Google Developer Policy - April 16, 2020

Juntos, podemos criar a plataforma de apps e jogos mais confiável do mundo

Sua inovação impulsiona o sucesso de todos nós. No entanto, esse sucesso traz responsabilidades. As Políticas do programa para desenvolvedores e o Contrato de distribuição do desenvolvedor garantem que nossa parceria continue a oferecer os apps mais inovadores e confiáveis do mundo a mais de um bilhão de pessoas no Google Play. Conheça nossas políticas abaixo ou na visualização de impressão.

Pessoas de todo o mundo usam o Google Play para acessar apps e jogos todos os dias. Antes de enviar um app, verifique se ele é adequado para o Google Play e se está em conformidade com as legislações locais.

Conteúdo prejudicial a crianças

Apps com conteúdo que sexualiza menores de idade estão sujeitos à remoção imediata da Play Store. Não são permitidos apps com atratividade para crianças, mas que apresentam temas adultos.

Se tomarmos conhecimento de conteúdo com imagens de abuso sexual infantil, isso será denunciado às autoridades competentes, e as Contas do Google dos envolvidos com a distribuição desse conteúdo serão excluídas.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Conteúdo sexual

Não permitimos apps que tenham ou promovam conteúdo sexual, como pornografia, nem qualquer conteúdo ou serviços com o objetivo de gerar satisfação sexual. O conteúdo com nudez poderá ser permitido se for principalmente para fins educacionais, documentais, científicos ou artísticos, e não apenas uma exposição sem justificativa.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Representações de nudez em que há pessoas nuas ou seminuas e em que a roupa seria inadequada em um contexto público adequado
- Representações, animações ou ilustrações de atos sexuais ou poses sexualmente sugestivas.
- Conteúdo que retrate acessórios sexuais e de fetiche.
- Conteúdo obsceno ou de linguagem obscena
- Conteúdo que retrate, descreva ou incentive a bestialidade
- Apps que promovam entretenimento relacionado a sexo, serviços de acompanhantes ou outros serviços que possam ser interpretados como fornecimento de atos sexuais em troca de uma remuneração

Discurso de ódio

Não são permitidos apps que promovam a violência ou incitem ódio contra indivíduos ou grupos com base em raça ou origem étnica, religião, deficiência, idade, nacionalidade, condição de veterano, orientação sexual, gênero, identidade de gênero ou outras características associadas à discriminação sistêmica ou à marginalização.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Compilações de afirmações destinadas a provar que um grupo protegido é desumano, inferior ou digno de ser odiado
- Os apps que contêm teorias sobre um grupo protegido ter características negativas (por exemplo, ser mal-intencionado, corrupto, maligno etc.) ou que, afirmam, explícita ou implicitamente, que o grupo é considerado uma ameaça.
- Conteúdo ou discurso que incentive os outros a acreditar que pessoas devem ser odiadas ou discriminadas porque são membros de um grupo protegido

Violência

Não são permitidos apps que retratem ou promovam violência gratuita ou outras atividades perigosas.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- São proibidas as representações gráficas ou descrições de violência realista ou ameaças violentas a qualquer pessoa ou animal.
- Não são permitidos apps que promovam automutilação, suicídio, transtornos alimentares, jogos de asfixia nem outras ações que podem resultar em ferimentos graves ou morte.

Conteúdo terrorista

Não permitimos que organizações terroristas publiquem apps no Google Play para nenhum propósito, incluindo recrutamento.

Não são permitidos apps com conteúdo relacionado a terrorismo, como a promoção de atos terroristas, a incitação à violência ou a glorificação de ataques terroristas. Se você postar algum conteúdo relacionado a terrorismo para fins educacionais, documentais, científicos ou artísticos, forneça informações suficientes para que os usuários entendam o contexto.

Eventos controversos

Não são permitidos apps que tratem desastres naturais, atrocidades, conflitos, mortes ou outros eventos trágicos com pouca sensibilidade ou gerem lucro com esses acontecimentos. Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Insensibilidade em relação à morte de uma ou mais pessoas reais devido a suicídio, overdose, causas naturais etc.
- Negação de um evento trágico de grandes proporções
- Lucro aparente com um evento trágico sem benefício perceptível para as vítimas

Bullying e assédio

Não são permitidos apps que tenham ou promovam ameaças, assédio ou bullying.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Bullying com vítimas de conflitos internacionais ou religiosos
- Conteúdo com o objetivo de explorar pessoas, incluindo extorsão, chantagem etc.
- Postagem de conteúdo para humilhar um indivíduo publicamente
- Assédio a vítimas de um evento trágico ou a amigos e familiares dessas pessoas

Produtos perigosos

Não permitimos apps que possibilitem a venda de explosivos, armas de fogo, munição nem determinados acessórios para armas de fogo.

- Os acessórios restritos incluem aqueles que permitem que uma arma de fogo simule acionamento automático ou seja convertida em uma arma automática (por exemplo, coronhas com amortecimento, gatilhos com sistema Gatling, encaixes para trava de gatilho automática ou kits de conversão), além de carregadores ou cintas com mais de 30 cartuchos.

Não são permitidos apps que fornecem instruções para a fabricação de explosivos, armas de fogo, munição, acessórios restritos para armas de fogo ou outras armas. Isso inclui instruções sobre como converter uma arma de fogo para simulação ou uso de acionamento automático.

Maconha

Não permitimos apps que facilitem a venda de maconha ou produtos derivados, independentemente da legalidade da substância.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Permitir que os usuários solicitem maconha por meio de um recurso de carrinho de compras no app
- Ajudar os usuários a organizar a entrega ou a retirada de maconha.
- Facilitar a venda de produtos que contêm THC

Tabaco e bebidas alcoólicas

Não são permitidos apps que facilitem a venda de tabaco (incluindo cigarros eletrônicos) ou incentivem o uso irresponsável dessas substâncias ou de bebidas alcoólicas.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Descrever ou incentivar o uso ou a venda de bebidas alcoólicas ou tabaco a menores
- Sugerir que o consumo de tabaco pode melhorar o comportamento social, sexual, profissional, intelectual ou atlético.
- Retratar o uso excessivo de bebidas alcoólicas de maneira favorável, incluindo a representação de consumo compulsivo ou de competições

Não permitimos apps que exponham os usuários a produtos e serviços financeiros enganosos e nocivos.

Para os fins desta política, são considerados produtos e serviços financeiros aqueles que estão relacionados ao gerenciamento e investimento de moedas e criptomoedas, incluindo consultoria personalizada.

Caso seu app tenha ou promova produtos e serviços financeiros, ele precisará estar em conformidade com as regulamentações estaduais e locais de todos os países ou regiões a que ele é destinado. Por exemplo, inclua a divulgação de informações específicas exigidas pela legislação local.

Opções binárias

Não são permitidos apps que ofereçam aos usuários a capacidade de negociar opções binárias.

Criptomoedas

Não são permitidos apps que mineram criptomoeda nos dispositivos. Permitimos apps que gerenciam remotamente a mineração de criptomoeda.

Empréstimos pessoais

Definimos os empréstimos pessoais como a concessão de crédito em dinheiro por um indivíduo, organização ou entidade a um consumidor individual de modo não recorrente e sem o propósito de financiamento estudantil ou compra de um ativo fixo. Os consumidores de empréstimos pessoais precisam de informações sobre a qualidade, as características, as taxas, os riscos e as vantagens desses produtos para tomar decisões conscientes sobre a possibilidade de assumir o empréstimo.

> Alguns exemplos disso são os empréstimos pessoais, consignados, P2P (peer-to-peer) e com alienação da propriedade.
> Não estão incluídos: hipotecas, financiamentos de carros, financiamentos estudantis e linhas de crédito rotativo, como cartões de crédito ou linhas de crédito pessoal.

Os apps de empréstimo pessoal precisam divulgar as seguintes informações nos próprios metadados:

> Períodos mínimo e máximo para quitação
> A taxa percentual anual (APR, na sigla em inglês) máxima, que geralmente inclui juros, taxas e outros custos por um ano, ou outra taxa similar calculada de acordo com a legislação local
> Um exemplo representativo do custo total do empréstimo, incluindo todas as taxas aplicáveis

Não são permitidos apps de empréstimo pessoal que exijam quitação em até 60 dias a partir da data de emissão. Definimos esse serviço como "empréstimo pessoal de curto prazo". A política se aplica aos apps que oferecem empréstimos de maneira direta, aos geradores de leads e aos que conectam consumidores a credores terceirizados.

Empréstimos pessoais com APRs altas

Nos Estados Unidos, não são permitidos apps de concessão de empréstimo pessoal em que a taxa percentual anual (APR, na sigla em inglês) seja igual ou maior que 36%. Os apps de empréstimo pessoal nos Estados Unidos precisam exibir a APR máxima, calculada de maneira consistente com a lei de transparência em empréstimos Truth in Lending Act (TILA).

A política se aplica aos apps que oferecem empréstimos de maneira direta, aos geradores de leads e aos que conectam consumidores a credores terceirizados.

Jogos de azar

Permitimos conteúdo, serviços e anúncios que promovam jogos de azar on-line, desde que eles atendam a requisitos específicos. Permitimos também apps de fantasy sports por rodada (DFS, na sigla em inglês) que atendam a determinados requisitos.

Apps de jogos de azar

Permitidos somente na França, na Irlanda e no Reino Unido no momento

É permitido utilizar conteúdos e serviços que promovam jogos de azar on-line, desde que eles atendam aos seguintes requisitos:

- O desenvolvedor precisa passar pelo processo de inscrição para distribuir o app no Google Play.
- O app precisa obedecer a todas as leis e padrões do setor aplicáveis dos países em que é distribuído.
- O desenvolvedor precisa ter uma licença de jogo válida para cada país onde o app é distribuído.
- O app precisa impedir que usuários menores de idade participem de jogos de azar no app.
- O app precisa impedir o uso em países que não são cobertos pela licença de jogo fornecida pelo desenvolvedor.
- O app NÃO pode ser publicado como pago no Google Play nem usar o Faturamento do Google Play no app.
- O app precisa ser gratuito para download e instalação na Play Store.
- O app precisa ter a classificação "SA" (Somente adultos) ou equivalente pela Coalizão Internacional de Classificação Etária (IARC, na sigla em inglês).
- O app e os detalhes correspondentes precisam mostrar informações claras sobre a participação responsável em jogos de azar.

Em todos os outros locais, não é permitido usar conteúdos nem serviços que promovam jogos de azar on-line, incluindo, entre outros, cassinos on-line, loterias e apostas esportivas, assim como jogos de habilidade que ofereçam prêmios em dinheiro ou outros itens de valor.

Anúncios de jogos de azar em apps distribuídos pelo Google Play

É permitido utilizar anúncios que promovam jogos de azar on-line, desde que eles atendam aos seguintes requisitos:

- O app, o anúncio e os anunciantes de jogos de azar precisam obedecer a todas as leis e padrões do setor aplicáveis em qualquer local onde o anúncio de jogos de azar seja exibido.
- O anúncio precisa atender aos requisitos locais de licenciamento para todos os produtos e serviços promovidos que sejam relacionados com jogos de azar.
- O app não pode exibir anúncios de jogos de azar para menores de 18 anos.
- O app não pode estar inscrito no programa Feito para família.
- O app não pode segmentar pessoas menores de 18 anos.

O anúncio precisa mostrar claramente informações sobre como participar de jogos de azar de maneira responsável na página de destino, nos detalhes do app anunciado ou no próprio app.
O app com anúncios de jogos de azar não pode ser um simulador de jogos de azar (um jogo de entretenimento que não envolve apostas com dinheiro real).

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

O app "KIDS 123" tem um anúncio promovendo serviços de jogos de azar

Apps de fantasy sports por rodada (DFS, na sigla em inglês)

São permitidos apps de fantasy sports por rodada (DFS), desde que atendam aos seguintes requisitos:

O app só pode permitir o acesso e ser distribuído nos Estados Unidos. Os apps de DFS para jurisdições fora dos EUA precisam comprovar qualificação por meio do processo para apps de jogos de azar com dinheiro real.
O desenvolvedor precisa passar pelo processo de inscrição para DFS e ser aceito para distribuir o app no Google Play.
O app precisa obedecer a todas as leis e a todos os padrões do setor aplicáveis dos estados ou territórios dos EUA em que é distribuído.
O desenvolvedor precisa ter uma licença válida para cada estado ou território dos EUA que exija licença para apps de DFS.
O app precisa impedir que usuários menores de idade apostem ou façam transações monetárias por meio dele.
O app precisa impedir o uso em estados ou territórios dos EUA em que o desenvolvedor não tem a licença necessária para apps de DFS.
O app precisa impedir o uso em estados ou territórios dos EUA em que apps de DFS são ilegais.
O app NÃO pode ser publicado como pago no Google Play nem usar o Faturamento do Google Play no app.
O app precisa ser gratuito para download e instalação na Play Store.
O app precisa ter a classificação "SA" (Somente adultos) ou equivalente pela Coalizão Internacional de Classificação Etária (IARC, na sigla em inglês).
O app e os detalhes correspondentes precisam mostrar informações claras sobre a participação responsável em jogos de azar.

Apps que facilitem ou promovam atividades ilícitas não são permitidos.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Facilitar a venda ou compra de drogas ilícitas ou medicamentos sem receita médica

Descrever ou incentivar o uso ou a venda de drogas, álcool ou tabaco para menores.
Instruções para o cultivo ou fabricação de drogas ilícitas

Conteúdo gerado pelo usuário

O conteúdo gerado pelo usuário (UGC, na sigla em inglês) são as contribuições dos usuários para o app que ficam visíveis ou acessíveis para pelo menos um subconjunto de usuários. O conteúdo questionável é aquele que viola nossas políticas.

Os apps que contêm ou exibem UGC precisam:

exigir que os usuários aceitem os Termos de Uso e/ou a política do usuário do app antes de criarem ou fazerem o upload de UGC;
definir, de maneira compatível com o espírito das políticas do programa de desenvolvedores do Google Play, o UGC questionável e proibido por meio dos Termos de Uso e/ou da política do usuário do app;
implementar uma moderação de UGC robusta, eficaz e contínua, de maneira razoável e compatível com os tipos de UGC hospedados pelo app;
fornecer no app um sistema fácil de usar para denúncia e remoção de UGC questionável;
    no caso de apps de transmissão ao vivo, o UGC problemático precisa ser removido o mais próximo possível do tempo real;
remover ou bloquear usuários abusivos que violem os Termos de Uso e/ou a política do usuário do app;
fornecer salvaguardas para evitar que a monetização no app incentive o comportamento questionável do usuário.

Os apps que tiverem como função principal a exibição de UGC questionável serão removidos do Google Play. Da mesma forma, os apps usados principalmente para hospedar UGC questionável ou que tiverem reputação entre os usuários de ser um local para esse tipo de conteúdo também serão removidos do Google Play.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Promoção de conteúdo sexualmente explícito gerado pelo usuário, incluindo a implementação de recursos pagos que incentivam principalmente o compartilhamento de conteúdo censurável
Apps que tenham conteúdo gerado pelo usuário (UGC, na sigla em inglês) e que não tenham salvaguardas suficientes contra ameaças, assédio ou bullying, especialmente voltados a menores
Postagens, comentários ou fotos em um app que tenham como objetivo principal assediar ou expor outra pessoa a abuso, ataque malicioso ou deboche

Apps que não atendam às reclamações dos usuários sobre conteúdo questionável

O Google Play não permite apps que promovam ou vendam substâncias não aprovadas, independentemente de qualquer declaração de legalidade. Exemplos:

- Todos os itens desta lista não exaustiva de suplementos e produtos farmacêuticos proibidos
- Produtos com éfedra
- Produtos com gonadotrofina coriônica humana (hCG) destinados à perda ou ao controle de peso ou promovidos em conjunto com esteroides anabolizantes
- Suplementos herbáceos e dietéticos com componentes farmacêuticos ativos ou ingredientes perigosos
- Declarações falsas ou enganosas sobre saúde, incluindo afirmações que implicam que um produto tem a mesma eficácia de substâncias controladas ou medicamentos vendidos sob prescrição médica
- Promoção de produtos não aprovados pelo governo implicando que eles são seguros e eficazes para a prevenção, cura ou tratamento de doenças ou problemas de saúde específicos
- Produtos sujeitos a qualquer aviso ou ação regulamentar ou governamental
- Produtos com nomes muito semelhantes a uma substância farmacêutica, suplemento ou substância controlada não aprovada

Para informações adicionais sobre os suplementos e produtos farmacêuticos reprovados ou enganosos que nós monitoramos, acesse www.legitscript.com.

