilizadores não podem ser manipulados nem forçados a consentir qualquer autorização não crítica. Tem de envidar um esforço razoável para integrar os

utilizadores que não concederem acesso a autorizações confidenciais (por exemplo, permitir que um utilizador introduza um número de telefone manualmente caso tenha restringido o acesso aos registos de chamadas).

Determinadas Autorizações restritas poderão estar sujeitas a requisitos adicionais, conforme detalhado abaixo. O objetivo destas restrições é salvaguardar a privacidade do utilizador. Podemos criar exceções limitadas aos requisitos abaixo em casos muito raros em que as apps forneçam uma funcionalidade altamente apelativa ou essencial e não exista um método alternativo disponível para fornecer a funcionalidade. Avaliamos as exceções propostas relativamente ao potencial impacto nos utilizadores ao nível da privacidade ou da segurança.

Autorizações de SMS e de registo de chamadas

As Autorizações de SMS e de registo de chamadas são consideradas dados pessoais e confidenciais do utilizador sujeitos à Política de Informações Pessoais e Confidenciais e às seguintes restrições:

Autorização restrita	**Requisito**
Grupo de autorizações do Registo de chamadas (por exemplo, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Tem de estar ativamente registado como o controlador predefinido do Telemóvel ou do Assistente no dispositivo.
Grupo de autorizações de SMS (por exemplo, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Tem de estar ativamente registado como o controlador predefinido de SMS ou do Assistente no dispositivo.

As apps que não tiverem a capacidade de controlador predefinido de SMS, do Telemóvel ou do Assistente não podem declarar a utilização das autorizações acima no manifesto. Isto inclui o marcador de posição de texto no manifesto. Além disso, as apps têm de estar ativamente registadas como o controlador predefinido de SMS, Telemóvel ou Assistente antes de solicitarem aos utilizadores que aceitem qualquer uma das autorizações acima e têm de parar imediatamente a utilização da autorização quando já não forem o controlador predefinido. As utilizações e as exceções permitidas estão disponíveis nesta página do Centro de Ajuda.

As apps apenas podem utilizar a autorização (e quaisquer dados derivados da autorização) para fornecer a funcionalidade essencial da app aprovada. A funcionalidade essencial é definida como o objetivo principal da app. Isto pode incluir um conjunto de funcionalidades essenciais, que tem de documentar e promover proeminentemente na descrição da app. Sem a funcionalidade essencial, a app é considerada "danificada" ou inutilizável. A transferência, a partilha ou a utilização licenciada destes dados apenas se podem destinar a fornecer funcionalidades ou serviços essenciais na app e a respetiva utilização não pode ser alargada a qualquer outra finalidade (por exemplo, melhorar outras apps ou serviços, publicidade ou

marketing). Não pode utilizar métodos alternativos (incluindo outras autorizações, APIs ou origens de terceiros) para derivar os dados atribuídos às autorizações relacionadas com SMS ou registo de chamadas.

Autorizações de acesso à localização

Atualização de 16 de abril de 2020: compreendemos que a conformidade com a Política de Localização poderá exigir um trabalho significativo de alguns programadores, como tal, concedemos-lhe um prazo alargado para efetuar as alterações necessárias. Para ver os prazos e outras atualizações, visite o nosso Centro de Ajuda.

A localização do dispositivo é considerada como dados pessoais e confidenciais do utilizador sujeitos à Política de Informações Pessoais e Confidenciais e aos seguintes requisitos:

- As apps não podem aceder a dados protegidos por autorizações de acesso à localização (por exemplo, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) depois de esse acesso deixar de ser necessário para fornecer as funcionalidades ou os serviços atuais na sua app.
- Nunca deve solicitar aos utilizadores autorizações de acesso à localização com o único objetivo de anunciar ou obter estatísticas. As apps que estendam a utilização autorizada destes dados para publicar anúncios têm de agir em conformidade com a nossa Política de Anúncios.
- As apps devem solicitar o âmbito mínimo necessário (ou seja, grosso em vez de fino e em primeiro plano em vez de em segundo plano) para fornecer a funcionalidade ou o serviço atual que está a solicitar a localização e os utilizadores devem esperar de forma razoável que a funcionalidade ou o serviço precisa do nível de localização solicitado. Por exemplo, podemos rejeitar apps que solicitem ou acedam à localização em segundo plano sem uma justificação fundamentada.
- A localização em segundo plano apenas pode ser utilizada para oferecer funcionalidades benéficas para o utilizador e relevantes para a funcionalidade essencial da app.

As apps podem aceder à localização através da autorização do serviço em primeiro plano (quando a app apenas tem acesso em primeiro plano, por exemplo, "durante a utilização") se a utilização:

- tiver sido iniciada como uma continuação de uma ação iniciada pelo utilizador na app e for imediatamente terminada após o caso de utilização previsto da ação iniciada pelo utilizador ter sido concluído pela aplicação.

As apps concebidas especificamente para crianças têm de agir em conformidade com a Política do Programa Concebido para Famílias.

Abuso na rede e em dispositivos

Não são permitidas apps que interfiram, perturbem, danifiquem ou acedam de forma não autorizada ao dispositivo do utilizador, outros dispositivos ou computadores, servidores, redes, interfaces de programação de apps (APIs) ou serviços, incluindo, entre outros, outras apps no dispositivo, qualquer serviço Google ou uma rede de operador autorizado.

As apps no Google Play têm de cumprir os requisitos de otimização do sistema Android predefinidos documentados nas Diretrizes de qualidade de apps principais do Google Play.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Apps que bloqueiam ou interferem com outra app ao apresentar anúncios.
- Aplicações de batota em jogos que afetam a jogabilidade de outras aplicações.
- Aplicações que facilitam ou forneçam instruções sobre como piratear serviços, software ou hardware, ou contornar proteções de segurança.
- Apps que acedem ou utilizam um serviço ou uma API de uma forma que viola os respetivos termos de utilização.
- Apps que tentam ignorar a gestão de energia do sistemae que não são elegíveis para a lista de autorizações.
- Apps que facilitam serviços de proxy a terceiros só podem fazê-lo em apps em que seja a finalidade principal centrada no utilizador da app.

Comportamento malicioso

Não permitimos apps que roubem dados, monitorizem ou prejudiquem secretamente os utilizadores, ou que sejam maliciosas de qualquer outra forma.

Uma aplicação distribuída através do Google Play não se pode modificar, substituir ou atualizar a si própria através de qualquer método que não seja o mecanismo de atualização do Google Play. Do mesmo modo, uma aplicação não pode transferir código executável (por exemplo, ficheiros dex, JAR ou .so) proveniente de outras fontes que não o Google Play. Esta restrição não se aplica a código executável numa máquina virtual e que tenha acesso limitado a APIs do Android (como JavaScript num WebView ou navegador).

Apenas podem ser transferidos recursos de apps adicionais (por exemplo, recursos de jogos) se forem necessários para os utilizadores utilizarem a app. Os recursos transferidos têm de estar em conformidade com todas as Políticas do Google Play e, antes de iniciar a transferência, a app deve avisar os utilizadores e divulgar claramente o tamanho da transferência.

As apps de vigilância e spyware comercial são explicitamente proibidas no Google Play. Apenas as apps em conformidade com as políticas concebidas e comercializadas exclusivamente para monitorização parental (incluindo família) ou gestão empresarial podem ser distribuídas na Google Play Store com funcionalidades de controlo e relatório, desde que cumpram totalmente os requisitos descritos abaixo.

Os itens seguintes são expressamente proibidos:

- Vírus, cavalos de Troia, programas maliciosos, spyware ou qualquer outro software malicioso.
- Apps que estabelecem ligação ou facilitam a distribuição ou a instalação de software malicioso.
- Apps ou SDKs que transfiram código executável, como ficheiros dex ou código nativo, proveniente de outras fontes que não o Google Play.
- Apps que introduzem ou exploram vulnerabilidades de segurança.
- Apps que roubam informações de autenticação de um utilizador (como nomes de utilizador ou palavras-passe) ou que imitam outras apps ou Websites para enganar os utilizadores ao levá-los a divulgarem informações pessoais ou de autenticação.
- As apps não podem conter números de telefone, contactos, endereços ou informações de identificação pessoal reais ou não validadas de pessoas ou entidades sem autorização das mesmas.
- Apps que instalam outras apps num dispositivo sem a autorização prévia do utilizador.
- Apps com transferências facilitadas por uma rede de fornecimento de conteúdo (RFC) que não avisam o utilizador nem divulgam o tamanho da transferência antes da mesma.
- Apps concebidas para recolher secretamente dados de utilização do dispositivo, tais como apps de spyware comerciais.

As apps que monitorizam ou rastreiam o comportamento dos utilizadores num dispositivo têm de cumprir os seguintes requisitos:

- As apps não se podem apresentar como uma solução de espionagem ou vigilância secreta.
- As aplicações não podem ocultar nem utilizar o "cloaking" de comportamentos de monitorização nem tentar enganar os utilizadores quanto a esta funcionalidade.
- Apresente aos utilizadores uma notificação persistente e um ícone exclusivo que identifique claramente a app.
- As apps e as fichas das apps no Google Play não podem fornecer meios para ativar ou aceder a funcionalidades que violem estes termos, nomeadamente a ligação a um APK não conforme que esteja alojado fora do Google Play.
- O programador é o único responsável por determinar a legalidade da sua app no local segmentado. As apps que sejam consideradas ilegais nas localizações onde foram publicadas são removidas.

Consulte o nosso Programa de melhoria da segurança das apps para obter mais informações acerca dos problemas de segurança mais recentes sinalizados para os programadores no Google Play. Estão disponíveis detalhes de vulnerabilidades e soluções no link da página de apoio técnico de cada campanha.

Comportamento enganador

Não permitimos apps que tentem enganar os utilizadores ou permitam comportamentos desonestos, incluindo, entre outras, apps consideradas funcionalmente impossíveis. As apps devem fornecer uma divulgação, uma descrição e imagens/vídeos precisos da respetiva funcionalidade em todas as partes dos metadados e funcionar conforme razoavelmente esperado pelo utilizador. Não devem tentar imitar a funcionalidade ou os avisos do sistema operativo ou de outras apps. Quaisquer alterações às definições do dispositivo devem ser efetuadas com conhecimento e consentimento do utilizador, bem como ser facilmente reversíveis pelo mesmo.

Declarações enganadoras

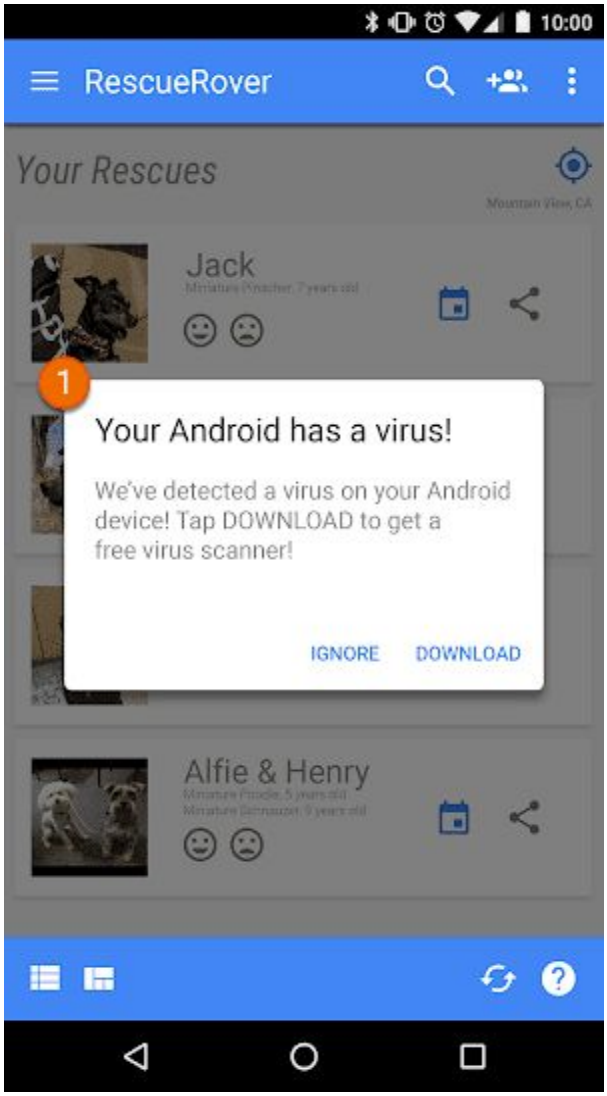
Não permitimos apps que incluam reivindicações ou informações falsas ou que induzam em erro, incluindo na descrição, no título, no ícone e nas capturas de ecrã.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Apps que deturpam ou não descrevem com precisão e claramente as respetivas funcionalidades:
  - Uma app que reivindica ser um jogo de corridas na descrição e nas capturas de ecrã, mas que, na realidade, é um puzzle em blocos com a imagem de um carro.
  - Uma aplicação que reivindica ser uma aplicação de antivírus, mas que contém apenas um guia de texto a explicar como remover vírus.
- Nomes de apps ou programadores que deturpam o seu desempenho ou estado atual no Google Play. (Por exemplo, "Escolha dos Editores", "App n.º 1", "Principais Pagas").
- Apps que apresentam conteúdo ou funcionalidades médicas ou relacionadas com a saúde que sejam enganadoras ou potencialmente prejudiciais.
- Apps que reivindicam funcionalidades que não é possível implementar.
- Apps que são categorizadas incorretamente.
- Conteúdo comprovadamente enganador que pode interferir com os processos de voto.
- Apps que falsamente reivindicam uma afiliação a uma entidade governamental ou que fornecem ou facilitam serviços governamentais para os quais não estão devidamente autorizadas.