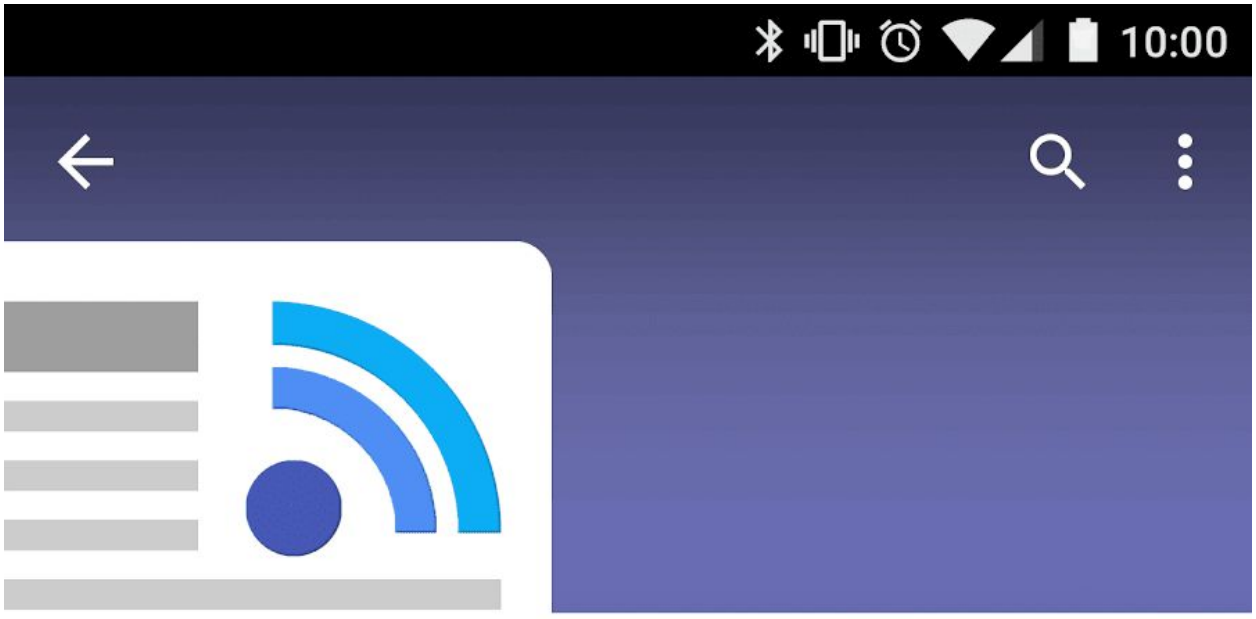
Falsificação de identidade e propriedade intelectual

Quando desenvolvedores copiam o trabalho de outros ou enganam os usuários, isso é prejudicial tanto para os usuários quanto para a comunidade de desenvolvedores. Não use o trabalho de outras pessoas de maneira enganosa ou injusta.

Falsificação de identidade

Não são permitidos apps que usem a marca, o título, o logotipo ou o nome de outro app ou entidade para enganar os usuários. Não tente sugerir uma associação ou relação com outra entidade quando não houver uma. A falsificação de identidade poderá ocorrer mesmo se não houver intenção de enganar. Portanto, tome cuidado ao mencionar marcas que não lhe pertencem. Isso se aplica mesmo a marcas que não estejam presentes no Google Play.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Desenvolvedores que sugerem uma afiliação falsa 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 do desenvolvedor listado para este app sugere uma relação oficial com o Google, apesar de tal relação não existir.
Títulos e ícones de apps que são tão semelhantes aos de produtos ou serviços existentes que podem enganar os usuários:

Apps que alegam falsamente ser o app oficial de uma entidade estabelecida. Títulos como "App oficial do Justin Bieber" não são permitidos sem os direitos ou as permissões necessárias.
Apps que violam as Diretrizes da marca Android.

Propriedade intelectual

Não são permitidos apps ou contas de desenvolvedor que violam direitos de propriedade intelectual de outras pessoas (incluindo marcas registradas, direitos autorais, patentes, segredos comerciais e outros direitos de propriedade). Também são proibidos os apps que incentivam a violação de direitos de propriedade intelectual ou levam a esse tipo de infração.

Responderemos a notificações claras de suposta violação de direitos autorais. Para receber mais informações ou preencher uma solicitação da DMCA, visite nossa página de procedimentos sobre direitos autorais.

Para enviar uma reclamação sobre a venda ou promoção de produtos falsificados em um app, envie um aviso de falsificação.

Se você for proprietário de uma marca registrada e acreditar que há um app no Google Play que viole seus direitos de marca registrada, entre em contato diretamente com o desenvolvedor para resolver o problema. Se não for possível chegar a uma solução, envie uma reclamação de marca registrada por meio deste formulário.

Se você tiver documentação por escrito comprovando sua permissão para usar a propriedade intelectual de terceiros no app ou na página "Detalhes do app" (como nomes de marcas,

logotipos e recursos gráficos), entre em contato com a equipe do Google Play antes do envio para garantir que o app não seja rejeitado por violação de propriedade intelectual.

Uso não autorizado de conteúdo protegido por direitos autorais

Apps que violem direitos autorais não são permitidos. Modificar conteúdo protegido por direitos autorais ainda pode ser considerado uma violação. Pode ser solicitado que os desenvolvedores forneçam evidências dos direitos deles sobre conteúdo protegido por direitos autorais.

Tenha cuidado ao usar conteúdo protegido por direitos autorais para demonstrar a funcionalidade do seu app. Em geral, a abordagem mais segura é criar algo original.

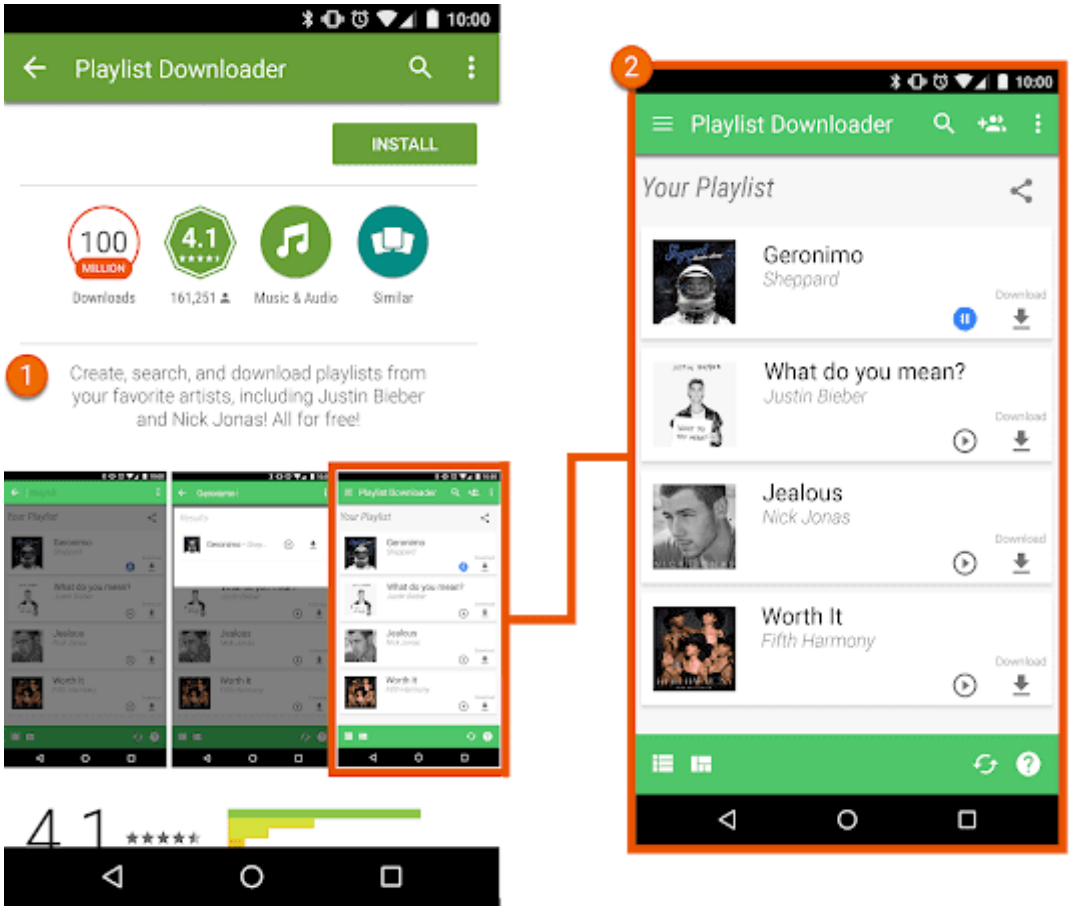
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Arte da capa de álbuns de música, videogames e livros
- Imagens de publicidade para filmes, programas de TV e jogos de video game.
- Pôsteres ou imagens de quadrinhos, desenhos animados, filmes, clipes musicais ou programas de TV.
- Logotipos de times profissionais ou de universidades.
- Fotos tiradas da conta de mídia social de uma figura pública.
- Imagens profissionais de figuras públicas.
- Reproduções ou "artes de fãs" indistinguíveis de uma obra original protegida por direitos autorais.
- Apps de sons que reproduzam clipes de áudio de conteúdo protegido por direitos autorais.
- Reproduções completas ou traduções de livros que não sejam de domínio público

Incentivo à violação de direitos autorais

Apps que incentivem a violação de direitos autorais ou estimulem tal prática não são permitidos. Antes de publicar seu app, verifique se ele não incentiva a violação de direitos autorais de alguma forma e, se necessário, busque orientação jurídica.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Apps de streaming que permitem aos usuários fazer o download de uma cópia local de conteúdo protegido por direitos autorais sem autorização
- Apps que incentivem os usuários a fazer streaming e download de obras protegidas por direitos autorais, incluindo músicas e vídeos, em violação a uma legislação de direitos autorais aplicável:



① A descrição nesta página "Detalhes do app" incentiva os usuários a fazer o download de conteúdo protegido por direitos autorais sem autorização.
② A captura de tela nesta página "Detalhes do app" incentiva os usuários a fazer o download de conteúdo protegido por direitos autorais sem autorização.

Violação de marca registrada

Apps que violem marcas registradas alheias não são permitidos. A marca registrada pode ser uma palavra, um símbolo ou uma combinação destes que identifique a origem de um produto ou serviço. Uma vez adquirida, a marca registrada oferece ao proprietário direitos exclusivos de uso da marca no que se refere a certos produtos ou serviços.

A violação de marca registrada se dá pelo uso indevido ou não autorizado de marca registrada idêntica ou semelhante de modo a confundir o usuário no que se refere à origem do produto. Se usar marcas registradas de terceiros de maneira que possa confundir o usuário, o app poderá ser suspenso.

Falsificação

Não permitimos apps que vendem ou promovem produtos falsificados. Esses produtos exibem marcas registradas ou logotipos idênticos ou extremamente semelhantes a outra marca registrada. Eles imitam as características da marca para tentar se passar por produtos originais do proprietário.

Privacidade, segurança e fraude

Estamos comprometidos em proteger a privacidade dos usuários e oferecer um ambiente seguro para eles. Apps maliciosos que abusam ou fazem uso indevido de redes, dispositivos ou dados pessoais são expressamente proibidos.

Dados do usuário

Você precisa ser transparente sobre como lida com os dados do usuário (por exemplo, dados coletados do usuário ou sobre ele, incluindo informações do dispositivo). É necessário divulgar como o app acessa, coleta, usa e compartilha dados, bem como limitar o uso dessas informações às finalidades divulgadas. Além disso, caso o app lide com dados pessoais ou confidenciais de usuários, consulte os requisitos adicionais na seção "Informações pessoais e confidenciais" abaixo. Além dessas exigências do Google Play, é preciso seguir os requisitos prescritos pelas legislações de privacidade e proteção de dados aplicáveis.

Informações pessoais e confidenciais

Os dados pessoais e confidenciais de usuários incluem, entre outros, informações de identificação pessoal, financeiras e de pagamentos, dados de autenticação, agenda, contatos, localização do dispositivo, SMS e chamadas, informações de microfones, câmeras e outros dados confidenciais de uso ou do dispositivo. Se o app lidar com dados confidenciais do usuário, será necessário fazer o seguinte:

- Limitar o acesso, a coleta, o uso e o compartilhamento de dados pessoais ou confidenciais adquiridos pelo app para finalidades diretamente relacionadas ao fornecimento e aprimoramento de recursos do app (por exemplo, um recurso que é esperado pelos usuários e foi documentado e promovido na descrição do app na Play Store). Os apps que aproveitam o uso desses dados para exibir publicidade precisam estar em conformidade com nossa política de Anúncios.
- Postar uma Política de Privacidade no campo correspondente no Play Console e no próprio app. A Política de Privacidade e as divulgações no app precisam revelar de maneira detalhada como o app acessa, coleta, usa e compartilha dados do usuário. Sua Política de Privacidade precisa divulgar os tipos de dados pessoais e confidenciais que o app acessa, coleta, usa e compartilha, além de informar com quem esses dados são compartilhados.

Lidar com todos os dados pessoais ou confidenciais do usuário de maneira segura, incluindo a transmissão desses dados por meio de criptografia moderna (por exemplo, por HTTPS).
Usar uma solicitação de permissões de tempo de execução sempre que disponível, antes de acessar os dados controlados por permissões do Android.
Não vender dados pessoais ou confidenciais de usuários.

Solicitação de consentimento e divulgação em destaque

Nos casos em que os usuários não esperam que dados pessoais ou confidenciais sejam necessários (conforme determinado pelo Google Play, de acordo com critérios próprios) para fornecer ou melhorar recursos ou funcionalidades do app que estejam em conformidade com a política, é preciso atender aos seguintes requisitos:

É necessário fornecer uma divulgação no app a respeito da coleta, do uso e do compartilhamento de dados. Essa divulgação:

precisa estar dentro do próprio app, não somente na descrição dele ou em um site;
precisa ser exibida no uso normal do app e não pode exigir que o usuário navegue até um menu ou até as configurações;
precisa descrever os dados que são acessados ou coletados;
precisa explicar como os dados serão usados e/ou compartilhados;
não pode ser colocada somente na Política de Privacidade ou nos Termos de Serviço;
não pode ser incluída em outras divulgações não relacionadas à coleta de dados pessoais ou confidenciais;

A divulgação no app precisa acompanhar e imediatamente preceder uma solicitação de consentimento do usuário e, quando disponível, ter uma permissão de tempo de execução associada a ela. Não é possível acessar nem coletar dados pessoais ou confidenciais sem o consentimento do usuário. Essa solicitação:

precisa apresentar a caixa de diálogo de consentimento de uma maneira clara e sem ambiguidades;
precisa exigir do usuário uma ação de confirmação, como um toque para aceitar, a marcação de uma caixa de seleção etc.;
não pode interpretar como consentimento a navegação para outra tela a partir da divulgação (por exemplo, tocar na tela para sair ou pressionar os botões home ou voltar); .
não pode usar mensagens que expiram ou são dispensadas automaticamente.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Um app que acessa o inventário de apps instalados do usuário e não trata esses dados como pessoais ou confidenciais sujeitos aos requisitos de transmissão segura, de divulgação em destaque e da Política de Privacidade
Um app que acessa dados do smartphone ou da lista de contatos do usuário e não trata esses dados como pessoais ou confidenciais sujeitos aos requisitos de transmissão segura, de divulgação em destaque e da Política de Privacidade
Um app que registra a tela do usuário e não trata esses dados como pessoais ou confidenciais sujeitos a essa política
Um app que coleta a localização do dispositivo e não revela de maneira detalhada o uso desses dados de acordo com os requisitos acima

Restrições para o acesso a dados confidenciais

Além dos requisitos acima, a tabela abaixo descreve as obrigações para atividades específicas.

Atividade	Requisito
O app lida com informações financeiras, de pagamento ou números de documentos de identidade.	O app jamais poderá divulgar dados pessoais ou confidenciais do usuário relacionados a atividades financeiras ou de pagamento, assim como números de documentos de identidade.
O app lida com dados privados de agenda ou de contatos.	Não permitimos a publicação ou divulgação não autorizada de contatos privados de pessoas.
O app tem funcionalidade de segurança ou antivírus, como antimalware ou recursos relacionados a proteção.	Será necessário postar uma Política de Privacidade que, juntamente com as divulgações no app, explique os dados do usuário que o app coleta e transmite, como eles são usados e com quem são compartilhados.

Privacy Shield para os Estados Unidos e a União Europeia

Se você acessar, usar ou processar informações pessoais disponibilizadas pelo Google que identificarem direta ou indiretamente um indivíduo e tiverem origem na União Europeia ou na Suíça ("Informações pessoais da UE"), será preciso:

agir em conformidade com todos os regulamentos, legislação, regras e diretrizes referentes à privacidade, segurança e proteção de dados;
acessar, usar ou processar as informações pessoais da UE somente para fins compatíveis com o consentimento recebido do indivíduo relacionado a esses dados;
implementar medidas técnicas e organizacionais adequadas para proteger as informações pessoais da UE contra perda e uso indevido, assim como divulgação, alteração, destruição ou acesso não autorizados ou ilegais;

fornecer o nível de proteção exigido pelos Princípios do Privacy Shield (Escudo de Proteção da Privacidade).

Monitore a conformidade com essas condições regularmente. Se em algum momento você não atender a essas condições ou se houver uma grande possibilidade de isso acontecer, notifique nossa equipe imediatamente enviando um e-mail para data-protection-office@google.com. Além disso, interrompa o processamento de informações pessoais da UE ou tome medidas razoáveis e apropriadas para restabelecer um nível adequado de proteção.

Permissões

As solicitações de permissão precisam fazer sentido para os usuários. O app só pode solicitar permissões que sejam necessárias para implementar recursos ou serviços atuais promovidos na página "Detalhes do app". Não é possível usar permissões que dão acesso a dados do usuário ou do dispositivo para finalidades ou recursos não revelados, não implementados ou não permitidos. Dados pessoais ou confidenciais acessados por meio de permissões nunca podem ser vendidos.

Solicite permissões de acesso a dados de acordo com o contexto (por meio da autorização incremental). Isso ajuda os usuários a entender por que a permissão é necessária. Use os dados somente para as finalidades consentidas pelo usuário. Posteriormente, se você quiser usar os dados para outros fins, será necessário pedir permissão aos usuários e receber a confirmação deles para os usos adicionais.

Permissões restritas

Além do indicado acima, as permissões restritas são aquelas designadas como Assinatura ou Perigoso na documentação do desenvolvedor e estão sujeitas aos seguintes requisitos e restrições adicionais:

> Os dados confidenciais do usuário ou do dispositivo acessados por meio de permissões restritas só podem ser transferidos a terceiros para fornecer ou aprimorar recursos ou serviços atuais no app em que os dados foram coletados. Você também pode transferir dados necessários para cumprir a legislação aplicável ou como parte de uma fusão, aquisição ou venda de ativos, com aviso legalmente adequado aos usuários. Todas as outras transferências ou vendas de dados do usuário são proibidas.
> Respeite a decisão dos usuários se eles recusarem uma solicitação de permissão restrita. Eles não podem ser manipulados nem forçados a consentir com permissões que não sejam essenciais. Faça o possível para atender os usuários que não concedem acesso a permissões confidenciais. Por exemplo, você pode permitir que o usuário insira manualmente um número de telefone, caso ele tenha restringido o acesso aos registros de chamadas.

Algumas permissões restritas podem estar sujeitas a requisitos adicionais, conforme detalhado abaixo. O objetivo dessas restrições é proteger a privacidade do usuário. Podemos fazer

exceções limitadas aos requisitos abaixo em casos muito raros em que os apps fornecem um recurso de alto interesse ou essencial ao usuário sem que haja algum método alternativo disponível para isso. Avaliamos as exceções propostas em relação aos possíveis efeitos sobre a privacidade ou segurança dos usuários.

Permissões de SMS e registro de chamadas

As permissões de SMS e registro de chamadas são consideradas dados pessoais e confidenciais de usuários sujeitos à política de Informações pessoais e confidenciais e às seguintes restrições:

Permissão restrita	Requisito
Grupo de permissões "Registro de chamadas". Por exemplo, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS	Ele precisa estar registrado ativamente como gerenciador padrão de "Telefone" ou "Assistente" no dispositivo.
Grupo de permissões "SMS". Por exemplo, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS	Ele precisa estar registrado ativamente como gerenciador padrão de "SMS" ou "Assistente" no dispositivo.

Apps sem o recurso de gerenciador padrão de "SMS" ou "Assistente" não podem declarar o uso das permissões acima no manifesto. Isso inclui o uso de texto marcador no manifesto. Os apps também precisam estar ativamente registrados como gerenciador padrão de "SMS", do "Telefone" ou do "Assistente" para poder solicitar que os usuários aceitem uma das permissões acima. Além disso, eles precisarão interromper imediatamente o uso da permissão quando não forem mais o gerenciador padrão. Os usos permitidos e exceções estão disponíveis nesta página da Central de Ajuda.

Os apps só podem usar a permissão e os dados derivados dela para fornecer a funcionalidade principal aprovada do app, que corresponde ao propósito principal dele. Isso pode incluir um conjunto de recursos principais que precisam ser documentados e promovidos com maior destaque na descrição do app. Sem os recursos principais, o app terá problemas. A transferência, o compartilhamento ou o uso licenciado desses dados só pode ocorrer para fornecer os recursos ou serviços do app. Além disso, o uso dessas informações não pode ser estendido para outras finalidades (por exemplo, melhorar outros apps e serviços ou para fins de marketing e publicidade). Não é permitido usar métodos alternativos (incluindo outras permissões, APIs ou fontes de terceiros) para receber dados atribuídos às permissões de registro de chamadas ou SMS.

Permissões de localização

Atualização de 16 de abril de 2020: sabemos que a conformidade com a política de localização pode exigir um grande trabalho de alguns desenvolvedores. Por isso, oferecemos um prazo maior para fazer as mudanças necessárias. Para ver os cronogramas e outras informações, acesse a Central de Ajuda.

A localização do dispositivo é considerada um dado pessoal e confidencial do usuário, sujeito à política de Informações pessoais e confidenciais e aos seguintes requisitos:

- Os apps não podem acessar dados protegidos por permissões de localização (por exemplo, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) que não sejam mais necessários para fornecer os recursos ou serviços atuais.
- Nunca solicite permissões de localização do usuário somente para fins de publicidade ou análise. Os apps que aproveitam o uso permitido desses dados para exibir publicidade precisam estar em conformidade com nossa política de Anúncios.
- Os apps precisam solicitar o escopo mínimo necessário (ou seja, localização aproximada em vez de exata e em primeiro plano em vez de segundo plano) para fornecer o recurso ou serviço atual que exige a localização. Além disso, os usuários devem esperar que o recurso ou serviço precise acessar o nível de localização solicitado. Por exemplo, podemos recusar apps que solicitam ou acessam o local de segundo plano sem uma justificativa convincente.
- A localização em segundo plano só pode ser usada para oferecer recursos úteis aos usuários e relevantes para a funcionalidade principal do app.

Os apps terão permissão para acessar a localização com o serviço em primeiro plano (quando o app só tem acesso em primeiro plano, ou seja, "durante o uso") se o uso:

- tiver sido iniciado para dar continuidade a uma ação do usuário no app; e
- for finalizado imediatamente após o app concluir o caso de uso pretendido pelo usuário.

Os apps desenvolvidos especificamente para crianças precisam estar em conformidade com a política do Feito para Família.

Abuso de dispositivos e de rede

Não são permitidos apps que causam danos, interferências ou interrupções ou acessam de maneira não autorizada o dispositivo do usuário, assim como outros dispositivos ou computadores, servidores, redes, interfaces de programação do app (APIs, na sigla em inglês) ou serviços. Isso inclui, sem limitação, outros apps no dispositivo, qualquer serviço do Google ou uma rede de operadora de telefonia autorizada.

Os apps no Google Play precisam obedecer aos requisitos padrão de otimização do sistema Android listados nas diretrizes principais de qualidade de apps para o Google Play.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Apps que impedem que outro app exiba anúncios ou interferem na exibição deles.
- Apps para fraudar jogos que afetam a jogabilidade de outros apps.
- Apps que facilitam ou oferecem instruções de como invadir serviços, softwares e hardwares ou como fraudar proteções de segurança.
- Apps que acessam ou usam um serviço ou uma API de um modo que viola os Termos de Serviço da API ou do serviço em questão.
- Apps que tentam ignorar o gerenciamento de energia do sistema sem estarem qualificados para a lista de permissões.
- Apps que facilitam serviços de proxy para terceiros, o que só pode ser feito se esse for o objetivo principal do app.

Comportamento malicioso

Não são permitidos apps que roubam dados, monitoram ou prejudicam usuários secretamente ou apresentam qualquer outro comportamento malicioso.

Os apps distribuídos pelo Google Play só podem ser modificados, substituídos ou atualizados por meio do mecanismo de atualização do Google Play. Da mesma forma, um app não poderá fazer download de código executável (por exemplo, arquivos dex, JAR ou .so) de uma fonte que não é o Google Play. Essa restrição não se aplica a códigos executados em máquinas virtuais e têm acesso limitado às APIs do Android (como o JavaScript em um WebView ou navegador).

Somente pode ser feito o download de recursos adicionais do app (por exemplo, de jogos) se eles forem necessários para usar o app. Os recursos salvos precisam obedecer a todas as políticas do Google Play e, antes de iniciar o download, é obrigatório fazer uma solicitação ao usuário e informar claramente o tamanho do app.

Apps de spyware comercial e vigilância são expressamente proibidos no Google Play. Somente apps que atendam à política e sejam projetados e comercializados exclusivamente para monitoramento dos pais (incluindo a família) ou gerenciamento empresarial podem ser distribuídos na loja com recursos de rastreamento e geração de relatórios, desde que atendam integralmente aos requisitos descritos abaixo.

Os elementos a seguir são expressamente proibidos:

- Vírus, cavalos de Troia, malware, spyware ou qualquer outro software malicioso.
- Apps que facilitam a distribuição ou instalação de software malicioso ou contêm links para esse tipo de software
- Apps ou SDKs que fazem download de código executável (como arquivos dex ou código nativo) de uma fonte que não seja o Google Play
- Apps que introduzem ou exploram vulnerabilidades na segurança

- Apps que roubam informações de autenticação de um usuário (como nomes de usuário ou senhas) ou imitam outros apps ou sites para enganar os usuários e fazê-los divulgar informações pessoais ou de autenticação
- Apps que exibem números de telefone, contatos, endereços ou informações de identificação pessoal não verificadas ou reais de pessoas ou entidades sem o consentimento delas
- Apps que instalam outros apps em um dispositivo sem o consentimento prévio do usuário
- Apps com downloads facilitados por rede de fornecimento de conteúdo (CDN, na sigla em inglês) quando não há uma solicitação ao usuário antes de começar nem é informado o tamanho do download
- Apps projetados para coletar secretamente o uso do dispositivo, como apps de spyware comercial

Os apps que monitoram ou rastreiam o comportamento de um usuário em um dispositivo precisam obedecer a estes requisitos:

- Não podem se apresentar aos usuários como soluções de vigilância secreta ou de espionagem.
- Não podem esconder ou ocultar comportamento de rastreamento nem tentar enganar os usuários sobre tal funcionalidade.
- Precisam apresentar aos usuários uma notificação contínua e um ícone exclusivo que identifique claramente o app.
- Os apps e páginas "Detalhes do app" no Google Play não podem fornecer meios de ativar ou acessar funcionalidades que violem esses termos, como links a um APK não compatível hospedado fora do Google Play.
- Você é exclusivamente responsável por determinar a legalidade do app na localidade de destino. Os apps considerados ilegais nos locais em que são publicados serão removidos.

Confira nosso Programa de aprimoramento de segurança de apps para conhecer os problemas de segurança mais recentes sinalizados para desenvolvedores no Google Play. Os detalhes de remediação e vulnerabilidade estão disponíveis no link da página de suporte de cada campanha.

Comportamento enganoso

Não são permitidos apps que tentam enganar os usuários ou permitem comportamento desonesto, como apps com um funcionamento inviável, entre outros. É obrigatório que os apps incluam divulgação, descrição e imagens/vídeos precisos das funções em todos os metadados. Além disso, o desempenho deve atender razoavelmente à expectativa do usuário. Os apps não podem tentar imitar a funcionalidade ou os avisos do sistema operacional ou de outros apps. As alterações nas configurações do dispositivo precisam ser facilmente reversíveis pelo usuário e ter o conhecimento e consentimento dele.

Declarações enganosas

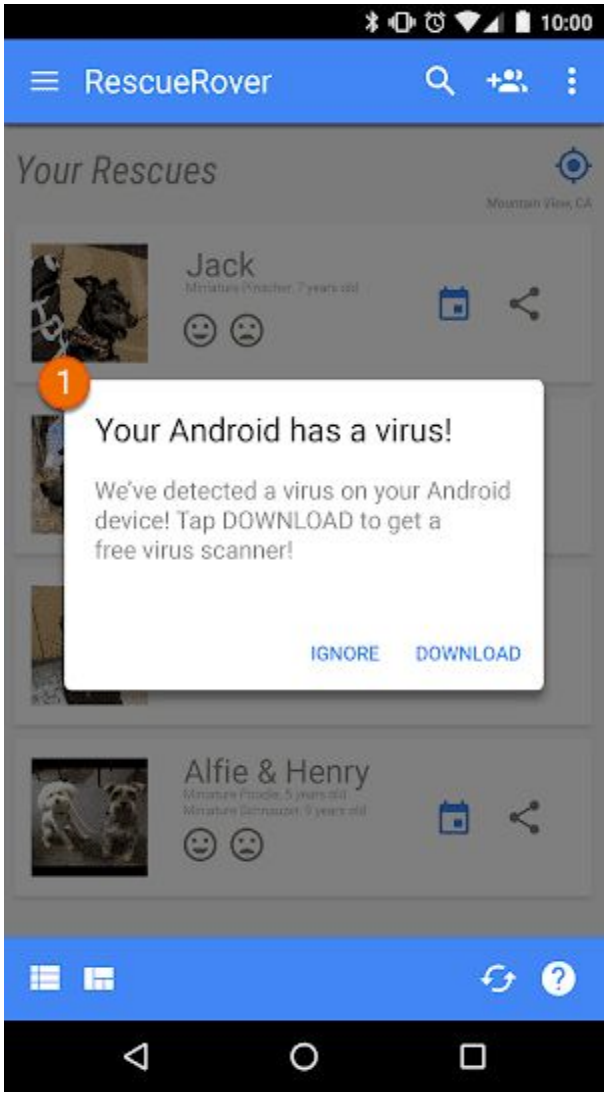
Apps que contenham informações ou declarações falsas ou enganosas, incluindo as presentes na descrição, no título, no ícone e nas capturas de tela, não são permitidos.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Apps que deturpem a funcionalidade ou que não a descrevam clara e precisamente:
  - Um app que alega ser um jogo de corrida na descrição e nas capturas de tela, mas na verdade é um quebra-cabeças usando a imagem de um carro
  - Um app que alega ser um antivírus, mas contém somente um manual explicando como remover vírus.
- Nomes de desenvolvedores ou de apps que contenham declarações falsas a respeito do status e do desempenho atual no Google Play, por exemplo, "Escolha do editor", "App número 1", "Top pagos"
- Apps com conteúdos ou recursos médicos ou relacionados à saúde que sejam enganosos ou potencialmente perigosos
- Apps que alegam funcionalidades impossíveis de serem implementadas
- Apps categorizados inadequadamente
- Conteúdo comprovadamente enganoso que pode interferir nos processos de votação
- Apps que alegam falsamente afiliação a uma entidade governamental ou dizem fornecer ou facilitar serviços governamentais sem a devida autorização

Uso não autorizado ou imitação de funcionalidade do sistema

Apps ou anúncios que imitem funcionalidades do sistema ou interfiram no funcionamento delas, como notificações ou avisos, não são permitidos. As notificações no nível do sistema só podem ser usadas para os recursos integrais de um app (por exemplo, quando um app de uma companhia aérea notifica os usuários sobre promoções especiais ou quando um jogo notifica os usuários sobre promoções no jogo).
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps ou anúncios exibidos por meio de uma notificação ou um alerta do sistema:



① A notificação do sistema exibida neste app está sendo usada para veicular um anúncio.