Utilização não autorizada ou imitação da funcionalidade do sistema

Não permitimos apps ou anúncios que imitem ou interfiram com a funcionalidade do sistema, como notificações ou avisos. Só é possível utilizar as notificações ao nível do sistema para funcionalidades integrais de uma app, como uma app de uma companhia aérea que notifica os utilizadores sobre ofertas especiais ou um jogo que notifica os utilizadores sobre promoções no jogo.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Apps ou anúncios que sejam fornecidos através de um alerta ou de uma notificação de sistema:



① A notificação de sistema mostrada nesta app está a ser utilizada para publicar um anúncio.

Para exemplos adicionais que envolvam anúncios, consulte a Política de Anúncios.

Alterações enganadoras de definições do dispositivo

Não permitimos apps que efetuem alterações às definições do dispositivo do utilizador ou a funcionalidades fora da app sem conhecimento e consentimento do utilizador. As definições e as funcionalidades do dispositivo incluem definições do navegador e do sistema, marcadores, atalhos, ícones, widgets e a apresentação de aplicações no ecrã principal.

Adicionalmente, não são permitidas:

- Aplicações que modifiquem as definições ou as funcionalidades do dispositivo com autorização do utilizador, mas que o façam de forma que não seja facilmente reversível.

Aplicações ou anúncios que modifiquem as definições ou as funcionalidades do dispositivo como um serviço para terceiros ou para fins publicitários.
Aplicações que enganam os utilizadores para que removam ou desativem aplicações de terceiros, ou para que modifiquem as definições ou as funcionalidades do dispositivo.
Apps que encorajam ou incentivam os utilizadores a remover ou desativar apps de terceiros, ou modifiquem definições ou funcionalidades, exceto se tal fizer parte de um serviço de segurança verificável.

Permissão de comportamentos desonestos

Não permitimos apps que ajudem os utilizadores a enganar outras pessoas ou sejam de qualquer forma funcionalmente enganadoras, incluindo, entre outras, apps que geram ou facilitam a geração de cartões de identificação, números da segurança social, passaportes, diplomas, cartões de crédito e cartas de condução. As apps devem fornecer divulgações, títulos, descrições e imagens/vídeos precisos relativamente ao respetivo conteúdo e/ou funcionalidade e devem funcionar da forma razoável e precisa esperada pelo utilizador.

Mesmo que uma app seja, alegadamente, uma "brincadeira", "apenas para fins de entretenimento" (ou outra designação equivalente), não está isenta da aplicação das nossas políticas.

Conteúdos multimédia manipulados

Não permitimos apps que promovam ou ajudem a criar reivindicações ou informações falsas ou enganadoras através de imagens, vídeos e/ou texto. Não permitimos apps determinadas a promover ou perpetuar imagens, vídeos e/ou texto comprovadamente enganadores que possam causar danos relacionados com um acontecimento sensível, política, questões sociais ou outros assuntos de interesse público.

As apps que manipulam ou alteram conteúdos multimédia, além dos ajustes convencionais e editorialmente aceitáveis para fins de clareza ou qualidade, têm de divulgar de forma proeminente ou adicionar uma marca de água aos conteúdos multimédia alterados quando possa não ser claro para o público que os mesmos foram alterados. Podem ser concedidas exceções em casos de interesse público ou sátira/paródia óbvias.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Apps que adicionam uma figura pública a um protesto durante um acontecimento politicamente sensível.
Apps que utilizam figuras públicas ou conteúdos multimédia de um acontecimento sensível para publicitar a capacidade de alteração de conteúdos multimédia na respetiva Ficha da loja.
Apps que alteram clipes de conteúdos multimédia para imitar uma transmissão de notícias.

Representação fraudulenta

Não permitimos apps ou contas de programador que roubem a identidade de qualquer pessoa ou entidade, que forneçam representações fraudulentas ou ocultem a respetiva propriedade ou objetivo principal. Não são permitidas aplicações ou contas de programador que participem em atividades coordenadas para enganar os utilizadores. Aqui incluem-se, entre outros, aplicações ou contas de programador que representem de forma fraudulenta ou ocultem o país de origem e que direcionem conteúdos para utilizadores noutro país.

Software malicioso

A nossa Política de Software Malicioso é simples: o ecossistema Android, incluindo a Google Play Store, e os dispositivos do utilizador devem estar livres de comportamentos maliciosos (ou seja, software malicioso). Através deste princípio fundamental, o nosso objetivo é fornecer um ecossistema Android seguro para os nossos utilizadores e respetivos dispositivos Android.

Software malicioso é qualquer código que possa colocar um utilizador, os dados de um utilizador ou um dispositivo em risco. O software malicioso inclui, entre outros, aplicações potencialmente prejudiciais (PHAs), binários ou modificações de framework e é constituído por categorias como cavalos de Troia, phishing e apps de spyware. Estamos continuamente a atualizar e a adicionar novas categorias.

Embora varie em tipo e capacidades, o software malicioso tem, normalmente, um dos seguintes objetivos:

> Comprometer a integridade do dispositivo do utilizador.
> Obter controlo sobre o dispositivo de um utilizador.
> Permitir operações controladas remotamente por um atacante para aceder, utilizar ou explorar de outra forma um dispositivo infetado.
> Transmitir dados pessoais ou credenciais a partir do dispositivo sem divulgação e consentimento adequados.
> Disseminar spam ou comandos a partir do dispositivo infetado para afetar outros dispositivos ou redes.
> Defraudar o utilizador.

Uma app, um binário ou uma modificação de framework pode ser potencialmente prejudicial e, assim, gerar comportamento malicioso, mesmo que não se destine a ser prejudicial. Isto acontece porque as apps, os binários ou as modificações de framework podem funcionar de forma diferente, consoante diversas variáveis. Assim, o que é prejudicial para um dispositivo Android pode não colocar de todo em risco outro. Por exemplo, um dispositivo com a versão mais recente do Android não é afetado por apps prejudiciais que utilizem APIs descontinuadas para causar comportamentos maliciosos, mas um dispositivo ainda com uma versão muito antiga do Android pode estar em risco. As apps, os binários ou as modificações de framework

são sinalizados como software malicioso ou PHA se constituírem claramente um risco para alguns ou todos os utilizadores e dispositivos Android.

As categorias de software malicioso abaixo refletem a nossa crença fundamental de que os utilizadores devem compreender de que forma os seus dispositivos estão a ser utilizados e promover um ecossistema seguro que permite uma inovação avançada e uma experiência do utilizador fidedigna.

Visite o Google Play Protect para obter mais informações.

Backdoors

Código que permite a execução de operações indesejadas, potencialmente prejudiciais e controladas remotamente num dispositivo.

Estas operações podem incluir comportamentos que coloquem a app, o binário ou a modificação de framework numa das outras categorias de software malicioso se forem executados automaticamente. Em geral, backdoor é uma descrição da ocorrência de uma operação potencialmente prejudicial num dispositivo e, por conseguinte, não está completamente alinhada com categorias como fraude por faturação ou spyware comercial. Como resultado, um subconjunto de backdoors, em algumas circunstâncias, é tratado pelo Google Play Protect como uma vulnerabilidade.

Fraude por faturação

Código que cobra automaticamente um valor ao utilizador de forma intencionalmente enganadora.

A Fraude por faturação em dispositivos móveis divide-se em Fraude por SMS, Fraude por chamada e Fraude por número pago.

Fraude por SMS

Código que cobra um valor aos utilizadores para enviar SMS premium sem o consentimento ou tenta disfarçar as respetivas atividades de SMS ao ocultar contratos de divulgação ou mensagens SMS do operador móvel que notificam o utilizador sobre cobranças ou confirmam subscrições.

Algum código, embora divulgue tecnicamente o comportamento de envio de SMS, apresenta um comportamento adicional que permite a fraude por SMS. Alguns exemplos incluem ocultar partes de um contrato de divulgação do utilizador, tornando-as ilegíveis e suprimindo de forma condicional mensagens SMS do operador móvel que informam o utilizador sobre cobranças ou confirmam uma subscrição.

Fraude por chamada

Código que permite cobrar um valor aos utilizadores quando efetua chamadas para números premium sem o consentimento dos mesmos.

Fraude por número pago

Código que engana os utilizadores ao levá-los a subscrever ou a comprar conteúdo através da respetiva fatura do telemóvel.

A Fraude por número pago inclui qualquer tipo de faturação, exceto SMS premium e chamadas premium. Alguns exemplos incluem a Faturação direta do operador, o ponto de acesso sem fios (WAP) e a transferência dos minutos de chamadas para telemóvel. A fraude por WAP é um dos tipos mais comuns de fraude por número pago. A fraude por WAP pode incluir enganar os utilizadores ao levá-los a clicar num botão num WebView transparente, carregado silenciosamente. Após realizar a ação, inicia-se uma subscrição recorrente e o SMS ou o email de confirmação é, muitas vezes, acedido indevidamente para impedir que os utilizadores reparem na transação financeira.

Spyware comercial

Código que transmite informações pessoais do dispositivo sem um aviso ou consentimento adequados e não apresenta uma notificação persistente de que tal está a ocorrer.

As apps de spyware comercial transmitem dados para outra parte que não seja o fornecedor de PHAs. Os pais podem utilizar versões legítimas destas apps para monitorizar os seus filhos. No entanto, estas apps não podem ser utilizadas para monitorizar uma pessoa (um cônjuge, por exemplo) sem o respetivo conhecimento ou autorização se uma notificação persistente não for apresentada enquanto os dados estão a ser transmitidos.

Negação de serviço (DoS)

Código que, sem conhecimento do utilizador, executa um ataque de negação de serviço (DoS) ou faz parte de um ataque DoS distribuído contra outros sistemas e recursos.

Por exemplo, tal pode ocorrer ao enviar um elevado volume de pedidos HTTP para produzir uma carga excessiva nos servidores remotos.

Gestores de transferências hostis

Código que, por si só, não é potencialmente prejudicial, mas transfere outras PHAs.

O código pode ser um gestor de transferências hostil se:

- Existirem motivos para acreditar que foi criado para distribuir PHAs e tiver transferido PHAs ou contiver código que pode transferir e instalar apps; ou
- Pelo menos, 5% das apps transferidas pelo mesmo forem PHAs com um limite mínimo de 500 transferências de apps observadas (25 transferências de PHAs observadas).

Os principais navegadores e apps de partilha de ficheiros não são considerados gestores de transferências hostis, desde que:

- Não iniciem transferências sem a interação do utilizador; e
- Todas as transferências de PHAs forem iniciadas por utilizadores que as consentiram.

Ameaça que não afeta o Android

Código que contém ameaças que não afetam o Android.

Estas apps não podem causar danos aos dispositivos nem aos utilizadores do Android, mas contêm componentes que são potencialmente prejudiciais para outras plataformas.

Phishing

Código que finge ser de uma origem fidedigna, solicita as credenciais de autenticação ou as informações de faturação de um utilizador e envia os dados a terceiros. Esta categoria também se aplica ao código que interceta a transmissão de credenciais do utilizador em trânsito.

Os alvos comuns de phishing incluem credenciais bancárias, números de cartões de crédito e credenciais de contas online para redes sociais e jogos.

Abuso de privilégios elevados

Código que compromete a integridade do sistema ao danificar o sandbox da app, obter privilégios elevados ou alterar/desativar o acesso a funções de segurança essenciais.

Os exemplos incluem:

- Uma app que viola o modelo de autorizações do Android ou rouba credenciais (tais como símbolos OAuth) de outras apps.
- Apps que abusam das funcionalidades para impedir a respetiva desinstalação ou paragem.
- Uma app que desativa o SELinux.

As apps de escalamento de privilégios que criam acesso máximo nos dispositivos sem a autorização do utilizador são classificadas como apps com acesso máximo.

Ransomware

Código que assume o controlo parcial ou extensivo de um dispositivo ou de dados num dispositivo e exige que o utilizador efetue um pagamento ou realize uma ação para libertar o controlo.

Alguns tipos de ransomware encriptam os dados no dispositivo e exigem um pagamento para os desencriptar e/ou tiram partido das funcionalidades de administração do dispositivo para que um utilizador típico não os possa remover. Os exemplos incluem:

Bloquear o acesso de um utilizador ao respetivo dispositivo e exigir dinheiro para restaurar o controlo do utilizador.
Encriptar os dados no dispositivo e exigir um pagamento aparentemente para desencriptar os dados.
Tirar partido das funcionalidades de gestão de políticas do dispositivo e bloquear a remoção por parte do utilizador.

O código distribuído com o dispositivo cujo objetivo principal seja a gestão de dispositivos subsidiados pode ser excluído da categoria de ransomware desde que cumpra os requisitos de gestão e bloqueio seguros, bem como os requisitos adequados de divulgação e consentimento do utilizador.

Acesso máximo

Código com acesso máximo ao dispositivo.

Existe uma diferença entre código com acesso máximo malicioso e não malicioso. Por exemplo, as apps com acesso máximo não maliciosas informam o utilizador antecipadamente de que irão controlar o dispositivo com acesso máximo e não executam outras ações potencialmente prejudiciais que se aplicam a outras categorias de PHAs.

As apps com acesso máximo maliciosas não informam o utilizador de que irão controlar o dispositivo com acesso máximo ou informam o utilizador antecipadamente acerca do acesso máximo, mas também executam outras ações que se aplicam a outras categorias de PHAs.

Spam

Código que envia mensagens não solicitadas aos contactos do utilizador ou que utiliza o dispositivo para a transmissão de spam por email.