Para mais exemplos que envolvem anúncios, consulte a política de anúncios.

Alterações enganosas nas configurações do dispositivo

Apps que façam alterações nas configurações do dispositivo ou em recursos fora do app sem o conhecimento e consentimento do usuário não são permitidos. As configurações e os recursos do dispositivo incluem configurações do sistema e do navegador, favoritos, atalhos, ícones e widgets, além da apresentação de apps na tela inicial.

Além disso, não são permitidos:

Apps que modifiquem as configurações ou os recursos de um dispositivo com o consentimento do usuário, mas de maneira que não possa ser revertida facilmente.
Apps ou anúncios que modifiquem as configurações ou os recursos do dispositivo, como um serviço para terceiros ou para fins de publicidade.
Apps que induzam os usuários a remover ou desativar apps de terceiros ou modificar configurações ou recursos do dispositivo.
apps que incentivem os usuários a remover ou desativar apps de terceiros ou modificar configurações ou recursos do dispositivo, a menos que sejam parte de um serviço de segurança verificável.

Permitir comportamento desonesto

Não são permitidos apps que ajudem os usuários a enganar outras pessoas ou com funcionamento enganoso de alguma forma, incluindo, entre outros, apps que gerem ou facilitem a geração de RGs, CPFs, passaportes, diplomas, cartões de crédito e carteiras de motorista. É necessário apresentar informações precisas em divulgações, títulos, descrições e imagens/vídeos relacionados à função e/ou ao conteúdo do app. Além disso, o desempenho e a precisão devem atender à expectativa do usuário.

A declaração do app como uma "brincadeira", "para fins de entretenimento" ou outro sinônimo não o isenta da aplicação das nossas políticas.

Mídia manipulada

Não são permitidos apps que promovam ou ajudem a criar informações falsas ou enganosas veiculadas por meio de imagens, vídeos e/ou texto. Não são aceitos apps desenvolvidos para promover ou perpetuar imagens, vídeos ou texto comprovadamente enganosos ou que possam causar danos relacionados a eventos sensíveis, política, questões sociais ou outras questões de interesse público.

Apps que manipulam ou modificam mídia, além dos ajustes convencionais e aceitáveis em termos editoriais por questões de clareza e qualidade, precisam informar ou usar marca-d'água em mídia modificada que pode não ser facilmente detectada como tal pelas pessoas em geral. Pode haver exceções em caso de interesse público e de sátiras ou paródias óbvias.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps que adicionam uma figura pública a uma exposição durante um evento político
Apps que usam figuras públicas ou mídia de eventos sensíveis para promover o recurso de modificação de mídia na página "Detalhes do app"
Apps que alteram clipes de mídia para imitar a transmissão de notícias

Declarações falsas

Não são permitidos apps nem contas de desenvolvedores com falsificação de identidade de outra pessoa ou organização. Também é proibido deturpar ou ocultar a propriedade ou o objetivo principal do app ou da conta. Não permitimos a presença de apps nem de contas de desenvolvedores que estejam envolvidos em atividades coordenadas para enganar os usuários. Isso inclui, entre outros, apps ou contas que deturpam ou ocultam o país de origem ou que direcionam conteúdo para usuários em outros países.

Malware

Nossa política sobre Malware é simples: o ecossistema Android, inclusive a Google Play Store, e os dispositivos do usuário não podem apresentar comportamentos maliciosos (ou seja, malware). A partir desse princípio fundamental, buscamos fornecer um ecossistema Android seguro para os usuários e os dispositivos Android deles.

Malware é qualquer código capaz de colocar um usuário, os dados de usuário ou um dispositivo em risco. O malware inclui aplicativos potencialmente nocivos (PHAs), binários ou modificações da estrutura que consistem em apps de trojans, phishing e spyware, entre outros. Além dessas, estamos continuamente atualizando e adicionando novas categorias.

Com diferentes tipos e recursos, o malware geralmente tem um dos seguintes objetivos:

- Comprometer a integridade do dispositivo do usuário
- Controlar um dispositivo do usuário
- Ativar operações controladas remotamente para que um invasor acesse, use ou explore um dispositivo infectado
- Transmitir dados pessoais ou credenciais do dispositivo sem a divulgação e o consentimento adequados
- Enviar spam ou comandos do dispositivo infectado a outros dispositivos ou redes
- Enganar o usuário

Um app, binário ou uma modificação da estrutura podem ser potencialmente nocivos e gerar um comportamento malicioso, mesmo que essa não tenha sido a intenção. Isso acontece porque apps, binários ou modificações na estrutura podem agir de diferentes maneiras, de acordo com uma série de variáveis. Portanto, o que é nocivo para um dispositivo Android pode não provocar risco algum em outro dispositivo Android. Por exemplo, um dispositivo que executa a última versão do Android não será afetado por apps nocivos que usam APIs obsoletas para realizar comportamentos maliciosos, mas um dispositivo que use uma versão muito antiga do Android pode estar em risco. Apps, binários ou modificações da estrutura serão sinalizados como malware ou PHA se claramente colocarem em risco vários ou todos os dispositivos e usuários do Android.

As categorias de malware abaixo refletem nossa crença fundamental de que os usuários devem compreender como os dispositivos deles estão sendo usados e promover um ecossistema seguro que permita uma inovação robusta e uma experiência confiável do usuário.

Acesse o Google Play Protect para saber mais.

Acessos "backdoor"

É um código que permite a execução de operações indesejadas, potencialmente nocivas e controladas remotamente em um dispositivo.

Essas operações podem incluir comportamentos que fazem com que o app, binário, ou a modificação da estrutura se classifique em uma categoria de malware quando a execução é automática. Em geral, o termo "backdoor" descreve como uma operação potencialmente nociva pode ocorrer em um dispositivo. Portanto, ele não se enquadra exatamente em categorias como fraude de faturamento e spyware comercial. Como resultado disso, em algumas circunstâncias, determinados acessos "backdoor" podem ser considerados uma vulnerabilidade pelo Google Play Protect.

Fraude por faturamento

É um código que cobra o usuário automaticamente de forma enganosa.

As fraudes de faturamento de dispositivos móveis estão divididas entre SMS, chamada e tarifa.

Fraude por SMS

É um código que emite cobranças pelo envio de SMS premium sem o consentimento do usuário ou que tenta encobrir a atividade de SMS ao ocultar acordos de divulgação ou mensagens SMS da operadora de telefonia móvel com notificações sobre cobranças ou confirmações de assinaturas.

É o mesmo código, mas apesar de tecnicamente expor o envio de SMS, também apresenta um comportamento adicional que inclui fraude de SMS. Os exemplos incluem ocultar partes de um acordo de divulgação do usuário para que não seja legível e bloquear intencionalmente as mensagens SMS da operadora de telefonia móvel informando o usuário sobre cobranças ou confirmando uma assinatura.

Fraude por chamada

É um código que emite cobranças ao realizar chamadas para números premium sem o consentimento do usuário.

Fraude por tarifa

É um código que engana o usuário para que ele assine ou compre conteúdos por meio da conta do celular.

A fraude por tarifa inclui qualquer tipo de faturamento, exceto SMS e chamadas premium. Os exemplos disso são Faturamento direto via operadora, ponto de acesso sem fio (WAP) e transferência de créditos para dispositivos móveis. A fraude por WAP é um dos tipos mais prevalentes de fraudes por tarifa. A fraude por WAP pode levar os usuários a clicar em um

botão ou em um WebView transparente e carregado de forma silenciosa. Ao cumprir a ação, uma assinatura recorrente é iniciada, e geralmente a mensagem por e-mail ou SMS é invadida para evitar que os usuários percebam a transação financeira.

Spyware comercial

É um código que transmite informações pessoais do dispositivo sem o devido consentimento ou aviso e não exibe uma notificação persistente de que isso está acontecendo.

Apps de spyware comercial transmitem dados para outro destino que não o provedor de PHA. Formas legítimas desses apps podem ser usadas por pais para monitorar os filhos. No entanto, não é possível utilizar esses apps para monitorar outras pessoas (um cônjuge, por exemplo) sem o conhecimento ou permissão delas se nenhuma notificação persistente é exibida durante a transmissão dos dados.

Negação de serviço (DoS)

É um código que, sem o conhecimento do usuário, executa um ataque de negação de serviço (DoS) ou faz parte de um ataque de DoS distribuído para outros sistemas e recursos.

Por exemplo, isso pode acontecer ao enviar um volume alto de solicitações HTTP para gerar um carregamento excessivo em servidores remotos.

Componentes de downloads hostis

É um código que não é potencialmente nocivo por si só, mas que faz o download de outros PHAs.

Ele pode ser um componente de downloads hostil se:

- houver razões para acreditar que ele foi criado para espalhar PHAs e que fez ou contém um código que poderia fazer o download de PHAs e instalá-los; ou
- pelo menos 5% dos downloads feitos por ele são de PHAs com um limite mínimo de 500 downloads de apps observados, ou seja, 25 downloads de PHAs observados.

Os principais navegadores e apps de compartilhamento de arquivos não serão considerados componentes de downloads hostis desde que:

- não façam downloads sem a interação do usuário; e
- todos os downloads de PHA sejam iniciados por usuários que deram consentimento.

Ameaça que não atinge o Android

É um código com ameaças que não atingem o Android.

Esses apps não causam danos ao usuário ou dispositivo Android, mas têm componentes potencialmente nocivos a outras plataformas.

Phishing

É um código que finge ser de uma fonte confiável, solicita credenciais de autenticação do usuário ou informações de faturamento e envia esses dados a terceiros. Esta categoria também se aplica a código que intercepta a transmissão de credenciais do usuário.

Alguns alvos comuns de phishing são credenciais bancárias, números de cartão de crédito e credenciais de contas on-line para redes sociais e jogos.

Abuso de privilégios elevados

É um código que compromete a integridade do sistema ao romper o sandbox do app, ter privilégios elevados ou alterar ou desabilitar o acesso a funções centrais ligadas à segurança.

Por exemplo:

- Um app que viola o modelo de permissões do Android ou rouba credenciais (como tokens OAuth) de outros apps
- Apps que abusam de recursos para impedir que sejam desinstalados ou interrompidos
- Um app que desativa o SELinux

Apps com escalonamento de privilégios que dão acesso root a dispositivos sem a permissão do usuário, considerados apps de acesso root

Ransomware

É um código que toma o controle parcial ou total de um dispositivo ou dados de um dispositivo e exige que o usuário faça um pagamento ou realize alguma ação para recuperá-lo.

Alguns tipos de ransomware criptografam dados no dispositivo e exigem o pagamento para descriptografá-los e/ou aproveitam os recursos de administração do dispositivo para que não possa ser removido por um usuário típico. Por exemplo:

- Bloquear um usuário do próprio dispositivo e exigir dinheiro para devolver o controle ao usuário
- Criptografar dados no dispositivo e exigir o pagamento para descriptografar os dados
- Aproveitar os recursos do Gerenciador de políticas do dispositivo e bloquear a remoção pelo usuário

O código distribuído com o dispositivo que tenha como objetivo principal o gerenciamento subsidiado do dispositivo pode ser excluído da categoria de ransomware, desde que cumpra com os requisitos de bloqueio e gerenciamento seguros e de divulgação e consentimento do usuário adequados.

Acesso root

É um código que faz root no dispositivo.

Há uma diferença entre códigos de root maliciosos e não maliciosos. Por exemplo, apps de root não maliciosos permitem que o usuário saiba antecipadamente que eles farão root no dispositivo e que não executarão mais ações potencialmente nocivas que se aplicam a outras categorias de PHA.

Os apps de root maliciosos não informam o usuário que farão root no dispositivo ou informam antecipadamente, mas também executam ações que se aplicam a outras categorias de PHA.

Spam

É um código que envia mensagens não solicitadas aos contatos dos usuários ou usa o dispositivo para o redirecionamento de spam de e-mail.

Spyware

É um código que transmite dados pessoais do dispositivo sem o devido consentimento ou aviso.

Por exemplo, a transmissão de qualquer uma das informações a seguir sem consentimento ou de maneira não esperada pelo usuário é suficiente para ser considerada spyware:

- Lista de contatos
- Fotos ou outros arquivos do cartão SD ou que não sejam de propriedade do app
- Conteúdo proveniente do e-mail do usuário
- Registro de chamadas
- Registro de SMS
- Histórico da Web ou favoritos do navegador padrão
- Informações dos diretórios /data/ de outros apps

Comportamentos considerados espionagem também podem ser identificados como spyware. Exemplos disso são a gravação de áudio e chamadas para o smartphone ou o roubo de dados do app.

Cavalo de Troia

É um código que parece ser benigno, como um jogo que afirma ser só um jogo, mas que realiza ações indesejáveis contra o usuário.

Essa classificação geralmente é usada em combinação com outras categorias de PHA. Um cavalo de Troia tem um componente inofensivo e um nocivo oculto. Por exemplo, um jogo que envia mensagens SMS premium do dispositivo em segundo plano e sem o conhecimento do usuário.

Observação sobre apps incomuns

Apps novos e raros poderão ser classificados como incomuns se o Google Play Protect não tiver informações suficientes para considerá-los seguros. Isso não significa que o app é

necessariamente nocivo, mas sim que é preciso uma avaliação mais profunda para que seja classificado como seguro.

Observação sobre a categoria "backdoor"

A classificação na categoria de malware "backdoor" depende de como o código funciona. Uma condição necessária para que qualquer código seja classificado como de "backdoor" é que, ao ser executado automaticamente, ele habilite comportamentos classificados em uma das outras categorias de malware. Por exemplo, se um app permitir o carregamento dinâmico de código que extrai mensagens de texto, o app será classificado como malware "backdoor".

Porém, se um app permitir a execução arbitrária de código, mas não tivermos motivos para acreditar que esse código tenha sido adicionado com o objetivo de realizar um comportamento malicioso, o app será considerado vulnerável, e não malware "backdoor". Nesse caso, será solicitado que o desenvolvedor crie um patch para corrigir o problema.

Apps que contêm anúncios enganosos ou invasivos não são permitidos. Os anúncios só podem ser exibidos dentro do app em que são veiculados. Consideramos anúncios veiculados no seu app como parte do app. Os anúncios exibidos no app precisam estar em conformidade com todas as nossas políticas. Para ver as políticas relativas a anúncios de jogos de azar, clique aqui.
O Google Play é compatível com diversas estratégias de monetização para beneficiar desenvolvedores e usuários. Essas estratégias incluem distribuição paga, produtos no aplicativo, assinaturas e modelos baseados em anúncios. Para garantir a melhor experiência do usuário, é necessário obedecer a essas políticas.

Pagamentos

Os apps que utilizam compras na loja ou no aplicativo precisam obedecer às seguintes diretrizes:

Compras na loja: os desenvolvedores que cobram por apps e downloads do Google Play precisam usar o sistema de pagamento da plataforma.

Compras no aplicativo:

- Os desenvolvedores que oferecem produtos dentro de um jogo transferido do Google Play ou acesso a conteúdo do jogo têm que usar o Faturamento do Google Play no app como forma de pagamento.
- Os desenvolvedores que oferecem produtos dentro de apps transferidos do Google Play de outra categoria precisam usar o Faturamento do Google Play no app como forma de pagamento, exceto nos seguintes casos:
    - Se o pagamento for relacionado somente a produtos físicos.