Spyware

Código que transmite dados pessoais do dispositivo sem aviso ou consentimento adequados.

Por exemplo, a transmissão de quaisquer das seguintes informações sem divulgação ou de uma forma inesperada para o utilizador é suficiente para ser considerada spyware:

Lista de contactos
Fotos ou outros ficheiros do cartão SD ou não pertencentes à app
Conteúdo do email do utilizador
Registo de chamadas
Registo de SMS
Histórico da Web ou marcadores do navegador predefinido
Informações dos diretórios /data/ de outras apps.

Comportamentos que possam ser considerados espionagem sobre o utilizador também podem ser sinalizados como spyware. Por exemplo, gravação de áudio ou de chamadas efetuadas para o telemóvel ou roubo de dados de apps.

Cavalo de Troia

Código que parece benigno, como um jogo que afirma ser apenas um jogo, mas que realiza ações indesejadas contra o utilizador.

Normalmente, esta classificação é utilizada em combinação com outras categorias de PHAs. Um cavalo de Troia tem um componente inócuo e um componente prejudicial oculto. Por exemplo, um jogo que envia mensagens SMS premium do dispositivo do utilizador em segundo plano sem o seu conhecimento.

Nota sobre apps invulgares

Apps novas e raras podem ser classificadas como invulgares se o Google Play Protect não tiver informações suficientes para as considerar seguras. Isto não significa que a app seja necessariamente prejudicial, mas, sem uma revisão adicional, também não pode ser considerada segura.

Nota sobre a categoria Backdoor

A classificação de categoria de software malicioso de backdoor depende da forma como o código atua. Uma condição necessária para qualquer código ser classificado como backdoor é permitir comportamentos que colocariam o código numa das outras categorias de software malicioso se fosse executado automaticamente. Por exemplo, se uma app permitir o carregamento de código dinâmico e o código carregado dinamicamente estiver a extrair mensagens de texto, será classificada como software malicioso de backdoor.

No entanto, se uma app permitir a execução de código arbitrário e não tivermos qualquer razão para acreditar que esta execução de código foi adicionada para realizar um comportamento malicioso, a app será tratada como tendo uma vulnerabilidade, em vez de ser considerada software malicioso de backdoor, e será solicitado ao programador que a corrija.

Não são permitidas apps que incluam anúncios enganadores ou perturbadores. Os anúncios apenas devem ser apresentados na app que os publica. Consideramos que os anúncios publicados na sua app fazem parte dela. Os anúncios apresentados na sua app têm de estar em conformidade com todas as nossas políticas. Para consultar as políticas sobre anúncios de jogos de azar, clique aqui.
O Google Play apoia várias estratégias de rentabilização para beneficiar os programadores e os utilizadores, incluindo distribuição paga, produtos na app, subscrições e modelos baseados em anúncios. Para garantir a melhor experiência do utilizador, tem de cumprir estas políticas.

Pagamentos

As apps que utilizam as compras na app ou na loja têm de cumprir as seguintes diretrizes:

Compras na loja: os programadores que cobrem apps e transferências do Google Play têm de utilizar o sistema de pagamento do Google Play.

Compras na app:

- Os programadores que ofereçam produtos dentro de um jogo transferido do Google Play ou que forneçam acesso a conteúdo de jogos têm de utilizar a Faturação em apps do Google Play como método de pagamento.
- Os programadores que ofereçam produtos dentro de outra categoria de apps transferidas do Google Play têm de utilizar a Faturação em apps do Google Play como método de pagamento, exceto nos seguintes casos:
  - O pagamento destina-se apenas a produtos físicos.
  - O pagamento destina-se a conteúdo digital que é possível consumir fora da própria app (por exemplo, músicas que é possível reproduzir noutros leitores de música).
- Só é possível utilizar moedas virtuais na app dentro da app ou do título do jogo para o qual foram compradas.
- Os programadores não podem enganar os utilizadores acerca das apps que estão a vender nem sobre quaisquer serviços, bens, conteúdos ou funcionalidades na app que estejam a disponibilizar para venda. Se a descrição do seu produto no Google Play se referir a funcionalidades na app que possam exigir custos específicos ou adicionais, a descrição tem de informar claramente os utilizadores de que é necessário pagar para aceder a essas funcionalidades.
- As apps que disponibilizem mecanismos para receber itens virtuais aleatórios de uma compra (ou seja, "caixas de saque") têm de divulgar de forma clara as probabilidades de receção desses itens antes da compra.

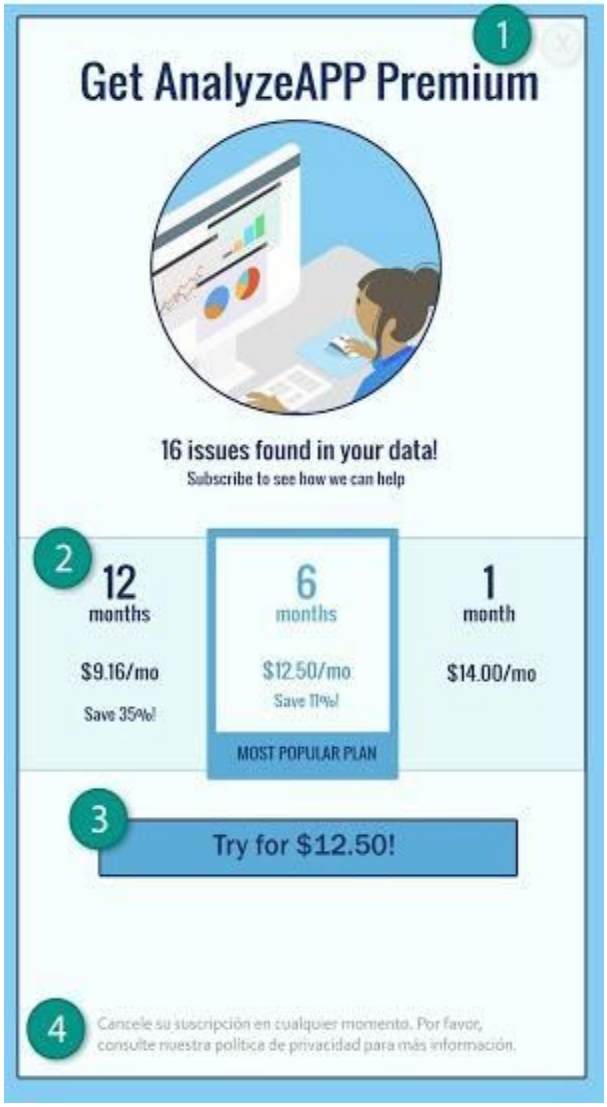
Subscrições

Como programador, não pode enganar os utilizadores relativamente a quaisquer serviços de subscrição ou conteúdos que disponibilize na sua app. É essencial comunicar claramente a sua oferta em todos os ecrãs iniciais ou promoções na app.

Na sua app: tem de ser transparente relativamente à sua oferta. Isto inclui explicar detalhadamente os termos da sua oferta, incluindo o custo da subscrição, a frequência do ciclo de faturação e se é obrigatório ter uma subscrição para utilizar a app. Os utilizadores não devem ter de efetuar qualquer ação adicional para rever as informações.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Subscrições mensais que não informam os utilizadores de que serão automaticamente renovadas e que lhes será cobrado um valor todos os meses.
Subscrições anuais que apresentam os preços mais proeminentemente em termos de custo mensal.
Termos e preços da subscrição que estão localizados de forma incompleta.
Promoções na app que não demonstram claramente que o utilizador pode aceder ao conteúdo sem uma subscrição (se disponível).
Nomes de SKUs que não transmitem com exatidão a natureza da subscrição, como "Avaliação gratuita" para uma subscrição com uma cobrança periódica automática.



① O botão Ignorar não está claramente visível e os utilizadores podem não compreender que podem aceder à funcionalidade sem aceitar a oferta da subscrição.

② A oferta apenas apresenta o preço em termos de custo mensal e os utilizadores podem não compreender que lhes será cobrado o preço referente a um período de seis meses no momento em que subscrevem.

③ A oferta apenas apresenta o preço inicial e os utilizadores podem não compreender o que lhes será automaticamente cobrado no final do período inicial.

④ A oferta deve estar localizada no mesmo idioma que os termos de utilização para que os utilizadores possam compreender toda a oferta.

Avaliações gratuitas e ofertas iniciais

Antes de um utilizador estar inscrito na sua subscrição: tem de descrever de forma clara e precisa os termos da sua oferta, incluindo a duração, o preço e a descrição dos conteúdos ou serviços acessíveis. Certifique-se de que informa os seus utilizadores sobre quando e como uma avaliação gratuita será convertida numa subscrição paga, quanto a mesma irá custar e que podem cancelar se não quiserem converter numa subscrição paga.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Ofertas que não explicam de forma clara quanto tempo durará a avaliação gratuita ou o preço inicial.
- Ofertas que não explicam de forma clara que o utilizador será automaticamente inscrito numa subscrição paga no final do período da oferta.
- Ofertas que não demonstram de forma clara que um utilizador pode aceder ao conteúdo sem uma avaliação (quando disponível).
- Termos e preços da oferta que estão localizados de forma incompleta.

① O botão Ignorar não está claramente visível e os utilizadores podem não compreender que podem aceder à funcionalidade sem se inscreverem na avaliação gratuita.

② A oferta realça a avaliação gratuita e os utilizadores podem não compreender que lhes será automaticamente efetuada uma cobrança no final da avaliação.

③ A oferta não indica um período de avaliação e os utilizadores podem não compreender durante quanto tempo o acesso gratuito ao conteúdo da subscrição irá durar.

④ A oferta deve estar localizada no mesmo idioma que os termos de utilização para que os utilizadores possam compreender toda a oferta.

Gestão e cancelamento de subscrições

Como programador, tem de se certificar de que as suas apps divulgam claramente como um utilizador pode gerir ou cancelar a respetiva subscrição.

Se um utilizador cancelar uma subscrição comprada numa app do Google Play, a nossa política prevê que o utilizador não receberá qualquer reembolso pelo período de faturação atual, mas continuará a receber os conteúdos da sua subscrição durante o período de faturação restante, independentemente da data de cancelamento. O cancelamento do utilizador entra em vigor após a conclusão do período de faturação atual.

O programador (enquanto fornecedor de conteúdo ou de acesso) pode implementar uma política de reembolso mais flexível diretamente com os seus utilizadores. É da sua responsabilidade notificar os utilizadores de quaisquer alterações às suas políticas de subscrição, cancelamento e reembolso e garantir que as mesmas cumprem a lei aplicável.

Não são permitidas apps que incluam anúncios enganadores ou perturbadores. Os anúncios apenas devem ser apresentados na app que os publica. Consideramos que os anúncios publicados na sua app fazem parte dela. Os anúncios apresentados na sua app têm de estar em conformidade com todas as nossas políticas. Para consultar as políticas sobre anúncios de jogos de azar, clique aqui.
Não são permitidas apps que incluam anúncios enganadores ou perturbadores. Os anúncios apenas devem ser apresentados na app que os publica. Consideramos que os anúncios publicados na sua app fazem parte dela. Os anúncios apresentados na sua app têm de estar em conformidade com todas as nossas políticas. Para consultar as políticas sobre anúncios de jogos de azar, clique aqui.

Utilização de dados de localização para anúncios

As apps que estendam a utilização de dados de localização do dispositivo com base na autorização para publicar anúncios estão sujeitas à Política de Informações Pessoais e Confidenciais e têm de agir em conformidade com os seguintes requisitos:

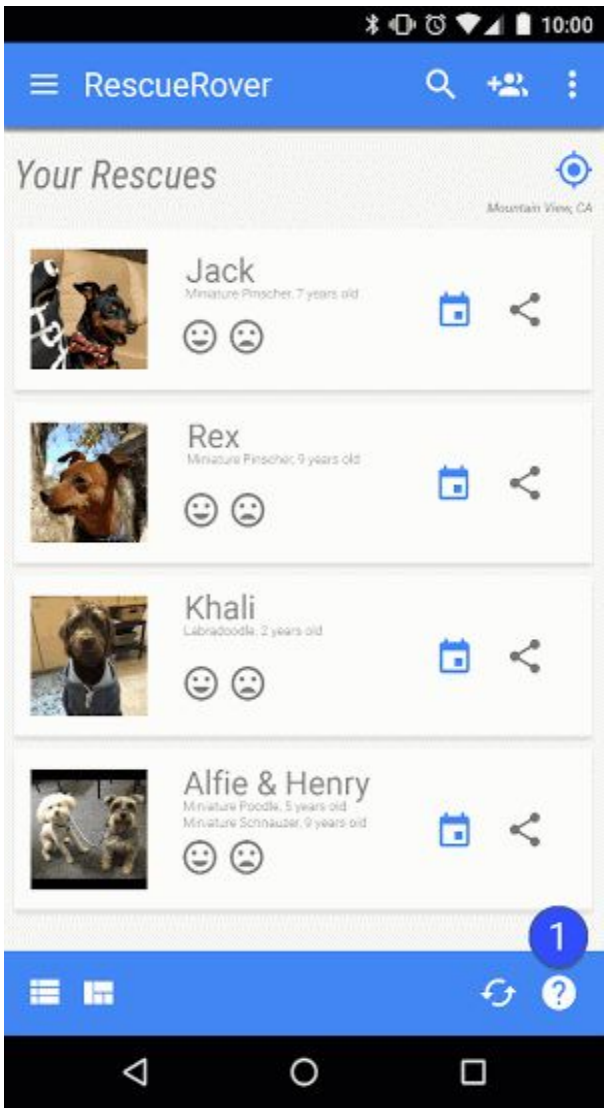
> A utilização ou recolha de dados de localização do dispositivo com base na autorização para fins de publicidade deve ser clara para o utilizador e documentada na política de privacidade obrigatória da app, incluindo links para quaisquer políticas de privacidade relevantes da rede de publicidade referentes à utilização dos dados de localização.
> Em conformidade com os requisitos de Autorizações de acesso à localização, as autorizações de acesso à localização apenas podem ser solicitadas para implementar funcionalidades ou serviços atuais na app e não podem solicitar autorizações de acesso à localização do dispositivo exclusivamente para a utilização de anúncios.