Se o pagamento for relacionado a conteúdos digitais que possam ser usados fora do próprio app (por exemplo, a compra de músicas que podem ser reproduzidas em outros players de música).

As moedas virtuais no app só poderão ser usadas dentro do app ou jogo em que foram compradas.

Os desenvolvedores não podem enganar os usuários em relação aos apps nem a qualquer outro serviço, produto, conteúdo ou outra funcionalidade oferecidos para compra. Se a descrição do produto no Google Play mencionar recursos no app que exijam uma cobrança específica ou adicional, essa descrição precisará notificar claramente os usuários de que é necessário pagar para ter acesso a esses recursos.

Os apps que oferecem mecanismos de envio de itens virtuais aleatórios a partir de uma compra (ou seja, "loot boxes") precisam divulgar claramente as chances de os usuários receberem esses itens antes de efetuarem o pagamento.

Inscrições

Os desenvolvedores não podem enganar os usuários sobre qualquer serviço ou conteúdo de assinatura oferecido no app. É fundamental fornecer informações claras em qualquer promoção no app ou na tela de apresentação.

No seu app: é preciso ser transparente sobre as ofertas. Isso inclui informar explicitamente quais são os termos da oferta, o custo da assinatura, a frequência do ciclo de faturamento e se é necessária uma assinatura para usar o app. Os usuários não podem ter que realizar ações adicionais para acessar as informações.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

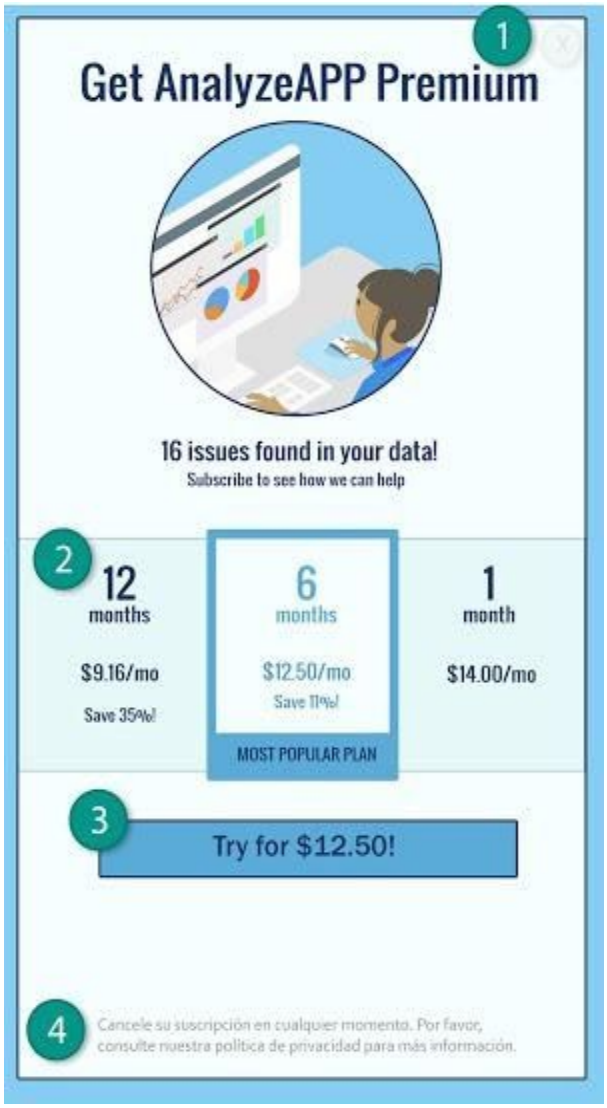
Assinaturas mensais que não informam aos usuários que serão renovadas e cobradas automaticamente todos os meses

Assinaturas anuais que mostram o custo mensal associado com mais destaque

Preços e termos da assinatura que não foram completamente localizados

Promoções no app que não demonstram claramente que o usuário pode acessar o conteúdo sem uma assinatura (quando disponível)

Nomes de SKU que não indicam com precisão a natureza da assinatura, como "Avaliação gratuita" para uma assinatura com cobrança recorrente automática



① O botão de dispensar não é claramente visível, e talvez os usuários não entendam que podem acessar recursos sem aceitar a oferta de assinatura.

② A oferta exibe somente o custo mensal, e talvez os usuários não entendam que serão cobrados por seis meses ao fazer a assinatura.

③ A oferta exibe somente o preço inicial, e talvez os usuários não entendam o valor que será cobrado automaticamente quando o período promocional acabar.

④ A oferta não obedece às regras. Ela precisa ser localizada no mesmo idioma dos Termos e Condições para que os usuários a entendam completamente.

Avaliações gratuitas e ofertas iniciais

Antes de um usuário se inscrever na sua assinatura: é preciso descrever os termos da oferta de maneira clara e precisa, incluindo a duração, o preço e a descrição dos conteúdos ou serviços

acessíveis. Informe aos usuários como e quando a avaliação gratuita se tornará uma assinatura paga, quanto ela custará e como funciona o cancelamento, caso o usuário não queira mudar para o acesso pago.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Ofertas que não explicam claramente a duração da avaliação gratuita ou do preço inicial
- Ofertas que não explicam claramente que o usuário será automaticamente inscrito em uma assinatura paga ao final do período de avaliação
- Ofertas que não demonstram claramente que o usuário pode acessar conteúdo sem uma avaliação (quando disponível)
- Ofertas com termos e preços que não foram completamente localizados

① O botão de dispensar não é claramente visível, e talvez os usuários não entendam que podem acessar recursos sem se inscrever na avaliação gratuita.

② A oferta enfatiza a avaliação gratuita, e os usuários podem não entender que serão cobrados automaticamente no final desse período.

③ A oferta não informa o período de avaliação, e os usuários podem não compreender por quanto tempo terão acesso gratuito ao conteúdo da assinatura.

④ A oferta não obedece às regras. Ela precisa ser localizada no mesmo idioma dos Termos e Condições para que os usuários a entendam completamente.

Gerenciamento e cancelamento de assinaturas

Como desenvolvedor, você precisa garantir que seus apps divulguem claramente como os usuários podem gerenciar ou cancelar assinaturas.

De acordo com nossa política, se o usuário cancelar uma assinatura comprada de um app no Google Play, ele não receberá um reembolso pelo período de faturamento atual. No entanto, ele continuará recebendo o conteúdo da assinatura até o fim do período de faturamento atual independentemente da data do cancelamento. O cancelamento entrará em vigor após o término do período de faturamento atual.

Como fornecedor de conteúdo ou de acesso, você pode implementar uma política de reembolso mais flexível diretamente com os usuários. É responsabilidade sua notificar os usuários de qualquer alteração nas políticas de assinatura, cancelamento e reembolso e garantir que elas obedeçam à legislação aplicável.

Apps que contêm anúncios enganosos ou invasivos não são permitidos. Os anúncios só podem ser exibidos dentro do app em que são veiculados. Consideramos anúncios veiculados no seu app como parte do app. Os anúncios exibidos no app precisam estar em conformidade com todas as nossas políticas. Para ver as políticas relativas a anúncios de jogos de azar, clique aqui.
Apps que contêm anúncios enganosos ou invasivos não são permitidos. Os anúncios só podem ser exibidos dentro do app em que são veiculados. Consideramos anúncios veiculados no seu app como parte do app. Os anúncios exibidos no app precisam estar em conformidade com todas as nossas políticas. Para ver as políticas relativas a anúncios de jogos de azar, clique aqui.

Uso de dados de local para publicidade

Os apps que aproveitam o uso dos dados de local do dispositivo com base em permissão para exibir anúncios estão sujeitos à política de Informações pessoais e confidenciais e aos seguintes requisitos:

> O uso ou coleta de dados de local do dispositivo com base em permissão para fins publicitários precisa estar claro para o usuário e documentado na Política de

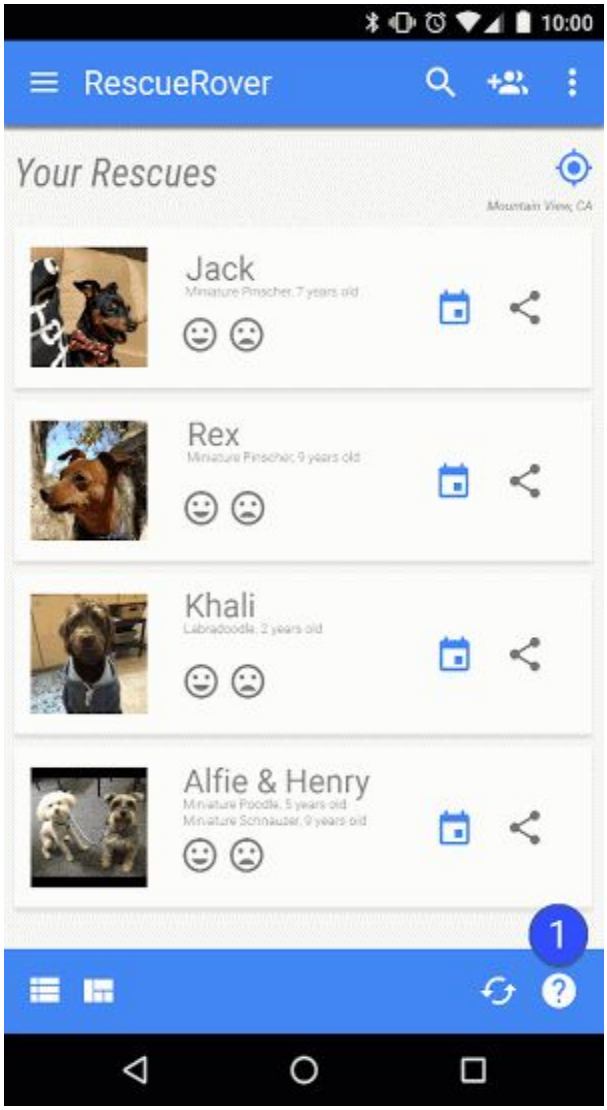
Privacidade obrigatória do app. Isso inclui links para as Políticas de Privacidade relevantes da rede de publicidade que abordem o uso desse tipo de dados.
De acordo com os requisitos de permissões de localização, essas permissões só podem ser solicitadas para implementar recursos ou serviços atuais no app, e não apenas para uso publicitário.

Anúncios enganosos

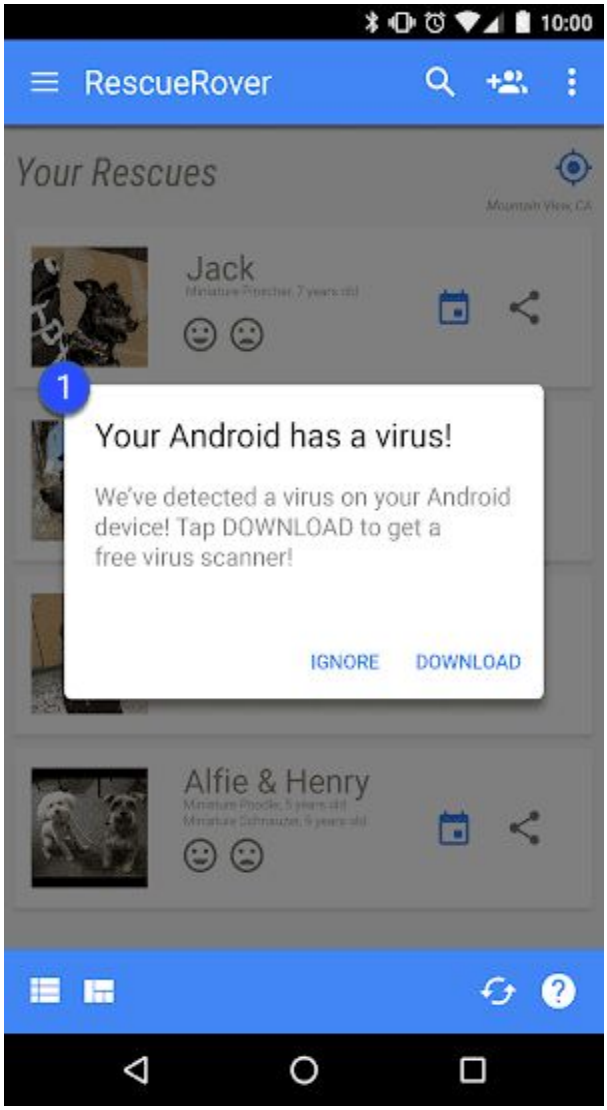
Os anúncios não podem simular nem imitar a interface do usuário de apps ou dos elementos de aviso ou de notificação de um sistema operacional. É preciso indicar claramente para o usuário qual app veicula cada anúncio.

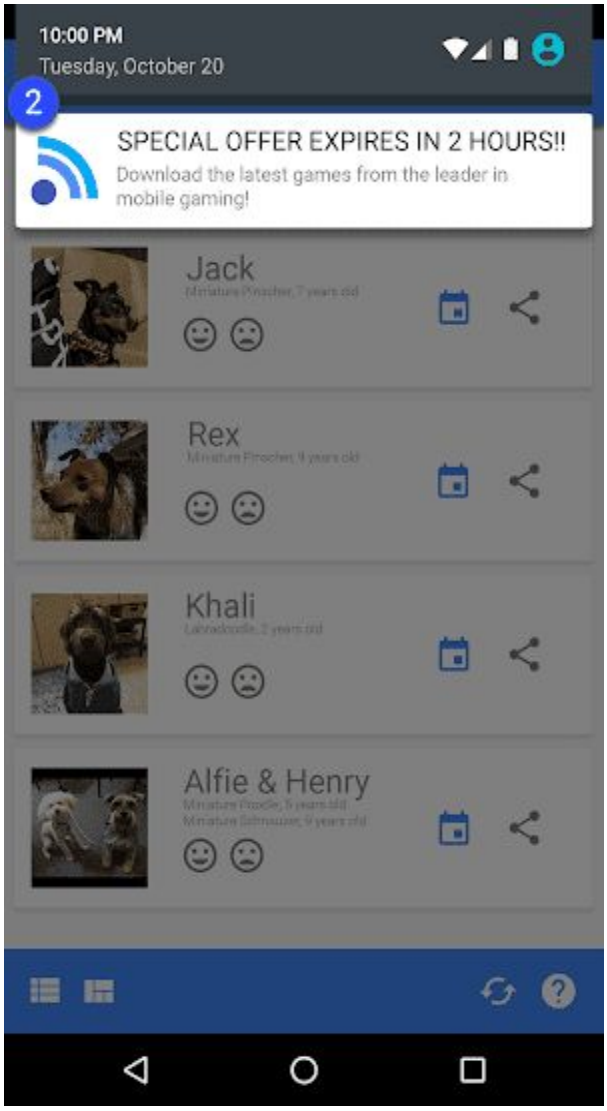
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Anúncios que imitam a interface do usuário de um app:



① O ícone de interrogação neste app é um anúncio que leva o usuário para uma página de destino externa.
Anúncios que imitam uma notificação do sistema:





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

Monetização da tela de bloqueio

Os apps não podem apresentar anúncios ou recursos que gerem receita a partir da tela bloqueada de um dispositivo, a menos que o único objetivo do app seja oferecer o serviço de tela de bloqueio.

Anúncios invasivos

Os anúncios não podem ser exibidos de maneira que resulte em cliques acidentais. É proibido condicionar a liberação do uso integral de um app por parte do usuário ao clique em um anúncio ou ao envio de informações pessoais para fins de publicidade.