Anúncios enganadores

Os anúncios não podem simular nem imitar a interface de utilizador de uma app nem os elementos de aviso ou de notificação de um sistema operativo. Deve ser claro para o utilizador que app está a publicar cada anúncio.

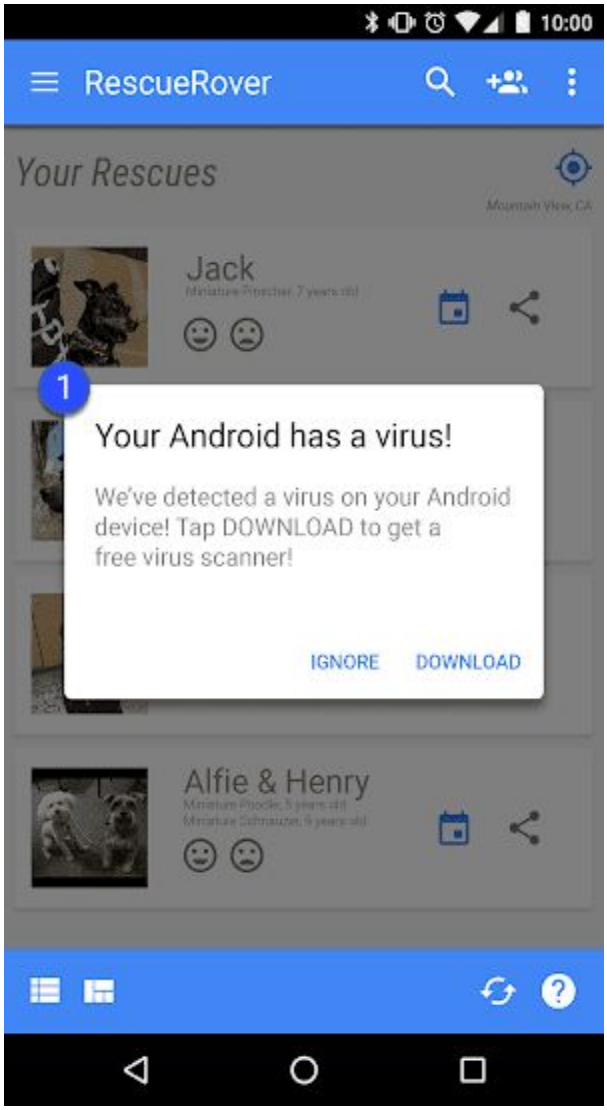
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

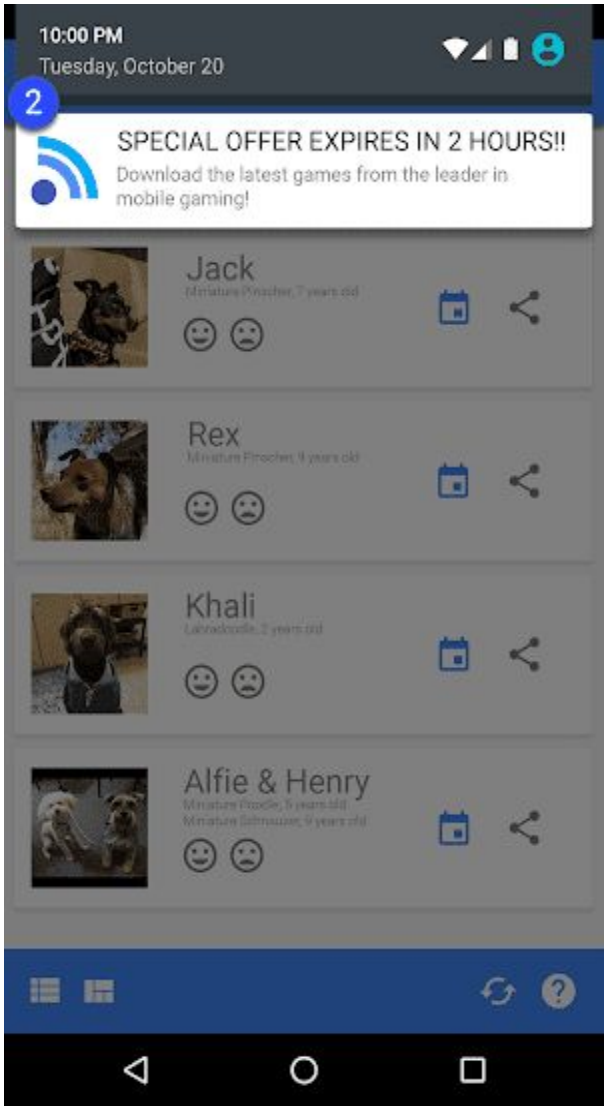
Anúncios que imitam a IU de uma app:



① O ícone do ponto de interrogação nesta aplicação é um anúncio que direciona o utilizador para uma página de destino externa.

Anúncios que imitam uma notificação de sistema:





① ② Os exemplos acima ilustram anúncios que imitam várias notificações de sistema.

Rentabilização do ecrã de bloqueio

Exceto quando o objetivo exclusivo da app é ser um ecrã de bloqueio, as apps não podem introduzir anúncios ou funcionalidades que rentabilizem o ecrã bloqueado de um dispositivo.

Anúncios perturbadores

Os anúncios não devem ser apresentados de uma forma que provoque cliques inadvertidos. É proibido forçar um utilizador a clicar num anúncio ou a enviar informações pessoais para fins publicitários antes de poder utilizar uma aplicação na íntegra.

Os anúncios intercalares só podem ser apresentados dentro da aplicação que os publica. Se a sua app apresentar anúncios intercalares ou outros anúncios que interfiram com a utilização normal, estes devem ser fáceis de ignorar sem penalizações.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Anúncios que ocupam o ecrã inteiro ou interferem com a utilização normal e não fornecem um meio claro para os ignorar:

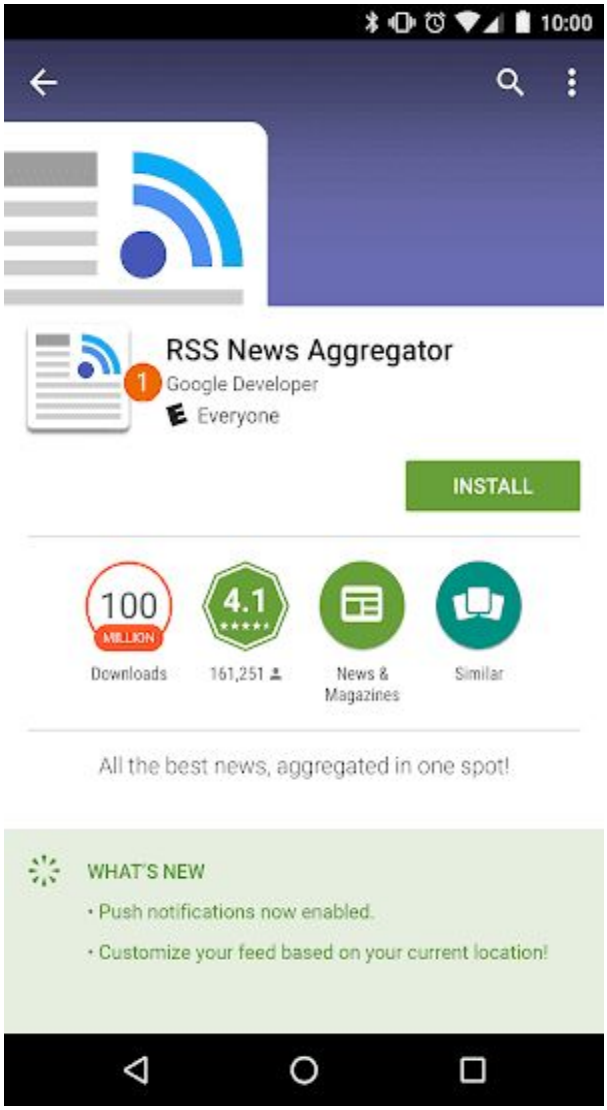
① Este anúncio não tem um botão de ignorar.

Interferência com apps, anúncios de terceiros ou a funcionalidade do dispositivo

Os anúncios associados à sua app não podem interferir com outras apps, anúncios ou o funcionamento do dispositivo, incluindo botões e portas do dispositivo ou do sistema. Isto inclui sobreposições, funcionalidade associada e blocos de anúncios com widgets. Os anúncios apenas devem ser apresentados na app que os publica.

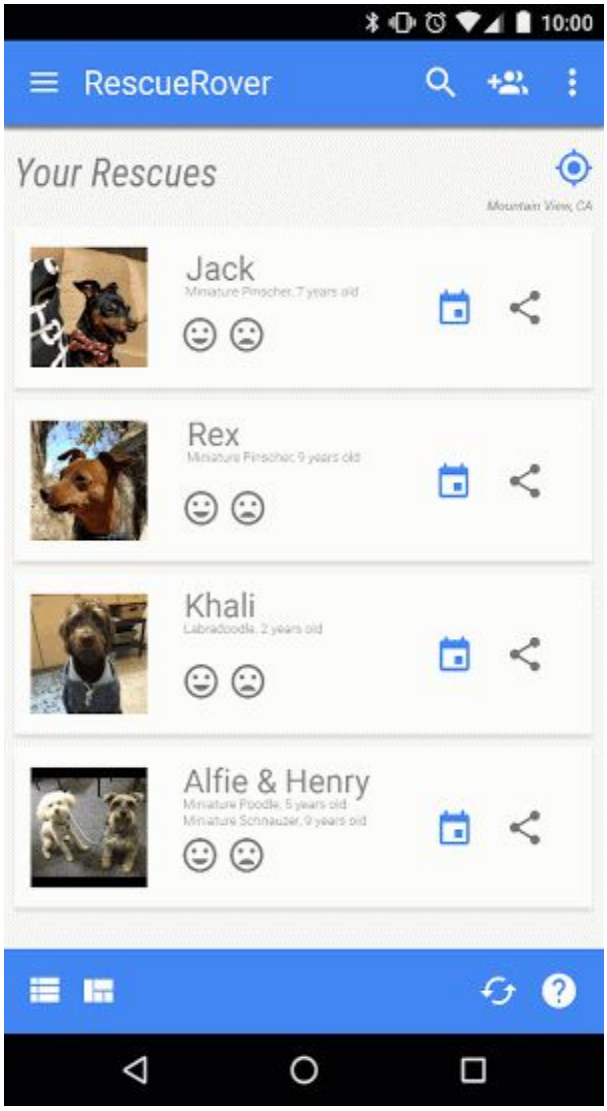
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Anúncios apresentados fora da app que os publica:



Descrição: o utilizador navega para o ecrã principal a partir desta aplicação e, de repente, surge um anúncio no ecrã principal.

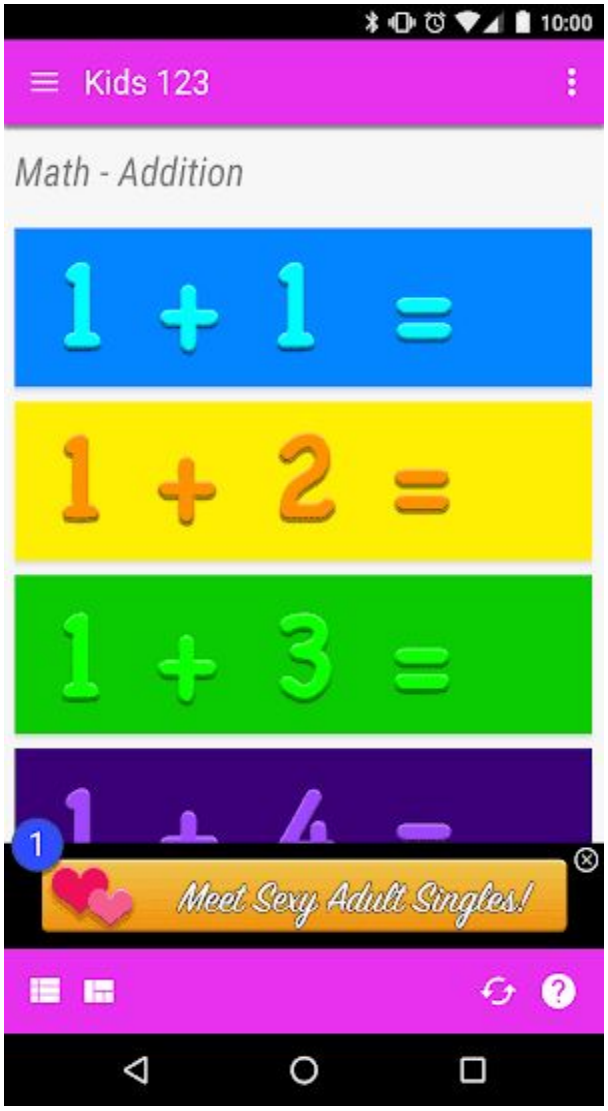
Anúncios que são acionados pelo botão Página inicial ou por outras funcionalidades expressamente concebidas para sair da aplicação:



Descrição: o utilizador tenta sair da app e navegar até ao ecrã principal, mas, em vez disso, o fluxo esperado é interrompido por um anúncio.

Anúncios impróprios

Os anúncios apresentados na sua app têm de ser adequados para o público-alvo pretendido para a mesma, independentemente de o próprio conteúdo estar em conformidade com as nossas políticas.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.



① Este anúncio é impróprio para o público-alvo a que se dirige esta app.

Utilização do ID de publicidade Android

A versão 4.0 dos Serviços do Google Play introduziu novas APIs e um ID para serem utilizados por fornecedores de análises e de publicidade. Seguem-se os Termos de Utilização deste ID.

> Utilização. O identificador de publicidade Android apenas deve ser utilizado para análises de utilizadores e de publicidade. O estado da definição "Excluir publicidade baseada em interesses" ou "Desativar a personalização de anúncios" deve ser validado em cada acesso do ID.
> Associação a informações de identificação pessoal ou outros identificadores. O identificador de publicidade não pode estar ligado a informações de identificação pessoal ou associado a qualquer identificador de dispositivo persistente (por exemplo: SSAID, endereço MAC, IMEI, etc.) sem o consentimento expresso do utilizador.

Respeito das seleções dos utilizadores. Em caso de reposição, um novo identificador de publicidade não pode estar associado a um identificador de publicidade anterior ou a dados derivados de um identificador de publicidade anterior sem o consentimento expresso do utilizador. Além disso, tem de respeitar a definição "Excluir publicidade baseada em interesses" ou "Desativar a personalização de anúncios" do utilizador. Se um utilizador tiver ativado esta definição, não pode utilizar o identificador de publicidade para criar perfis de utilizador para fins de publicidade ou segmentar utilizadores com publicidade personalizada. As atividades permitidas incluem a publicidade por contexto, o limite de frequência, o acompanhamento de conversões, os relatórios, a segurança e a deteção de fraude.
Transparência para os utilizadores. A recolha e a utilização do identificador de publicidade e o compromisso para com os presentes termos devem ser divulgados aos utilizadores através de uma notificação de privacidade juridicamente adequada. Para saber mais acerca das nossas normas de privacidade, reveja a nossa Política de Dados do Utilizador.
Cumprimento dos Termos de Utilização. Só é possível utilizar o identificador de publicidade de acordo com os presentes termos, incluindo por qualquer parte com a qual o possa partilhar no decorrer da sua atividade. Todas as aplicações carregadas ou publicadas no Google Play têm de utilizar o ID de publicidade (quando estiver disponível num dispositivo) em detrimento de quaisquer outros identificadores de dispositivos para quaisquer fins publicitários.

Programa de anúncios para famílias

Se publicar anúncios na sua app e o público-alvo da mesma incluir apenas crianças, tal como descrito na Política para Famílias, tem de utilizar SDKs de anúncios com conformidade autocertificada com as Políticas do Google Play, incluindo os requisitos de certificação dos SDKs de anúncios abaixo. Se o público-alvo da sua app incluir tanto crianças como utilizadores mais velhos, tem de implementar medidas de filtragem de idade e assegurar que os anúncios apresentados a crianças são provenientes exclusivamente de um destes SDKs de anúncios autocertificados. As apps no programa Concebido para Famílias apenas podem utilizar SDKs de anúncios autocertificados.

A utilização de SDKs de anúncios certificados pelo Google Play só é obrigatória se estiver a utilizar SDKs de anúncios para publicar anúncios para crianças. O seguinte é permitido sem autocertificação de um SDK de anúncios no Google Play. No entanto, ainda é responsável por garantir que o conteúdo dos anúncios e as suas práticas de recolha de dados estão em conformidade com a Política de Dados do Utilizador e a Política para Famílias do Google Play:

Publicidade interna, através da qual utiliza SDKs para gerir a promoção cruzada das suas apps ou outro merchandising e multimédia dos quais é proprietário.
Estabelecer ofertas diretas com anunciantes, através das quais utiliza SDKs para gestão de inventário.

Requisitos de certificação de SDKs de anúncios

- Defina o que são comportamentos e conteúdos de anúncios censuráveis e proíba-os nos termos ou nas políticas do SDK de anúncios. As definições não devem resultar na não conformidade com as Políticas do Programa para Programadores do Google Play.
- Crie um método de classificação dos seus criativos de anúncios de acordo com grupos adequados à faixa etária, incluindo, no mínimo, grupos para Todos e Adultos. A metodologia de classificação tem de estar em linha com a metodologia que a Google fornece aos SDKs assim que tiverem preenchido o formulário de interesse abaixo.
- Permita que os publicadores, por pedido ou por app, solicitem o tratamento dirigido a crianças para a publicação de anúncios. Este tratamento tem de estar em conformidade com as leis e regulamentos aplicáveis, tais como a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA e o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE. O Google Play requer igualmente a desativação de anúncios personalizados, publicidade baseada em interesses e remarketing como parte do tratamento dirigido a crianças.
- Certifique-se de que, quando forem utilizados lances em tempo real para publicar anúncios para crianças, os criativos foram revistos e os indicadores de privacidade são propagados para os licitadores.
- Forneça à Google informações suficientes para validar a conformidade do SDK de anúncios com todos os requisitos de certificação e responda atempadamente a quaisquer pedidos de informação subsequentes.

Nota: os SDKs de anúncios têm de suportar a publicação de anúncios em conformidade com todos os estatutos e regulamentos relevantes no que se refere a crianças que possam ser aplicáveis aos respetivos publicadores.

Requisitos de mediação para plataformas de publicação ao publicar anúncios para crianças:

- Utilize apenas SDKs de anúncios certificados pelo Google Play ou implemente as salvaguardas necessárias para assegurar que todos os anúncios publicados a partir da mediação estão em conformidade com estes requisitos; e
- Transmita os sinais necessários para indicar a classificação do conteúdo do anúncio e qualquer tratamento dirigido a crianças aplicável.

Os programadores podem encontrar uma lista de SDKs de anúncios autocertificados aqui.

Os programadores podem ainda partilhar este formulário de interesse com os SDKs de anúncios que se pretendam tornar autocertificados.

Ficha da loja e promoção

A promoção e a visibilidade da sua app afetam dramaticamente a qualidade da loja. Evite Fichas da loja com spam, promoções de baixa qualidade e tentativas de otimizar artificialmente a visibilidade da app no Google Play.

Promoção de apps

Não são permitidas apps que participem ou beneficiem, direta ou indiretamente, de práticas de promoção enganadoras ou que sejam prejudiciais para os utilizadores ou para o ecossistema de programadores. Isto inclui aplicações que apresentem os seguintes comportamentos:

- Utilização de anúncios enganadores em Websites, aplicações ou outras propriedades, incluindo notificações que sejam semelhantes aos alertas e às notificações do sistema.
- Táticas de instalação ou de promoção que redirecionem os utilizadores para o Google Play ou transfiram aplicações sem uma ação informada por parte do utilizador.
- Promoção não solicitada através de serviços de SMS.

É da responsabilidade do programador garantir que todas as redes de publicidade ou afiliadas associadas à sua app ajam em conformidade com estas políticas e não empreguem quaisquer práticas de promoção proibidas.

Não permitimos apps com metadados enganadores, incorretamente formatados, não descritivos, irrelevantes, excessivos ou impróprios, incluindo, entre outros, a descrição da app, o nome do programador, o título, o ícone, as capturas de ecrã e as imagens promocionais. Os programadores têm de fornecer uma descrição clara e bem escrita. Da mesma forma, não permitimos testemunhos de utilizadores não atribuídos ou anónimos na descrição da app. Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

① Testemunhos de utilizadores não atribuídos ou anónimos

② Comparação de dados de apps ou marcas

③ Blocos de palavras e listas de palavras verticais/horizontais

Eis alguns exemplos de texto, imagens ou vídeos impróprios na sua ficha:

Imagens ou vídeos que incluem conteúdo com conotações sexuais. Evite imagens sugestivas com seios, nádegas, órgãos genitais ou outra parte anatómica, ou outro conteúdo alvo de fetiches, independentemente de serem ilustrados ou reais.
Linguagem imprópria para um público-alvo geral. Evite uma linguagem profana e vulgar na ficha da sua aplicação. Se se tratar de um elemento crítico da app, tem de censurar a respetiva apresentação na Ficha da loja.
Violência gráfica representada proeminentemente em símbolos de apps, vídeos ou imagens promocionais.

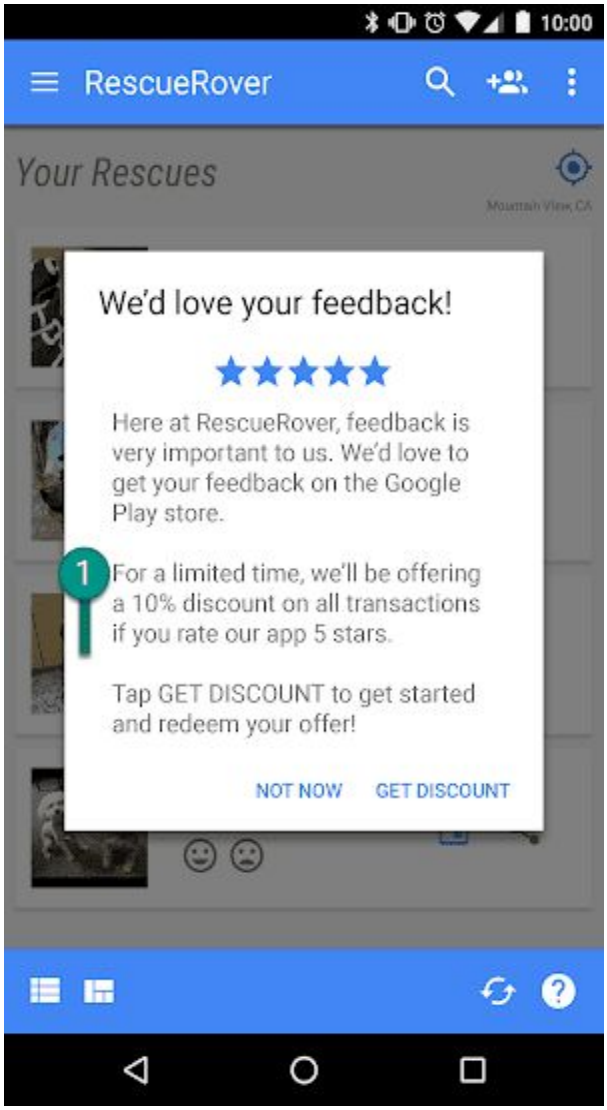
Representações do uso ilícito de drogas. O conteúdo EDSA (educativo, documental, científico ou artístico) também tem de ser adequado a todos os públicos-alvo da Ficha da loja.

Eis algumas práticas recomendadas:

Realce o que a sua app tem de melhor. Partilhe factos interessantes e entusiasmantes acerca da sua app para ajudar os utilizadores a compreenderem o que a torna especial.
Certifique-se de que o título e a descrição da app descrevem com precisão a funcionalidade da mesma.
Evite utilizar palavras-chave ou referências repetitivas ou não relacionadas.
Mantenha a descrição da sua aplicação breve e objetiva. As descrições mais curtas tendem a resultar numa melhor experiência do utilizador, especialmente em dispositivos com ecrãs menores. Tamanho, repetições, detalhes excessivos ou formatação imprópria podem resultar na violação desta política.
Lembre-se de que a sua ficha deve ser adequada a um público-alvo geral. Evite utilizar texto, imagens ou vídeos impróprios na ficha e cumpra as diretrizes acima.

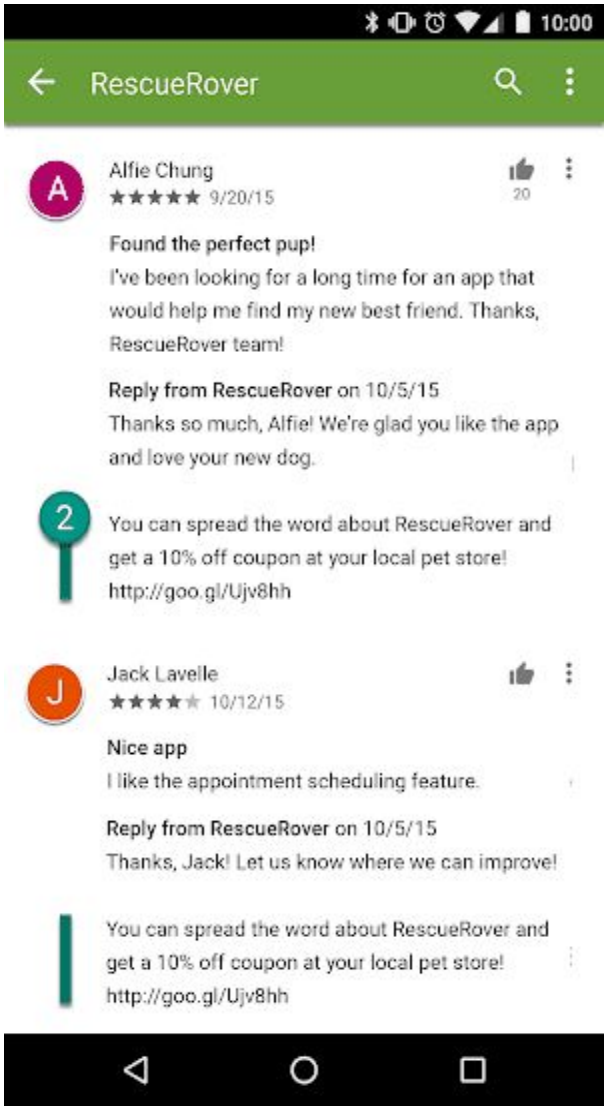
Os programadores não podem tentar manipular o posicionamento de quaisquer apps no Google Play. Isto inclui, entre outras ações, inflacionar as classificações, as opiniões ou o número de instalações do produto por meios ilegítimos, como instalações, opiniões e classificações fraudulentas ou incentivadas.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Pedir aos utilizadores para classificar a app ao oferecer um incentivo:



① Esta notificação oferece aos utilizadores um desconto em troca de uma classificação elevada.