Os anúncios intersticiais só podem ser exibidos dentro do app em que são veiculados. Caso seu app exiba anúncios intersticiais ou outros anúncios que interfiram no uso normal, é necessário que eles sejam fáceis de dispensar sem qualquer prejuízo aos usuários.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Anúncios que ocupam a tela inteira ou interferem na utilização normal e não fornecem um meio claro de dispensar o anúncio:

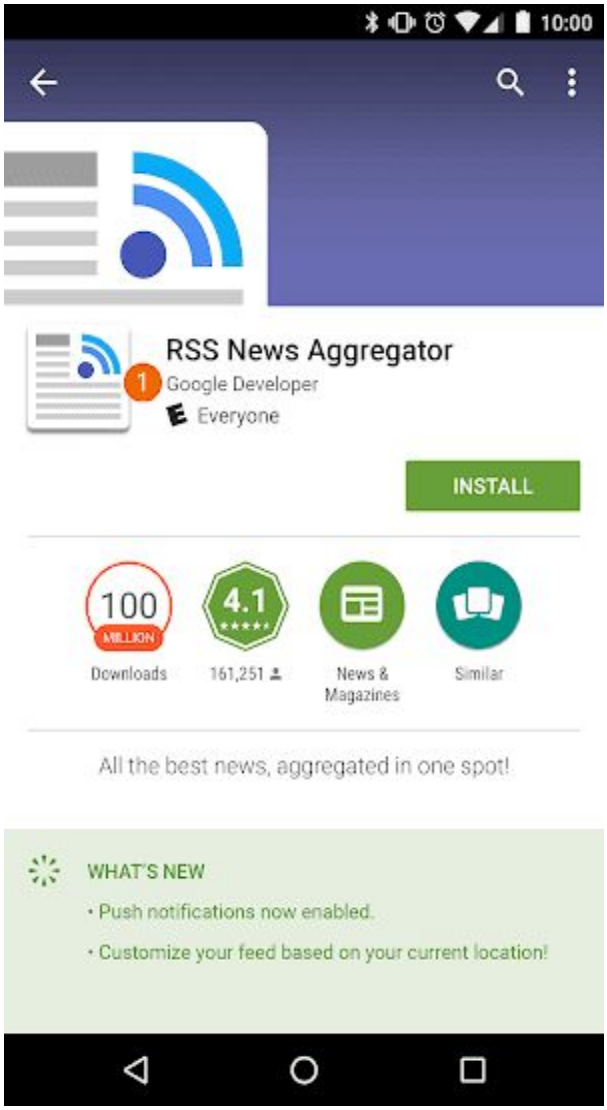
① Este anúncio não tem um botão para dispensar.

Interferência em apps, anúncios de terceiros ou funcionalidade do dispositivo

Os anúncios associados ao app não podem interferir em outros apps e anúncios nem na operação do dispositivo, incluindo botões e portas do sistema ou do dispositivo. Isso inclui sobreposições, recursos complementares e blocos de anúncios em forma de widget. Os anúncios só podem ser exibidos dentro do app em que são veiculados.

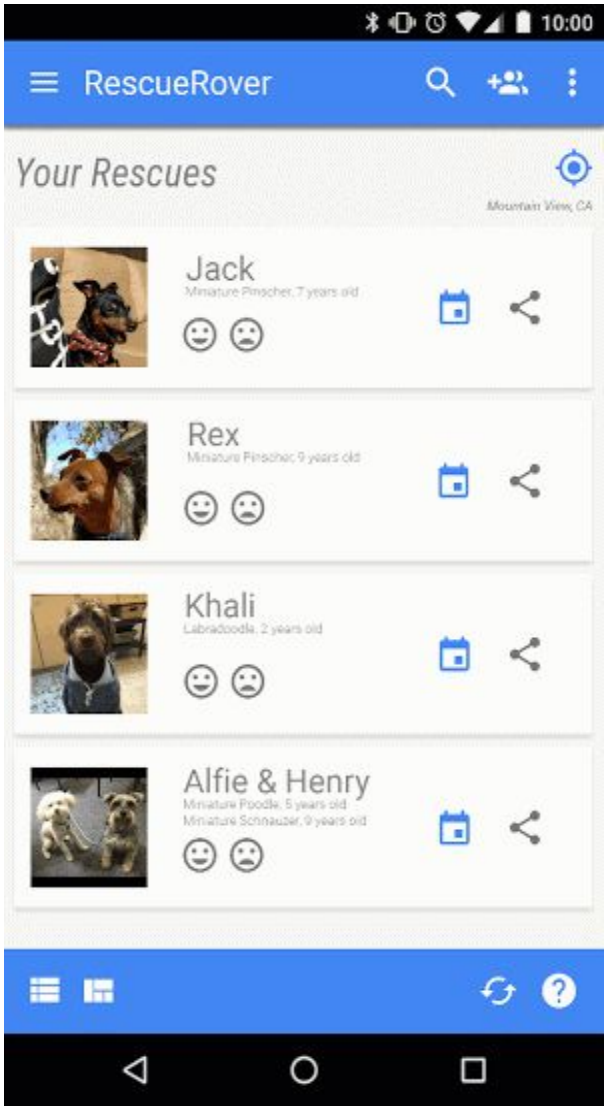
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Anúncios que são exibidos fora do app em que são veiculados:



Descrição: O usuário navega até a tela inicial a partir deste app e, de repente, um anúncio aparece na tela inicial.

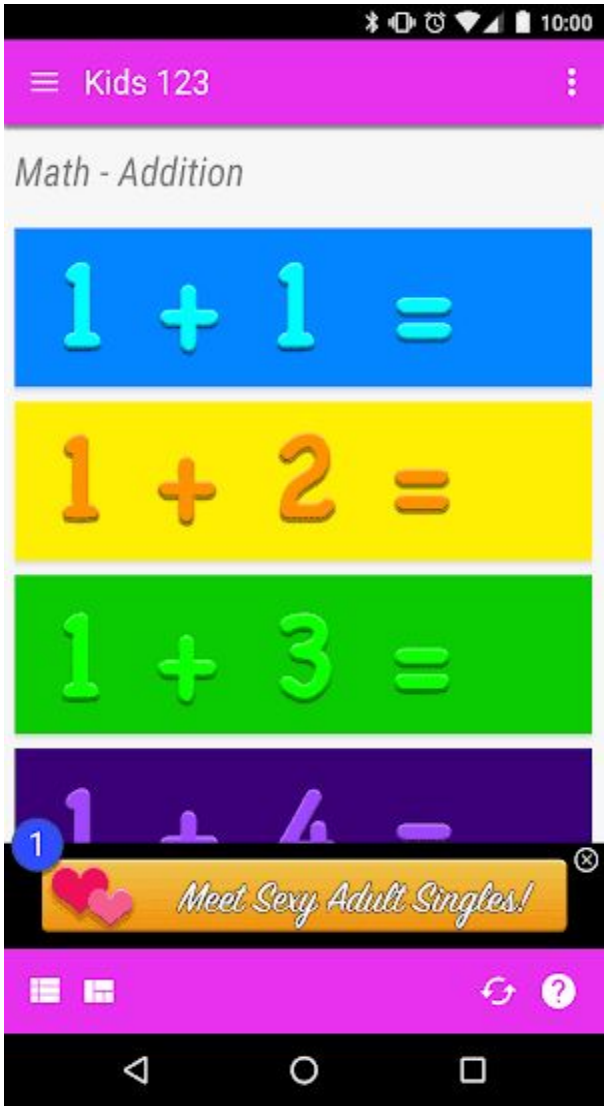
Anúncios que são acionados pelo botão de início ou por outros recursos projetados especificamente para sair do app:



Descrição: o usuário tenta sair do app e navegar até a tela inicial, mas o fluxo esperado é interrompido por um anúncio.

Anúncios inadequados

Os anúncios exibidos dentro do app precisam ser adequados para o público-alvo, além de estar em conformidade com nossas políticas.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.



① Este anúncio é inadequado para o público-alvo deste app.

Uso do código de publicidade do Android

A versão 4.0 do Google Play Services introduziu novas APIs e um código para ser usado por provedores de análise e publicidade. Os termos para o uso desse código estão disponíveis abaixo.

> Uso. O identificador de publicidade do Android só pode ser utilizado para publicidade e análise de usuário. O status das configurações "Desativar publicidade com base em interesses" e "Desativar a Personalização de anúncios" precisa ser verificado em cada acesso do código.
> Associação a informações de identificação pessoal ou outros identificadores. O identificador de publicidade não pode estar vinculado a informações pessoais de identificação nem associado a qualquer identificador de dispositivo em tempo integral

(por exemplo, SSAID, endereço MAC, IMEI etc.) sem o consentimento explícito do usuário.
Respeito às seleções dos usuários. Se for redefinido, o novo identificador de publicidade não poderá ser vinculado a outro anterior nem a dados derivados desse identificador sem o consentimento explícito do usuário. Além disso, é preciso respeitar a configuração "Desativar publicidade com base em interesses" ou "Desativar a Personalização de anúncios" do usuário. Se um usuário tiver ativado essa configuração, o identificador de publicidade não poderá ser usado na criação de perfis de usuários para fins publicitários ou para segmentação de usuários com publicidade personalizada. As atividades permitidas incluem publicidade contextual, limite de frequência, acompanhamento de conversões, geração de relatórios, segurança e detecção de fraudes.
Transparência aos usuários. A coleta e o uso do identificador de publicidade e o cumprimento destes termos precisam ser divulgados aos usuários em uma notificação de privacidade adequada às normas legais. Para saber mais sobre nossos padrões de privacidade, consulte nossa política de Dados do usuário.
Concordância com os Termos de Uso. O identificador de publicidade só pode ser utilizado de acordo com estes termos, tanto por você quanto por qualquer parte com quem ele seja compartilhado em função dos seus negócios. Todos os apps enviados ou publicados no Google Play precisam usar o código de publicidade (quando disponível em um dispositivo) em vez de outros identificadores de dispositivo para fins publicitários.

Programa de Anúncios para Famílias

Se você veicula anúncios no app e o público-alvo dele inclui apenas crianças, conforme descrito na Política para famílias, é necessário usar SDKs com autocertificação de cumprimento das Políticas do Google Play, incluindo os requisitos de certificação de SDKs de anúncios abaixo. Caso o público-alvo do app inclua crianças e adultos, implemente medidas de triagem de idade e garanta que os anúncios exibidos para crianças tenham origem exclusivamente em um desses SDKs de anúncios com autocertificação. Os apps do Programa Feito para Família precisam usar somente SDKs de anúncios com autocertificação.

O uso de SDKs de anúncios certificados do Google Play só será necessário se você utilizar SDKs para veicular anúncios a crianças. Os casos a seguir são aceitos sem a autocertificação de SDK com o Google Play. No entanto, você continua sendo responsável por garantir que o conteúdo dos anúncios e as práticas de coleta de dados obedeçam à Política de dados do usuário e à Política para famílias do Google Play:

Publicidade interna em que você use SDKs para fazer promoção cruzada entre apps ou outras mídias e produtos de merchandising
Transações diretas com anunciantes em que os SDKs são usados para o gerenciamento de inventário

Requisitos de certificação de SDKs de anúncios

- Defina o que são conteúdos e comportamentos de anúncios questionáveis e proíba-os nos termos ou nas políticas do SDK de anúncios. As definições precisam estar em conformidade com as Políticas do programa para desenvolvedores do Google Play.
- Crie um método para classificar os anúncios de acordo com grupos adequados à idade dos usuários, incluindo, pelo menos, grupos para "Todos" e "Adulto". A metodologia de classificação precisa estar de acordo com a fornecida pelo Google aos SDKs uma vez que o formulário de interesse abaixo tenha sido preenchido.
- Seja por solicitação ou por app, permita que os editores solicitem tratamento para direcionamento a crianças para veiculação de anúncios. Esse tratamento precisa obedecer a todas as legislações e regulamentações aplicáveis de proteção infantil, como a Lei de Proteção da Privacidade On-line das Crianças (COPPA, na sigla em inglês) dos EUA e o Regulamento geral de proteção de dados (GDPR, na sigla em inglês) da UE. O Google Play também requer a desativação de anúncios personalizados, publicidade com base em interesses e remarketing como parte do tratamento para direcionamento a crianças.
- Quando forem usados lances em tempo real para veicular anúncios para crianças, garanta que os criativos tenham sido revisados e que os indicadores de privacidade sejam propagados aos bidders.
- Forneça ao Google informações suficientes para a verificação da conformidade do SDK de anúncios com todos os requisitos de certificação e responda em tempo hábil às solicitações de dados subsequentes.

Observação: os SDKs de anúncios precisam ser compatíveis com a veiculação de anúncios feita em conformidade com todos os estatutos e regulamentos relevantes em relação a crianças quando houver regras desse tipo que se apliquem aos editores.

Requisitos de mediação para plataformas de veiculação ao exibir anúncios para crianças:

- Use somente SDKs de anúncios certificados do Google Play ou implemente as salvaguardas necessárias para garantir que todos os anúncios veiculados por mediação obedeçam a esses requisitos.
- Transmita os sinais necessários para indicar a classificação do conteúdo do anúncio e qualquer tratamento para direcionamento a crianças aplicável.

Os desenvolvedores podem encontrar uma lista de SDKs autocertificados neste link.

Além disso, os desenvolvedores podem compartilhar este formulário de interesse com os SDKs de anúncios que querem receber a certificação.

Página "Detalhes do app" e promoção

A promoção e a visibilidade do app têm um forte impacto na qualidade dele na Google Play Store. Evite usar spam, promoções de baixa qualidade e meios artificiais de aumentar a visibilidade do app na página "Detalhes do app" no Google Play.

Promoção de apps

Apps que usem, direta ou indiretamente, práticas enganosas ou prejudiciais aos usuários ou ao ecossistema do desenvolvedor ou que se beneficiem de tais práticas não são permitidos. Isso inclui apps com os seguintes tipos de comportamento:

- Uso de anúncios enganosos em websites, apps ou outras propriedades, incluindo alertas ou notificações semelhantes àquelas do sistema.
- Promoção ou técnicas de instalação que causam o redirecionamento para o Google Play ou para o download do app sem uma ação informada do usuário.
- Promoção não solicitada por meio de serviços de SMS.

É responsabilidade do desenvolvedor garantir que as redes de anúncios e os afiliados associados ao app dele cumpram com estas políticas e não empreguem práticas de promoção proibidas.

Metadados

Não permitimos apps com metadados enganosos, excessivos, irrelevantes, inadequados, com formatação incorreta ou sem valor descritivo, incluindo a descrição do app, nome do desenvolvedor, título, ícone, capturas de tela e imagens promocionais. Os desenvolvedores precisam fornecer uma descrição clara e bem escrita. Também não permitimos depoimentos de usuários anônimos ou não identificados na descrição do app.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

① Depoimentos de usuários anônimos ou não identificados

② Comparação de dados de apps ou marcas

③ Blocos ou listas verticais/horizontais de palavras

Veja alguns exemplos de texto, imagens ou vídeos inadequados na página "Detalhes do app":

Imagens ou vídeos com conteúdo sexualmente sugestivo. Evite imagens sugestivas que tenham seios, nádegas, órgãos genitais ou outro conteúdo ou anatomia de fetiche, seja real ou ilustração.

Linguagem inapropriada para o público em geral. Evite linguagem profana e vulgar nos detalhes do seu app. Se for um elemento crítico do seu app, será necessário censurar a apresentação dessa linguagem na página "Detalhes do app".

Não é permitido retratar violência explícita de maneira proeminente em imagens promocionais, vídeos nem ícones do app.

Representação do uso ilícito de drogas. Mesmo o conteúdo educacional, documental, científico ou artístico (EDSA, na sigla em inglês) precisa ser adequado para todos os públicos na página "Detalhes do app".

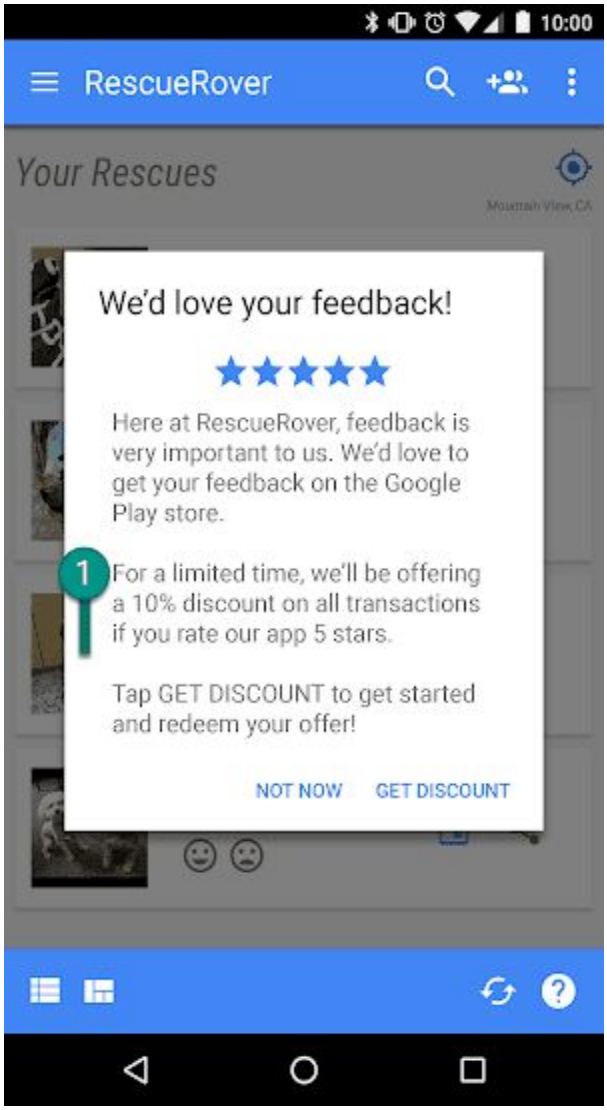
Veja algumas práticas recomendadas:

Destaque o que há de melhor no seu app. Compartilhe fatos interessantes para que os usuários entendam o que ele tem de especial.
Verifique se o título e a descrição do app mostram precisamente a funcionalidade dele. Evite usar palavras-chave ou referências repetitivas ou sem relação com o app.
A descrição do app precisa ser concisa e direta. Descrições mais curtas costumam resultar em uma experiência do usuário melhor, principalmente em dispositivos com telas menores. Uma descrição excessivamente extensa, com muitos detalhes, formatação incorreta ou repetições, pode resultar na violação desta política.
A página "Detalhes do app" precisa ser adequada para o público em geral. Evite o uso de textos, imagens ou vídeos inadequados e obedeça às diretrizes acima.

Instalações, notas e avaliações de usuários

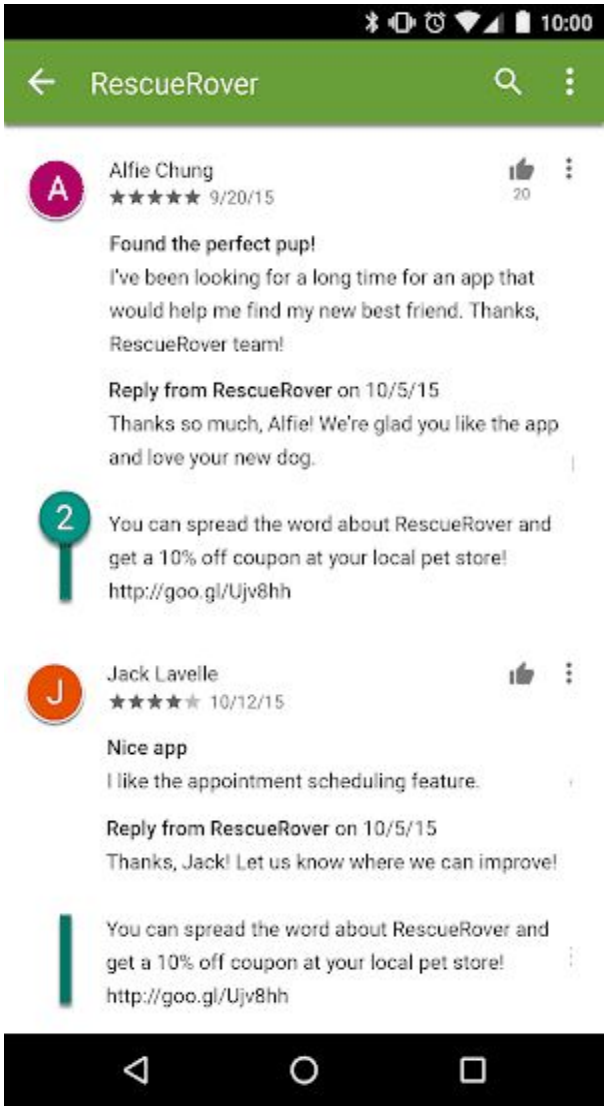
Os desenvolvedores não podem tentar manipular a colocação de apps no Google Play. Isso inclui, entre outras práticas, melhorar os indicadores dos produtos por meios ilegítimos como instalações, notas e avaliações fraudulentas ou induzidas por incentivo.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Pedir que os usuários deem um nota ao app e oferecer um incentivo para isso:



① Esta notificação oferece um desconto ao usuário em troca de uma nota alta.

Enviar várias notas para influenciar a colocação do app no Google Play
Enviar ou incentivar os usuários a enviar avaliações que incluam conteúdo inadequado, como afiliados, cupons, códigos de jogos, endereços de e-mail ou links para sites ou outros apps:



② Esta avaliação incentiva os usuários a promover o app Rescue Rover, oferecendo um cupom.

As notas e avaliações são indicadores da qualidade do app. É importante para os usuários que essas informações sejam autênticas e relevantes. Veja algumas práticas recomendadas sobre como responder às avaliações dos usuários:

Mantenha sua resposta focada nas questões levantadas nos comentários dos usuários e não peça uma classificação melhor.
Inclua referências para recursos úteis, como um endereço de suporte ou uma página "Perguntas frequentes".

Classificações de conteúdo

Nosso sistema de classificação de conteúdo inclui classificações oficiais da Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês) e foi desenvolvido para

ajudar os desenvolvedores a comunicar classificações de conteúdo localmente relevantes aos usuários.

Como as classificações de conteúdo são usadas

As classificações de conteúdo são usadas para informar os consumidores, principalmente os pais, sobre conteúdo potencialmente questionável em um app. Elas também ajudam a filtrar ou bloquear seu conteúdo em determinados territórios ou para usuários específicos quando exigido por lei. Além disso, elas ajudam a determinar a qualificação do seu app para programas especiais de desenvolvedores.

Como são atribuídas as classificações de conteúdo

Para receber uma classificação do conteúdo, é necessário preencher um questionário de classificação no Play Console com perguntas sobre a natureza do conteúdo dos seus apps. De acordo com suas respostas, o app receberá uma classificação de conteúdo nos padrões de várias autoridades competentes. Declarações falsas sobre o conteúdo levam à remoção ou suspensão do app. Por isso, é importante responder corretamente ao questionário de classificação de conteúdo.

Para evitar que seu app seja listado como "Sem classificação", preencha o questionário de classificação de conteúdo para cada novo app enviado ao Play Console e para todos aqueles que já estão ativos no Google Play. Os apps sem classificação de conteúdo serão removidos da Play Store.

Se você fizer alterações em recursos ou no conteúdo do app que afetem as respostas fornecidas no questionário de classificação do conteúdo, será necessário preencher esse documento novamente no Play Console.

Acesse a Central de Ajuda para ver mais informações sobre as diferentes autoridades de classificação e saber como preencher o questionário de classificação do conteúdo.

Contestação de classificações

Se você não concordar com a classificação atribuída ao seu app, faça uma contestação diretamente para a autoridade de classificação da IARC pelo link fornecido no e-mail do seu certificado.

Spam e recursos mínimos

Os apps precisam oferecer, no mínimo, recursos básicos e uma experiência do usuário apropriada. Os apps com falhas e que exibem outros comportamentos incompatíveis com uma experiência do usuário funcional ou que servem somente para enviar spams aos usuários ou ao Google Play não ampliam o catálogo de maneira relevante.

Spam

Não são permitidos apps que enviam spam aos usuários ou ao Google Play, como os que enviam mensagens não solicitadas. Também são proibidos os apps repetitivos ou de baixa qualidade.

Spam de mensagens

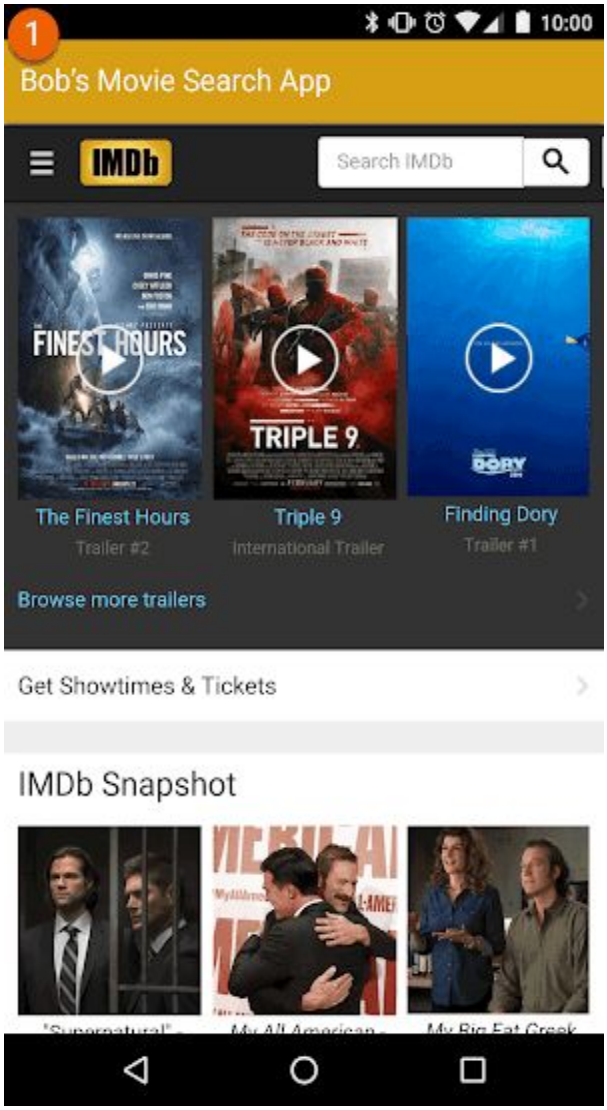
Não são permitidos apps que enviem SMS, e-mails ou outras mensagens em nome do usuário sem que este possa confirmar o conteúdo e os destinatários pretendidos.

Spam de afiliados e visualizações da Web

Não são permitidos apps com a função principal de direcionar o tráfego afiliado a um site ou fornecer uma visualização da Web de um site sem a permissão do administrador ou proprietário deste.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

> Apps com a função principal de direcionar o tráfego por referência a um site para receber crédito por inscrições ou compras do usuário no site em questão

Apps com a função principal de exibir um WebView de um site sem permissão:



① Este app se chama "Pesquisa de Filmes do Bob", mas ele só fornece um WebView do IMDb.

Conteúdo repetitivo

Não são permitidos apps que simplesmente proporcionam a mesma experiência de outros já disponíveis no Google Play. É preciso criar conteúdos ou serviços exclusivos aos apps para oferecer valor agregado aos usuários.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Não é permitido copiar conteúdo de outros apps sem adicionar valor nem conteúdo original.

Não é permitido criar vários apps com funcionalidade, conteúdo e experiência do usuário muito semelhantes. Caso os apps tenham pouco volume de conteúdo, recomendamos que os desenvolvedores criem um único app com todo o conteúdo agregado.

Não são permitidos apps criados com base em modelos, por ferramentas automatizadas ou por serviços de assistente e enviados ao Google Play pelo operador do serviço em nome de outras pessoas. Esses apps só serão permitidos se forem publicados por uma conta de desenvolvedor que seja registrada individualmente e pertença ao usuário da ferramenta automatizada, não ao operador do serviço.

Apps feitos para veicular anúncios

Não permitimos apps que tenham a finalidade principal de veicular anúncios.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps com anúncios intersticiais após cada ação do usuário, incluindo clicar e deslizar, entre outras

Recursos mínimos

Verifique se o app oferece uma experiência do usuário estável e responsiva.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps que são desenvolvidos para não fazer nada ou que não têm uma função

Recursos com problemas

Não permitimos apps com falhas, fechamentos forçados, travamentos ou que funcionem de maneira anormal.
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps que não instalam
Apps que instalam, mas não carregam
Apps que carregam, mas não são responsivos

Outros programas

Além do cumprimento das Políticas de conteúdo estabelecidas nesta Central de políticas, os apps que foram projetados para outras experiências do Android e distribuídos pelo Google Play também estão sujeitos aos requisitos da política específica ao programa. Leia a lista abaixo para verificar se essas políticas se aplicam ao seu app.

Instant Apps Android

Nosso objetivo com o Instant Apps Android é criar experiências do usuário que sejam agradáveis e descomplicadas e que, ao mesmo tempo, atendam aos mais altos padrões de privacidade e segurança. Nossas políticas foram criadas para fundamentar esse objetivo.

Os desenvolvedores que optem por distribuir Instant Apps Android pelo Google Play precisam aderir às políticas a seguir e a todas as outras políticas do programa para desenvolvedores do Google Play.

Identidade

No caso dos apps instantâneos que incluem o recurso de login, os desenvolvedores precisam integrar o Smart Lock para senhas.

Suporte a links

É obrigatório que os desenvolvedores de Instant Apps Android ofereçam suporte adequado a links para outros apps. Se apps instantâneos ou instalados tiverem links que podem direcionar a um app instantâneo, o desenvolvedor desses apps precisará direcionar os usuários para o app instantâneo em questão, em vez de capturar os links em um WebView, por exemplo.

Especificações técnicas

É obrigatório que os desenvolvedores cumpram com as especificações e os requisitos técnicos do Instant Apps Android fornecidos pelo Google, incluindo as respectivas atualizações periódicas e aqueles listados na nossa documentação pública.

Oferta de instalação do app

O app instantâneo poderá oferecer ao usuário o app instalável, mas esta não pode ser a finalidade principal dele. Ao oferecer uma instalação, os desenvolvedores precisam:

usar o ícone "Instalar app" do Material Design (em inglês) e o rótulo "Instalar" para o botão de instalação;
incluir até dois ou três avisos de instalação implícitos no app instantâneo;

evitar o uso de banners ou outras técnicas semelhantes a anúncios ao mostrar solicitações de instalação aos usuários.

Veja mais detalhes sobre apps instantâneos e diretrizes adicionais de UX nas práticas recomendadas para a experiência do usuário.

Alteração do estado do dispositivo

Os apps instantâneos não podem fazer alterações no dispositivo do usuário que permanecem após a sessão do app em questão. Por exemplo, os apps instantâneos não podem alterar o plano de fundo do usuário ou criar um widget de tela inicial.

Visibilidade do app

Os desenvolvedores precisam garantir que os apps instantâneos fiquem visíveis ao usuário de modo que ele sempre saiba quando o app está em execução no dispositivo.

Identificadores de dispositivo

Os apps instantâneos não têm permissão de acesso a identificadores de dispositivo que (1) permanecem no dispositivo após o app instantâneo ser interrompido e (2) não podem ser redefinidos pelo usuário. Alguns exemplos são:

Série da versão
Endereços mac de qualquer chip de rede
IMEI e IMSI

Se obtidos por meio da permissão de tempo de execução, os apps instantâneos poderão acessar o número de telefone. O desenvolvedor não pode tentar reconhecer o usuário usando esses identificadores nem de qualquer outra maneira.

Tráfego de rede

O tráfego de rede dentro do app instantâneo precisa ser criptografado com um protocolo TLS como HTTPS.

Famílias

O Google Play oferece uma plataforma completa para que os desenvolvedores possam exibir conteúdo de alta qualidade com classificação indicativa adequada a toda a família. Antes de enviar um app ao programa Feito para Família ou publicar conteúdo voltado para crianças na

Google Play Store, você é responsável por garantir que ele seja adequado a esse público e obedeça a toda a legislação relevante.

Saiba mais sobre o processo relacionado ao conteúdo para famílias e confira a lista de verificação interativa na Formação para criar apps de sucesso.

Como criar apps para crianças e famílias

O uso da tecnologia como uma ferramenta para melhorar a vida das famílias é cada vez maior, assim como a procura dos pais por conteúdo seguro e de alta qualidade para compartilhar com os filhos. Você pode desenvolver apps específicos para crianças ou para atrair a atenção delas. O Google Play quer ajudar você a garantir que seu app seja seguro para todos os usuários, inclusive as famílias.