O envio repetido de classificações para influenciar o posicionamento da app no Google Play.
Enviar ou encorajar os utilizadores a enviarem opiniões com conteúdo impróprio, incluindo afiliados, cupões, códigos de jogos, endereços de email ou links para Websites ou outras apps:



② Esta opinião encoraja os utilizadores a promoverem a app RescueRover ao oferecer um cupão.

As classificações e as opiniões são referências quanto à qualidade da app. Os utilizadores dependem da sua autenticidade e relevância. Seguem-se algumas práticas recomendadas a utilizar nas respostas a opiniões de utilizadores:

- Limite a sua resposta aos problemas mencionados nos comentários do utilizador e não peça uma classificação superior.
- Inclua referências a recursos úteis, como um endereço de apoio técnico ou uma página de Perguntas frequentes.

O nosso sistema de classificação de conteúdo inclui classificações oficiais da International Age Rating Coalition (IARC) e foi concebido para ajudar os programadores a divulgar as classificações de conteúdo pertinentes do ponto de vista geográfico junto dos utilizadores.

Como são utilizadas as classificações de conteúdo

As classificações de conteúdo são utilizadas para informar os consumidores, em especial os pais, acerca de conteúdo potencialmente censurável existente numa app. Também ajudam a filtrar ou a bloquear o conteúdo em determinados territórios ou para utilizadores específicos onde tal seja legalmente exigido e a determinar a elegibilidade da app para programas especiais de programadores.

Como são atribuídas as classificações de conteúdo

Para receber uma classificação de conteúdo, tem de preencher um questionário de classificação na Play Console que indique a natureza do conteúdo das suas apps. É atribuída à app uma classificação de conteúdo de várias autoridades de classificação com base nas respostas do questionário. A representação fraudulenta do conteúdo da sua aplicação pode resultar na respetiva remoção ou suspensão, pelo que é importante fornecer respostas corretas ao questionário de classificação de conteúdo.

Para evitar que a app seja apresentada como "Sem classificação", tem de preencher o questionário de classificação de conteúdo para cada nova app enviada para a Play Console, bem como para todas as apps existentes ativas no Google Play. As apps sem classificação de conteúdo serão removidas da Play Store.

Se efetuar alterações ao conteúdo ou às funcionalidades da app que afetem as respostas ao questionário de classificação, tem de enviar um novo questionário de classificação de conteúdo na Play Console.

Visite o Centro de Ajuda para encontrar mais informações acerca das diferentes autoridades de classificação e de como preencher o questionário de classificação de conteúdo.

Recursos de classificação

Se não concordar com a classificação atribuída à sua app, pode apresentar recurso diretamente à autoridade de classificação IARC através do link fornecido no email de certificado.

Spam e funcionalidade mínima

No mínimo, as apps devem fornecer aos utilizadores um nível básico de funcionalidade e uma experiência do utilizador respeitosa. As apps que falham, exibem comportamentos que não condizem com uma experiência do utilizador funcional ou servem apenas para enviar spam para os utilizadores ou o Google Play são apps que não contribuem de forma positiva para a expansão do catálogo.

Spam

Não são permitidas apps que enviem spam para os utilizadores ou para o Google Play, como apps que enviem mensagens não solicitadas aos utilizadores ou apps que sejam repetitivas ou de baixa qualidade.

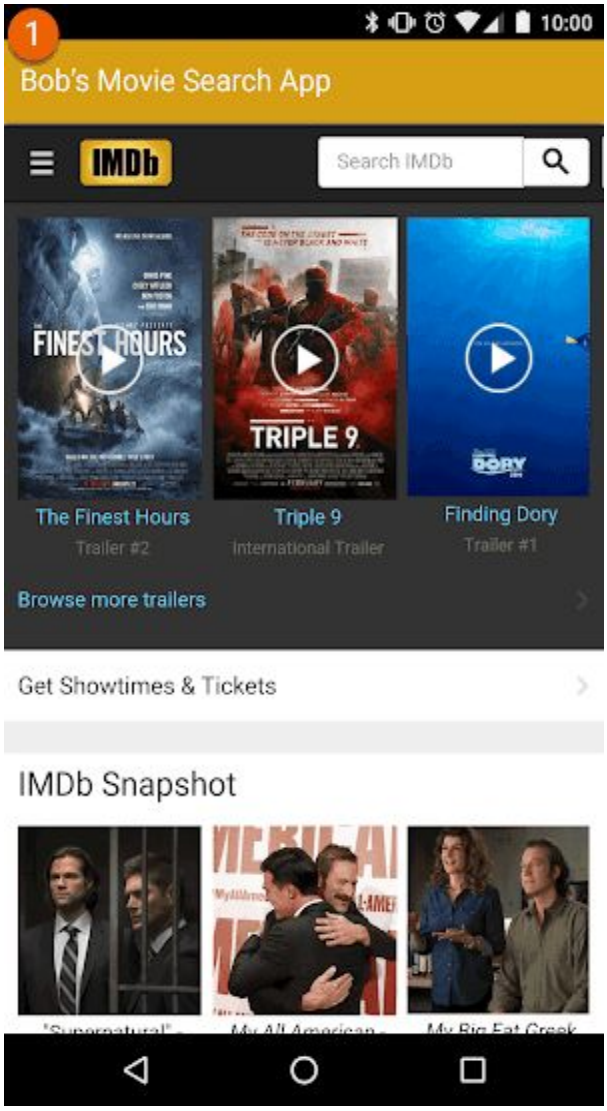
Spam em mensagens

Não são permitidas apps que enviem SMS, emails ou outras mensagens em nome do utilizador sem possibilitar ao utilizador a hipótese de confirmar o conteúdo e os destinatários pretendidos.

Spam de afiliados e em visualizações na Web

Não são permitidas apps cujo objetivo principal seja direcionar tráfego afiliado para um Website ou fornecer uma visualização na Web de um Website sem autorização do administrador ou do proprietário do Website.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

> Uma app cujo objetivo principal seja direcionar tráfego de referência para um Website para receber crédito para inscrições de utilizações ou compras nesse Website.
> Apps cujo objetivo principal seja fornecer uma visualização na Web de um Website sem autorização:



① Esta app chama-se "Bob's Movie Search App" e fornece simplesmente uma visualização na Web do IMDB.

Conteúdo repetitivo

Não são permitidas apps que se limitem a proporcionar a mesma experiência que outras apps já proporcionam no Google Play. As apps devem proporcionar valor aos utilizadores através da criação de conteúdos ou de serviços exclusivos.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Copiar conteúdos de outras apps sem adicionar qualquer conteúdo original ou valor.
Criar várias apps com conteúdos e uma experiência do utilizador extremamente semelhantes. Se estas apps forem todas pequenas em termos de volume de conteúdo, os programadores devem ponderar a criação de uma única app que agregue todo o conteúdo.

Não são permitidas apps criadas por uma ferramenta automática, um serviço de assistente ou baseadas em modelos e enviadas para o Google Play pelo operador desse serviço em nome de outras pessoas. Estas apps apenas são permitidas se forem publicadas por uma conta de programador registada individualmente pertencente ao utilizador da ferramenta automática, não ao operador do serviço.

Concebidas para anúncios

Não permitimos apps cujo principal objetivo seja a publicação de anúncios.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

> Apps em que são colocados anúncios intercalares após todas as ações do utilizador, incluindo, entre outras, cliques, deslizes rápidos, etc.

Funcionalidade mínima

Certifique-se de que a sua app proporciona uma experiência do utilizador estável, apelativa e eficaz.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

> Apps que são concebidas para não fazerem nada ou não terem nenhuma função.

Funcionalidade danificada

Não permitimos apps que falhem, forcem o encerramento, bloqueiem ou, de qualquer outro modo, funcionem incorretamente.
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

> Apps que não instalam.
> Apps que instalam, mas não carregam.
> Apps que carregam, mas com fraca capacidade de resposta.

Outros programas

Além da conformidade com as Políticas de Conteúdos estabelecidas noutras secções deste Centro de Políticas, as apps concebidas para outras experiências Android e distribuídas através do Google Play também podem estar sujeitas a requisitos de política específicos do programa. Certifique-se de que revê a lista abaixo para determinar se alguma destas políticas se aplica à sua app.

Apps instantâneas para Android

O objetivo das Apps instantâneas para Android consiste em criar experiências do utilizador agradáveis e totalmente compatíveis, ao mesmo tempo que respeitam os mais elevados padrões de privacidade e segurança. As nossas políticas foram concebidas para apoiar esse objetivo.

Os programadores que optem por distribuir Apps instantâneas para Android através do Google Play têm de respeitar as seguintes políticas, além de todas as outras Políticas do Programa para programadores do Google Play.

Identidade

Para as apps instantâneas que incluem a funcionalidade de início de sessão, os programadores têm de integrar o Smart Lock para palavras-passe.

Suporte de links

Os programadores de Apps instantâneas para Android têm de fornecer suporte adequado de links para outras apps. Se as apps instantâneas ou as apps instaladas do programador incluírem links que possam redirecionar para uma app instantânea, o programador tem de reencaminhar os utilizadores para essa app instantânea, em vez de, por exemplo, capturar os links numa WebView.

Especificações técnicas

Os programadores têm de cumprir as especificações técnicas das Apps instantâneas para Android e os requisitos fornecidos pela Google, assim como as respetivas modificações periódicas, incluindo os apresentados na nossa documentação pública.

Oferta da instalação de apps

A app instantânea pode oferecer ao utilizador a app passível de instalação, mas esta não deve ser a finalidade principal da app instantânea. Quando oferecerem a instalação, os programadores têm de cumprir os seguintes requisitos:

> Utilizar o ícone "Obter app" do Material Design e a etiqueta "Instalar" para o botão de instalação.
> Não ter mais de 2 ou 3 pedidos de instalação implícitos na respetiva app instantânea.
> Não utilizar uma faixa ou outra técnica semelhante a um anúncio para apresentar um pedido de instalação aos utilizadores.

Pode encontrar detalhes adicionais e diretrizes da experiência do utilizador relacionados com as apps instantâneas nas Práticas recomendadas para a experiência do utilizador.

Alterar o estado do dispositivo

As apps instantâneas não podem efetuar alterações ao dispositivo do utilizador que persistam durante mais tempo do que a sessão da app instantânea. Por exemplo, as apps instantâneas não podem alterar a imagem de fundo do utilizador nem criar um widget do ecrã principal.

Visibilidade das apps

Os programadores têm de assegurar que as apps instantâneas estão visíveis para o utilizador para que este tenha sempre conhecimento de que a app instantânea está em execução no respetivo dispositivo.

Identificadores do dispositivo

As apps instantâneas não estão autorizadas a aceder aos identificadores do dispositivo que (1) persistam após a app instantânea deixar de ser executada e (2) não sejam redefiníveis pelo utilizador. Os exemplos incluem, entre outros:

Número de série da compilação
Endereços Mac de quaisquer chips de rede
IMEI, IMSI

As aplicações instantâneas podem aceder ao número de telefone se este for obtido através da autorização de tempo de execução. O programador não pode tentar identificar o utilizador através destes identificadores ou de qualquer outro meio.

Tráfego de rede

O tráfego de rede proveniente da app instantânea tem de ser encriptado através de um protocolo TLS como o HTTPS.

Famílias

O Google Play disponibiliza uma plataforma avançada para os programadores apresentarem conteúdos de alta qualidade, adequados à idade, para toda a família. Antes de enviar uma aplicação para o programa Concebido para Famílias ou uma aplicação destinada a crianças para a Google Play Store, é responsável por assegurar que a aplicação é adequada para crianças e está em conformidade com todas as leis relevantes.

Saiba mais acerca do processo relativo às famílias e reveja a lista de verificação interativa no portal Academy for App Success.

Conceber apps para crianças e famílias

A utilização de tecnologia como ferramenta para enriquecer as vidas das famílias continua a crescer e os pais procuram conteúdos de alta qualidade seguros para partilharem com as crianças. Pode estar a conceber as suas aplicações especificamente para crianças ou a aplicação pode simplesmente atrair a sua atenção. O Google Play pretende ajudar a assegurar que a sua aplicação é segura para todos os utilizadores, incluindo famílias.

A palavra "crianças" pode significar diferentes coisas em diferentes locais e em diferentes contextos. É importante que consulte o seu representante jurídico para ajudar a determinar as obrigações e/ou as restrições baseadas na idade que podem ser aplicáveis à sua app. Sabe melhor como funciona a sua app, pelo que confiamos em si para nos ajudar a garantir que as apps existentes no Google Play são seguras para as famílias.

As apps concebidas especificamente para crianças têm de participar no programa Concebido para Famílias. No entanto, se as crianças forem apenas um dos públicos-alvo da sua app, a participação no programa Concebido para Famílias não deixa de ser uma ótima forma de a divulgar aos utilizadores certos. Se decidir não participar no programa Concebido para Famílias, continua a ter de agir em conformidade com os requisitos da Política do Google Play para Famílias abaixo, bem como todas as outras Políticas do Programa para programadores do Google Play e o Contrato de Distribuição para Programadores.

Requisitos da Play Console

Público-alvo e conteúdo

Na secção Público-alvo e conteúdo da Google Play Console, tem de indicar o público-alvo da sua app, antes da publicação, através da seleção na lista de faixas etárias fornecidas. Independentemente do que identificar na Google Play Console, se optar por incluir imagens e terminologia na app que possam ser consideradas destinadas a crianças, tal pode afetar a avaliação do Google Play do público-alvo declarado. O Google Play reserva-se o direito de conduzir a sua própria revisão das informações da app fornecidas para determinar se o público-alvo divulgado está correto.

Se selecionar um público-alvo que inclua apenas adultos, mas a Google determinar que não está correto porque a app se destina a crianças e adultos, tem a opção de clarificar os utilizadores de que a app não se destina a crianças ao incluir uma etiqueta de aviso.

Apenas deve selecionar mais de uma faixa etária para o público-alvo da app se tiver concebido a app e assegurado que a mesma é adequada para os utilizadores dentro da(s) faixa(s) etária(s) selecionada(s). Por exemplo, as apps concebidas para bebés, crianças pequenas e crianças em idade pré-escolar devem selecionar apenas "Até 5 anos" como a faixa etária destinada para essas apps. Se a app foi concebida para um ano escolar específico, selecione a

faixa etária que melhor representa esse ano. Apenas deve selecionar faixas etárias que incluam adultos e crianças se tiver concebido a aplicação verdadeiramente para todas as idades.

Atualizações à secção Público-alvo e conteúdo

Pode atualizar as informações da app na secção Público-alvo e conteúdo na Google Play Console sempre que pretender. É necessária uma atualização da app antes de estas informações serem refletidas na Google Play Store. No entanto, quaisquer alterações efetuadas nesta secção da Google Play Console podem ser revistas quanto à conformidade com as políticas mesmo antes de ser enviada uma atualização da app.

Recomendamos vivamente que permita aos utilizadores existentes saberem se alterou a faixa etária de segmentação da aplicação ou começou a utilizar anúncios ou compras na aplicação, através da secção "Novidades" da página da ficha da loja da aplicação ou de notificações na aplicação.

Representação fraudulenta na Play Console

A representação fraudulenta de quaisquer informações sobre a sua app na Play Console, incluindo na secção Público-alvo e conteúdo, pode resultar na remoção ou na suspensão da app, pelo que é importante fornecer informações corretas.

Requisitos da Política para Famílias

Se um dos públicos-alvo da app forem as crianças, tem de agir em conformidade com os requisitos seguintes. O incumprimento destes requisitos pode resultar na remoção ou suspensão da app.

1. Conteúdo da app: o conteúdo da app acessível a crianças tem de ser adequado para as mesmas.
2. Respostas da Google Play Console: tem de responder com precisão às perguntas na Google Play Console acerca da app e atualizar essas respostas para refletir de forma precisa quaisquer alterações à mesma.
3. Anúncios: se a app apresentar anúncios a crianças ou utilizadores de idade desconhecida, tem de:
    utilizar apenas SDKs de anúncios certificados pelo Google Play para apresentar anúncios a esses utilizadores;
    assegurar que os anúncios apresentados a esses utilizadores não envolvem remarketing ou publicidade baseada em interesses;
    assegurar que os anúncios apresentados a esses utilizadores mostram conteúdo adequado para crianças;
    assegurar que os anúncios apresentados a esses utilizadores seguem os requisitos de formato de anúncio para Famílias; e
    assegurar a conformidade com todos os regulamentos legais e as normas da indústria aplicáveis relativos à publicidade para crianças.

4. Recolha de dados: tem de divulgar a recolha de quaisquer informações pessoais e confidenciais de crianças na sua app, incluindo através de APIs e SDKs chamados ou utilizados na mesma. As informações confidenciais de crianças incluem, entre outras, informações de autenticação, dados do microfone e do sensor da câmara, dados do dispositivo, ID Android, dados de utilização de anúncios e ID de publicidade.
5. APIs e SDKs: tem de assegurar que a app implementa corretamente quaisquer APIs e SDKs.

    As apps destinadas unicamente a crianças não podem conter APIs ou SDKs não aprovados para utilização em serviços dirigidos a crianças. Isto inclui o Início de sessão do Google (ou qualquer outro serviço de APIs do Google que aceda aos dados associados a uma Conta Google), os serviços de jogos do Google Play e qualquer outro serviço de API com tecnologia OAuth para autenticação e autorização.

    As apps destinadas a crianças e públicos-alvo mais velhos não devem implementar APIs ou SDKs não aprovados para utilização em serviços dirigidos a crianças, exceto se forem utilizados atrás de um ecrã de idade neutro ou implementados de uma forma que não resulte na recolha de dados de crianças (por exemplo, fornecer o Início de sessão do Google como funcionalidade opcional). Tenha em atenção que todos os utilizadores têm de conseguir aceder à app e a uma parte razoável da respetiva funcionalidade.
6. Política de privacidade: tem de fornecer um link para a política de privacidade da app na respetiva página da Ficha da loja. Este link tem de ser sempre mantido enquanto a app estiver disponível na loja e tem de ser um link para uma política de privacidade que, entre outros aspetos, descreva com precisão a recolha e a utilização de dados da app.
7. Restrições especiais:

    Se a app utilizar a Realidade aumentada, tem de incluir um aviso de segurança imediatamente após o lançamento da secção Realidade aumentada. O aviso deve conter o seguinte:

        Uma mensagem adequada acerca da importância da supervisão parental.
        Um lembrete para ter cuidado com os perigos físicos no mundo real (por exemplo, ter cuidado com a área envolvente).

    A app não pode exigir a utilização de um dispositivo não aconselhado para crianças (por exemplo, Daydream, Oculus).
8. Conformidade com a lei: tem de assegurar que a sua app, incluindo quaisquer APIs ou SDKs chamados ou utilizados pela mesma, está em conformidade com a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA, Regulamento Geral sobre a Proteção de Dados (RGPD) da UE e quaisquer outros regulamentos ou leis aplicáveis.

Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

Apps que promovam jogos para crianças na Ficha da loja, mas cujo conteúdo apenas é adequado para adultos.

Apps que implementem APIs com termos de utilização que proíbem a respetiva utilização em apps dirigidas a crianças.
Aplicações que destaquem o uso de álcool, tabaco ou substâncias regulamentadas.
Apps que incluam jogos de azar reais ou simulados.
Apps que incluam violência, sanguinolência ou conteúdo chocante não adequado para crianças.
Apps que fornecem serviços de encontros ou oferecem conselhos sexuais ou matrimoniais.
Apps que mostrem anúncios não apropriados para menores a crianças.

Programa Concebido para Famílias

As apps concebidas especificamente para crianças têm de participar no programa Concebido para Famílias. Se a sua app for concebida para todos, incluindo crianças e famílias, também se pode candidatar a participar no programa.

Para ser aceite no programa, a sua app tem de cumprir todos os requisitos da Política para Famílias e de elegibilidade do Concebido para Famílias, para além dos critérios definidos nas Políticas do Programa para programadores do Google Play e Contrato de Distribuição para Programadores.

Para mais informações acerca do processo de envio da sua app para inclusão no programa, clique aqui.

Elegibilidade para o programa

Todas as aplicações incluídas no programa Concebido para Famílias têm de ter conteúdo da aplicação e do anúncio relevante e adequado para crianças e têm de satisfazer todos os requisitos abaixo. As aplicações aceites no programa Concebido para Famílias têm de permanecer em conformidade com todos os requisitos do programa. O Google Play reserva-se o direito de rejeitar ou de remover, por seu critério exclusivo, qualquer aplicação que seja considerada imprópria para o programa Concebido para Famílias.

Requisitos do programa Concebido para Famílias

1. As apps têm de incluir a classificação Todos ou Todos com mais de 10 anos da ESRB, ou uma classificação equivalente.
2. Tem de divulgar com precisão os elementos interativos da app no Questionário de classificação de conteúdo na Google Play Console, incluindo:
    - se os utilizadores podem interagir ou trocar informações;
    - se a aplicação partilha informações pessoais dos utilizadores com terceiros; e
    - se a app partilha a localização física do utilizador com outros utilizadores.
3. Se a sua app utilizar a API do Android Speech, tem de definir RecognizerIntent.EXTRA_CALLING_PACKAGE para o respetivo PackageName.
4. As apps só podem utilizar SDKs de anúncios certificados pelo Google Play.

5. As apps concebidas especificamente para crianças não podem solicitar autorizações de acesso à localização.
6. As apps têm de utilizar o Gestor de dispositivos associados (CDM) quando solicitarem o Bluetooth, exceto se a app se destinar apenas a versões do sistema operativo (SO) do dispositivo não compatíveis com o CDM.

Seguem-se alguns exemplos de apps comuns que não são elegíveis para o programa:

Apps com classificação Todos da ESRB, mas com anúncios de conteúdo de jogos de azar.
Apps para pais ou cuidadores (por exemplo, controlador de amamentação e guia de desenvolvimento).
Guias parentais ou apps de gestão de dispositivos apenas destinadas a serem utilizadas por pais ou cuidadores.

Categorias

Se for aceite para participar no programa Concebido para Famílias, pode escolher uma segunda categoria específica para famílias que descreva a sua app. Seguem-se as categorias disponíveis para as apps que participam no programa Concebido para Famílias:

Ação e aventura: apps/jogos de ação, incluindo jogos de corridas, aventuras de contos de fadas e outros jogos e apps concebidos para criar entusiasmo.

Quebra-cabeças: jogos que façam o utilizador pensar, incluindo puzzles, jogos de combinações, questionários e outros jogos que desafiem a memória, a inteligência ou a lógica.

Criatividade: apps e jogos que estimulem a criatividade, incluindo apps de desenho, pintura, programação e outros jogos e apps em que seja possível construir algo.

Educação: apps e jogos concebidos com dados de especialistas em aprendizagem (por exemplo, educadores, especialistas e investigadores) que promovem a aprendizagem, incluindo a aprendizagem académica, socioemocional, física e criativa, bem como a aprendizagem relacionada com aptidões básicas para a vida, pensamento crítico e resolução de problemas.

Música e vídeo: apps e jogos com uma componente musical ou de vídeo, incluindo apps de simulação de instrumentos e apps que fornecem conteúdo de vídeo e áudio musical.

Simulação: apps e jogos em que o utilizador pode desempenhar um papel, por exemplo, fingir ser um cozinheiro, um cuidador, um príncipe ou uma princesa, um bombeiro, um polícia ou uma personagem fictícia.

Anúncios e rentabilização

As políticas abaixo aplicam-se a qualquer tipo de publicidade (incluindo nas suas apps e em apps de terceiros), ofertas de compras na app ou qualquer outro conteúdo comercial (como posicionamentos de produtos pagos) apresentado aos utilizadores de apps sujeitas aos

requisitos da Política para Famílias e/ou aos requisitos do programa Concebido para Famílias. A publicidade, as ofertas de compras na aplicação e o conteúdo comercial nestas aplicações têm de estar em conformidade com as leis e os regulamentos aplicáveis (incluindo quaisquer diretrizes da indústria ou de autorregulação relevantes).

O Google Play reserva-se o direito de fazer cumprir as apps relativamente a táticas comerciais demasiado agressivas.

Requisitos de formato de anúncio

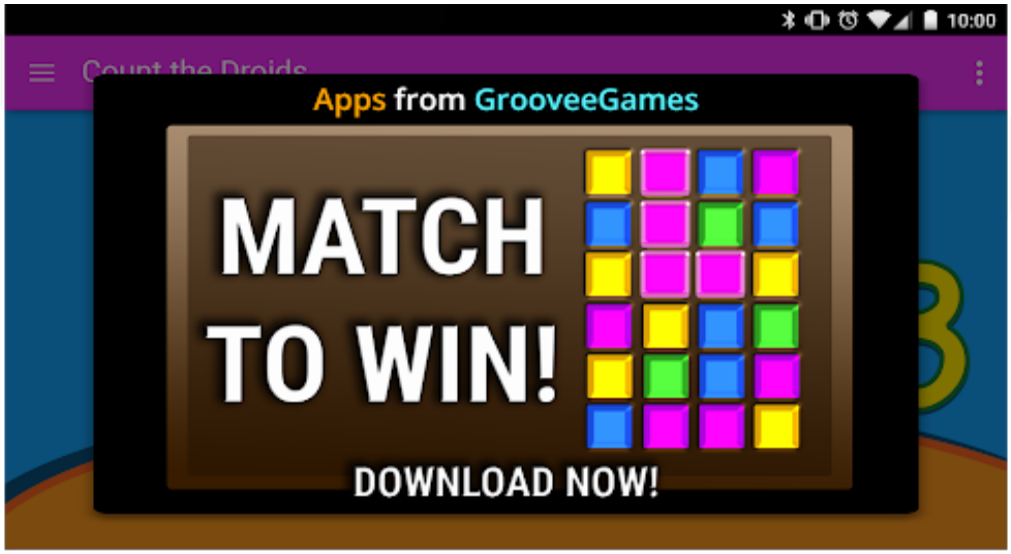
Os anúncios e as ofertas de compras na app não podem ter conteúdo fraudulento ou concebido de forma a provocar cliques inadvertidos de crianças. É proibido o seguinte:

- A utilização de murais de anúncios.
- Anúncios que interfiram com a utilização normal da app e que não possam ser fechados após 5 segundos.
- Anúncios intercalares ou ofertas de compras na app apresentadas imediatamente após o lançamento da app.
- Vários posicionamentos de anúncios numa página
- Anúncios ou ofertas de compras na app que não sejam facilmente distinguíveis do conteúdo da app.
- A utilização de táticas chocantes ou emocionalmente manipulativas para incentivar a visualização de anúncios ou as compras na app.
- Não fazer uma distinção entre a utilização de moedas de jogo virtuais e dinheiro real para efetuar compras na app.

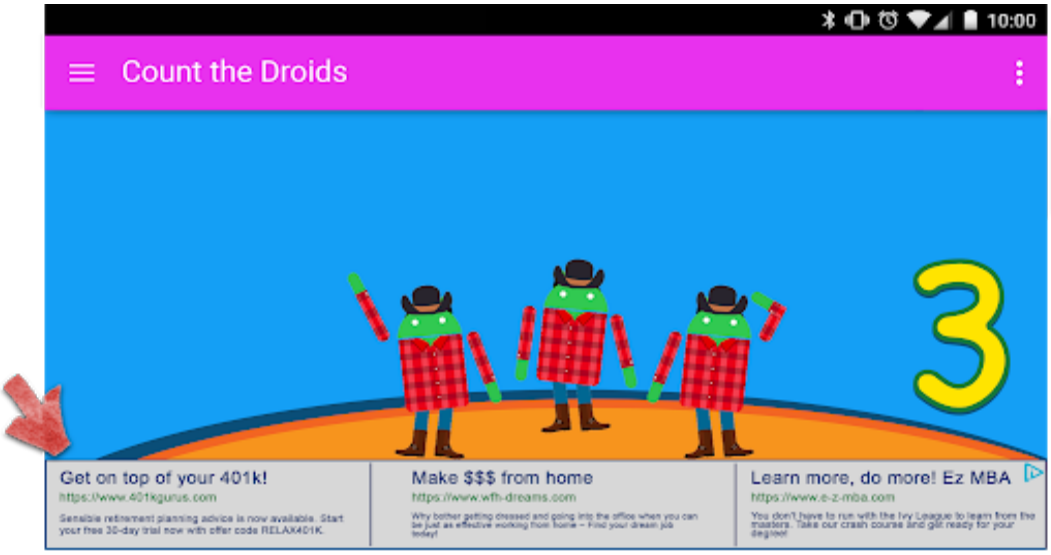
Para manter a segurança e o respeito no Google Play, criámos normas que definem e proíbem conteúdo nocivo e impróprio para os utilizadores.

- Anúncios que se afastam do dedo do utilizador à medida que este os tenta fechar.

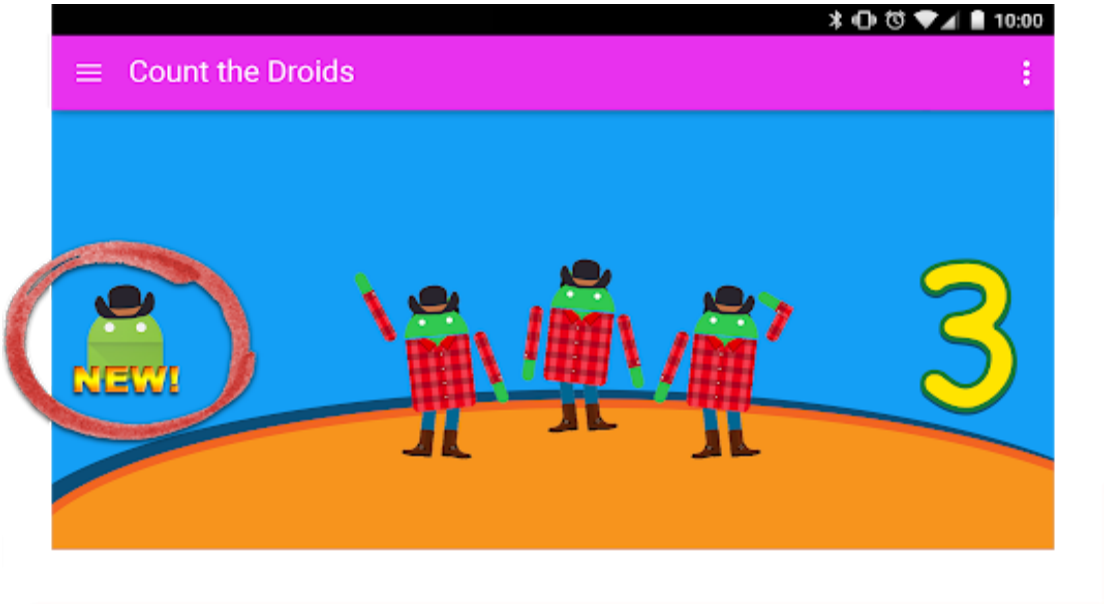
Anúncios que ocupam a maior parte ou todo o ecrã do dispositivo sem fornecer ao utilizador uma forma clara de os ignorar, conforme mostrado no exemplo abaixo:



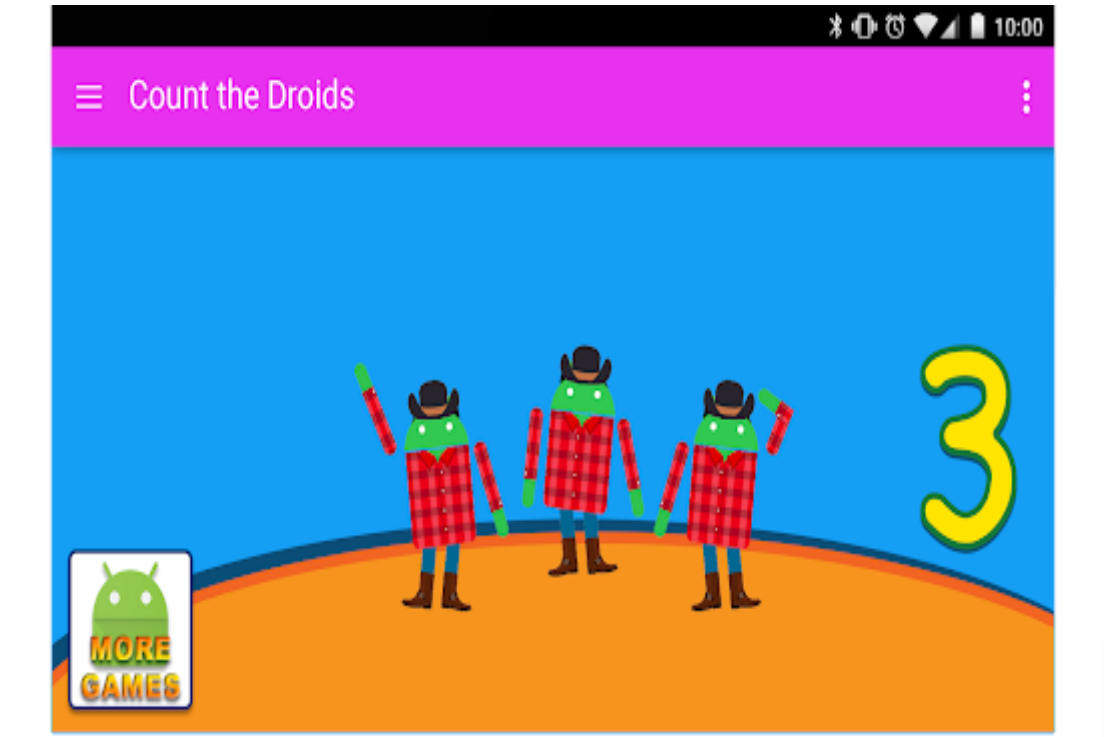
Anúncios de faixa com várias ofertas, conforme mostrado no exemplo abaixo:



Anúncios que podem ser confundidos pelo utilizador com o conteúdo da app, conforme mostrado no exemplo abaixo:



Botões ou anúncios que promovem as suas outras Fichas da loja do Google Play, mas que não se distinguem do conteúdo da app, conforme mostrado no exemplo abaixo:



Seguem-se alguns exemplos de conteúdo de anúncios impróprios que não deve ser apresentado a crianças.

Conteúdo multimédia impróprio: anúncios de programas de TV, filmes, álbuns de música ou quaisquer outros meios de comunicação que não sejam adequados para crianças.
Jogos de vídeo impróprios e software transferível: anúncios de software transferível e videojogos eletrónicos que não sejam adequados para crianças.
Substâncias controladas ou prejudiciais: anúncios de álcool, tabaco, substâncias controladas ou quaisquer outras substâncias prejudiciais.
Jogos de azar: anúncios de jogos de azar simulados, de concursos ou de promoções de apostas, mesmo se a participação for gratuita.
Conteúdo para adultos e com conotação sexual: anúncios com conteúdo sexual, com conotação sexual e não apropriado para menores.
Namoro ou relações: anúncios de sites de namoro ou relacionamentos para adultos.
Conteúdo violento: anúncios com conteúdo violento e explícito não adequado para crianças.

SDKs de anúncios

Só pode utilizar SDKs de anúncios certificados pelo Google Play para publicar anúncios para crianças. As apps no programa Concebido para Famílias apenas podem utilizar SDKs de anúncios certificados pelo Google Play. Para as apps também destinadas a utilizadores adultos, pode utilizar SDKs de anúncios não certificados se existir um ecrã de idade neutro na app e utilizar SDKs de anúncios não certificados apenas para publicar anúncios para utilizadores adultos conhecidos.

Consulte a Política do Programa de Anúncios para Famílias para obter mais detalhes acerca destes requisitos e ver a lista atual de SDKs de anúncios aprovados.

Se utilizar o AdMob, consulte o Centro de Ajuda do AdMob para obter mais informações acerca dos respetivos produtos.

É da sua responsabilidade assegurar que a sua app satisfaz todos os requisitos relativos a publicidade, compras na app e conteúdo comercial. Contacte o(s) fornecedor(es) do SDK de anúncios para saber mais acerca das respetivas políticas de conteúdos e práticas de publicidade.

Compras na app

O Google Play irá autenticar novamente todos os utilizadores antes de quaisquer compras na aplicação em aplicações aderentes ao programa Concebido para Famílias. Esta medida serve para ajudar a garantir que a entidade financeiramente responsável, e não as crianças, está a aprovar as compras.

Aplicação

Evitar a violação de uma política é sempre melhor do que fazer a sua gestão, mas quando as violações realmente ocorrem, empenhamo-nos em garantir que os programadores compreendem como podem fazer com que a sua app fique em conformidade. Informe-nos se vir quaisquer violações ou tiver dúvidas acerca de como gerir uma violação.

Abrangência das políticas

As nossas políticas aplicam-se a qualquer conteúdo que a sua app apresente ou para o qual estabeleça ligação, incluindo quaisquer anúncios que apresente aos utilizadores e qualquer conteúdo alojado gerado pelo utilizador ou para o qual estabeleça ligação. Além disso, aplicam-se a qualquer conteúdo da sua conta de programador cuja visualização seja pública no Google Play, incluindo o seu nome de programador e a página de destino do Website do programador fornecido.

Não são permitidas apps que levem os utilizadores a instalar outras apps nos respetivos dispositivos. As apps que fornecem acesso a outras apps, jogos ou software sem instalação, incluindo funcionalidades e experiências fornecidas por terceiros, têm de garantir que todo o conteúdo a que fornecem acesso cumpre todas as Políticas do Google Play e pode ainda estar sujeito a revisões de políticas adicionais.

Os termos definidos utilizados nestas políticas têm o mesmo significado que no Contrato de Distribuição para Programadores (DDA). Além de estar em conformidade com estas políticas e o DDA, o conteúdo da sua app tem de ser classificado de acordo com as nossas Diretrizes de classificação de conteúdo.

As apps que possam ser impróprias para um público-alvo geral ou que resultem numa experiência de má qualidade para os nossos utilizadores finais podem não ser elegíveis para promoção no Google Play. No entanto, desde que estejam em conformidade com estas políticas e o DDA, essas apps permanecem disponíveis no Google Play.

A Google reserva-se o direito de incluir ou remover apps do Google Play. Podemos efetuar ações com base em vários fatores que incluem, entre outros, um padrão de comportamento prejudicial ou elevado risco de abuso. Identificamos o risco de abuso através de vários itens, como o histórico de violações anteriores, o feedback dos utilizadores e a utilização de marcas, personagens e outros recursos populares.

Processo de aplicação

Se a sua app violar alguma das nossas políticas, é removida do Google Play e o programador recebe uma notificação por email com o motivo específico da remoção. Violações repetidas ou graves (como software malicioso, fraude e apps que possam provocar danos no dispositivo ou prejuízos para o utilizador) destas políticas ou do Contrato de Distribuição para Programadores (DDA) resultam no encerramento das contas individuais ou relacionadas.

Tenha em atenção que os avisos de remoção ou administrativos podem não indicar absolutamente todas as violações de políticas existentes na sua app ou no catálogo de apps mais abrangente. Os programadores são responsáveis por solucionarem qualquer problema sinalizado relativo às políticas e por aplicarem as devidas diligências adicionais para garantir que o restante da aplicação está totalmente em conformidade com as políticas. Se as violações não forem solucionadas, podem ser tomadas ações de aplicação adicionais, incluindo a remoção permanente da app ou o encerramento da conta.

Gestão e denúncia de violações de políticas

Se tiver dúvidas ou preocupações relativamente a uma remoção ou classificação/comentário de um utilizador, pode consultar os recursos abaixo ou contactar-nos através do Centro de Ajuda do Google Play. No entanto, não lhe podemos disponibilizar aconselhamento legal. Se necessitar de aconselhamento legal, deve contactar um consultor jurídico.

Verificação de apps e recursos
Denuncie a violação de uma política
Contacte o Google Play acerca do encerramento de uma conta ou da remoção de uma app
Avisos cordiais
Denuncie apps e comentários impróprios
A minha app foi removida do Google Play
Compreender o encerramento de contas de programador do Google Play

Developer Distribution Agreement