A palavra "crianças" pode ter diferentes significados dependendo do local e do contexto. É importante que você consulte um advogado para ajudar a determinar quais obrigações e/ou restrições de idade podem se aplicar ao app. Você é quem mais sabe como seu próprio conteúdo funciona. Por isso, contamos com sua ajuda para garantir que os apps do Google Play sejam seguros para todas as famílias.

Os apps desenvolvidos especificamente para crianças precisam participar do programa Feito para Família. Mesmo que o app também segmente outros públicos-alvo, a participação no programa não deixará de ser uma ótima maneira de exibi-lo aos usuários certos. Se você decidir não participar do programa, ainda será necessário seguir os requisitos da Política para famílias abaixo, bem como todas as outras Políticas do programa para desenvolvedores do Google Play e o Contrato de distribuição do desenvolvedor.

Requisitos do Play Console

Público-alvo e conteúdo

Na seção Público-alvo e conteúdo do Google Play Console, você precisa indicar o público-alvo a que se destina o app antes de publicá-lo, selecionando uma opção na lista de faixas etárias fornecidas. Independentemente do que você identificar no Google Play Console, se você optar por incluir no app imagens e termos que possam ser considerados voltados para crianças, talvez isso afete a avaliação do Google Play em relação ao público-alvo declarado. O Google Play reserva-se o direito de fazer a própria análise das informações do app fornecidas por você para determinar se o público-alvo divulgado está correto.

Se você selecionar um público-alvo que inclui somente adultos, mas o Google determinar que isso é impreciso porque o app segmenta crianças e adultos, você terá a opção de deixar claro para os usuários que o app não é destinado a crianças incluindo uma etiqueta de aviso.

Só selecione mais de uma faixa etária para o público-alvo se o app tiver sido desenvolvido e for apropriado aos usuários nas faixas etárias selecionadas. Por exemplo, apps para bebês, crianças pequenas ou em idade pré-escolar precisam ter somente a faixa etária "Até 5 anos"

selecionada como público-alvo. Se o app for destinado a uma série escolar específica, escolha a faixa etária que melhor representa esse nível de ensino. Selecione apenas faixas etárias que incluam adultos e crianças, caso você realmente tenha projetado seu app para todas as idades.

Atualizações da seção "Público-alvo e conteúdo"

É possível atualizar a qualquer momento as informações do app na seção "Público-alvo e conteúdo" no Google Play Console. É necessário atualizar o app para que essas informações sejam refletidas na Google Play Store. No entanto, todas as mudanças feitas nessa seção do Google Play Console poderão ser avaliadas quanto à conformidade com as políticas antes mesmo do envio da atualização do app.

Recomendamos que você informe aos usuários existentes do seu app sobre alterações no público-alvo ou sobre a ativação de recursos, como anúncios ou compras no aplicativo. Para fazer isso, use a seção "O que há de novo" na página "Detalhes do app" ou as notificações no app.

Declarações falsas no Play Console

Fazer declarações falsas no Play Console, inclusive na seção "Público-alvo e conteúdo", pode resultar na remoção ou suspensão do app. Por isso, é importante fornecer informações precisas.

Requisitos da Política para famílias

Se você tiver crianças como um dos públicos-alvo do app, será preciso cumprir os seguintes requisitos. A não conformidade com eles poderá resultar na remoção ou suspensão do app.

1. Conteúdo do app: o conteúdo disponível no app precisa ser apropriado para crianças.
2. Respostas no Google Play Console: você precisa responder com precisão às perguntas sobre o app no Google Play Console e atualizar as respostas para que reflitam corretamente qualquer mudança aplicada a ele.
3. Anúncios: caso o app exiba anúncios para crianças ou usuários de idade desconhecida, será necessário:
    usar somente SDKs de anúncios certificados do Google Play para veicular anúncios para esses usuários;
    garantir que os anúncios exibidos a esses usuários não envolvam publicidade nem remarketing com base em interesses;
    garantir que os anúncios exibidos a esses usuários apresentem conteúdo apropriado para crianças;
    garantir que os anúncios exibidos a esses usuários sigam os requisitos de formato do anúncio para famílias; e
    garantir o cumprimento de todos os regulamentos legais aplicáveis e padrões do setor relacionados à publicidade para crianças.
4. Coleta de dados: você precisa divulgar a coleta de todas as informações pessoais e confidenciais de crianças, inclusive por meio de APIs e SDKs chamados ou usados no

app. As informações confidenciais de crianças incluem informações de autenticação, dados do dispositivo, de uso, do sensor da câmera e do microfone e código do Android e de publicidade, entre outros.

5. APIs e SDKs: você precisa garantir a implementação correta de qualquer API e SDK no app.

   Os apps que segmentam somente crianças não podem conter APIs nem SDKs que não sejam aprovados para uso em serviços direcionados a esse público-alvo. Isso inclui o Login do Google (ou qualquer outro serviço das APIs do Google que acesse dados associados a uma Conta do Google), os serviços relacionados a jogos do Google Play e qualquer outro serviço de API usando a tecnologia OAuth para autenticação e autorização.

   Os apps que segmentam crianças e adultos não podem implementar APIs nem SDKs que não sejam aprovados para uso em serviços direcionados a crianças, a menos que sejam usados por trás de uma tela neutra de informações de idade ou implementados de uma maneira que não resulte na coleta de dados das crianças (por exemplo, fornecendo o Login do Google como um recurso opcional). Todos os usuários precisam ter acesso ao app e a uma parte significativa da funcionalidade dele.
6. Política de Privacidade: é preciso exibir um link para a Política de Privacidade na página "Detalhes do app". Esse link precisa estar sempre visível enquanto o app estiver disponível na Google Play Store. Além disso, ele precisa direcionar o usuário a uma Política de Privacidade que descreva com precisão o uso e a coleta de dados do app, entre outras informações.
7. Restrições especiais:

   Caso o app use o recurso de realidade aumentada, você precisará incluir um aviso de segurança imediatamente após a abertura da seção de RA. O aviso precisa exibir as seguintes informações:

   Uma mensagem apropriada sobre a importância da supervisão dos pais
   Um lembrete para que o usuário fique atento aos perigos físicos do mundo real (por exemplo, prestar atenção no que está no entorno)

   O app não pode exigir o uso de um dispositivo não recomendado para crianças (por exemplo, Daydream e Oculus).
8. Conformidade legal: você precisa garantir que o app, incluindo APIs ou SDKs chamados ou usados por ele, esteja em conformidade com a Lei de Proteção da Privacidade On-line das Crianças (COPPA, na sigla em inglês) dos EUA, o Regulamento geral de proteção de dados (GDPR, na sigla em inglês) da UE e qualquer outra legislação ou regulamento aplicável.

Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Apps que promovem jogos para crianças na página "Detalhes do app", mas o conteúdo deles só é apropriado para adultos

Apps que implementam APIs com Termos de Serviço que proíbem o uso delas em produtos direcionados a crianças
Apps que exaltam o uso de bebidas alcoólicas, tabaco ou substâncias controladas
Apps que incluem simulações ou jogos de azar reais
Apps que incluem violência, sangue ou conteúdo chocante não apropriado para crianças
Apps que fornecem serviços de relacionamento pessoal ou aconselhamento sexual e amoroso
Apps que exibem anúncios destinados a adultos para crianças

Programa Feito para Família

Os apps desenvolvidos especificamente para crianças precisam participar do programa Feito para Família. Caso o app tenha sido projetado para todos os públicos-alvo, incluindo crianças e famílias, você também pode se inscrever para participar do programa.

Para que o app seja aceito no programa, ele precisa atender a todas as condições da Política para famílias e a todos os requisitos de qualificação do Feito para Família, bem como aqueles descritos nas Políticas do programa para desenvolvedores do Google Play e no Contrato de distribuição do desenvolvedor.

Veja mais informações sobre o processo de envio de apps para inclusão no programa.

Qualificação para o programa

Todos os apps que participam do programa Feito para Família precisam ter conteúdo e anúncios relevantes e apropriados para crianças, além de atender a todos os requisitos abaixo. Os apps aceitos no programa Feito para Família precisam estar em conformidade com todos os requisitos do programa. O Google Play reserva-se o direito, de acordo com critérios próprios, de recusar ou remover qualquer app considerado inadequado para o programa Feito para Família.

Requisitos do Feito para Família

1. Os apps precisam ter a classificação de software de entretenimento (ESRB, na sigla em inglês) "Todos", "Não recomendado para menores de 10 anos" ou equivalente.
2. É necessário divulgar com precisão os elementos interativos do app no questionário de classificação do conteúdo no Google Play Console, especificando se:
    os usuários podem interagir ou trocar informações;
    seu app compartilha informações pessoais fornecidas pelo usuário com terceiros;
    seu app compartilha a localização física do usuário com outras pessoas.
3. Caso o app use a API Android Speech, o RecognizerIntent.EXTRA_CALLING_PACKAGE precisará estar definido para o respectivo PackageName.
4. Os apps precisam usar somente SDKs de anúncios certificados pelo Google Play.
5. Os apps desenvolvidos especificamente para crianças não podem solicitar permissões de localização.

6. Os apps precisam usar o Gerenciador de dispositivos complementar (CDM, na sigla em inglês) ao solicitar Bluetooth, a menos que o app segmente apenas versões de sistema operacional (SO) não compatíveis com CDM.

Veja alguns exemplos de apps comuns que não estão qualificados para o programa:

Apps com a classificação de software de entretenimento (ESRB, na sigla em inglês) "Todos" que contêm anúncios para conteúdo de jogos de azar
Apps para pais ou responsáveis (por exemplo, rastreador de amamentação e guia de desenvolvimento)
Apps de guias para pais ou de gerenciamento de dispositivos destinados somente aos pais ou responsáveis

Categorias

Se o app for aceito para participar do Feito para Família, será possível escolher uma segunda categoria específica que o descreva. Veja as categorias disponíveis para apps do programa:

Ação e aventura: são apps/jogos de ação, incluindo jogos básicos de corrida e aventuras de contos de fadas, além de outros apps e jogos projetados para envolver o público.

Quebra-cabeças: são jogos que instigam o usuário a pensar, como quebra-cabeças, jogos de combinar, testes e outros que desafiam a memória, a inteligência ou a lógica.

Criatividade: são apps e jogos que estimulam a criatividade, incluindo desenho, pintura, programação e outras atividades de criação.

Educação: são apps e jogos desenvolvidos com a supervisão de experts em aprendizado (por exemplo, educadores, especialistas e pesquisadores). São produtos destinados a promover o conhecimento, incluindo aprendizado acadêmico, socioemocional, físico e criativo, bem como habilidades básicas de vida, pensamento crítico e solução de problemas.

Música e vídeo: são apps e jogos que têm um componente musical ou de vídeo, desde apps de simulação de instrumentos até os que fornecem conteúdo de áudio e vídeo musical.

Faz de conta: são apps e jogos em que o usuário pode fingir assumir um papel, como ser chef de cozinha, responsável por uma criança, príncipe/princesa, bombeiro, policial ou um personagem fictício.

Anúncios e monetização

As políticas abaixo se aplicam a qualquer publicidade (incluindo seus apps e os de terceiros), ofertas de compras no aplicativo ou qualquer outro conteúdo comercial (como a veiculação paga de produtos) exibido a usuários de apps sujeitos aos Requisitos da Política para famílias e/ou aos Requisitos do Feito para Família. Além disso, o conteúdo publicitário e comercial

precisa obedecer às leis e a regulamentações aplicáveis, inclusive a quaisquer diretrizes do setor ou de autorregulamentação relevantes.

O Google Play reserva-se o direito de restringir o acesso a apps devido a táticas comerciais excessivamente agressivas.

Requisitos de formato do anúncio

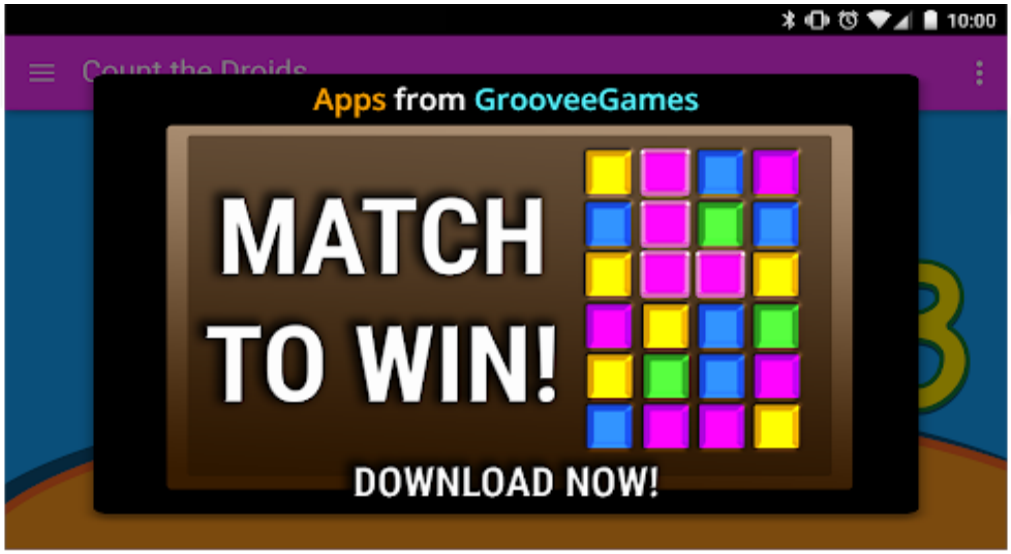
Anúncios e ofertas para compras no aplicativo não podem ter conteúdo enganoso nem ser projetados para gerar cliques acidentais de crianças. As seguintes ações são proibidas:

- Usar paredes de anúncios
- Incluir anúncios que interferem no uso normal do app ou que não podem ser fechados depois de cinco segundos
- Exibir anúncios intersticiais ou ofertas para compras no aplicativo imediatamente após a inicialização do app
- Mostrar vários canais de anúncios em uma página
- Exibir anúncios ou ofertas para compras no aplicativo que não podem ser facilmente diferenciadas do conteúdo do app
- Usar táticas chocantes ou que envolvem a manipulação emocional para incentivar a visualização de anúncios ou as compras no aplicativo
- Não fornecer uma distinção entre o uso de moedas virtuais no jogo e dinheiro real para fazer compras no aplicativo

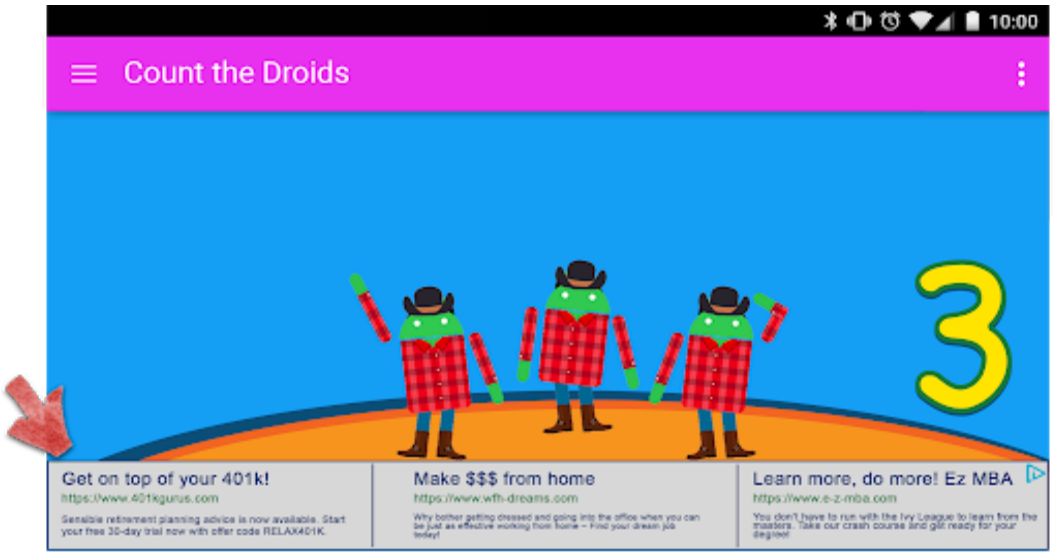
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Anúncios que se afastam do dedo do usuário quando ele tenta fechá-los

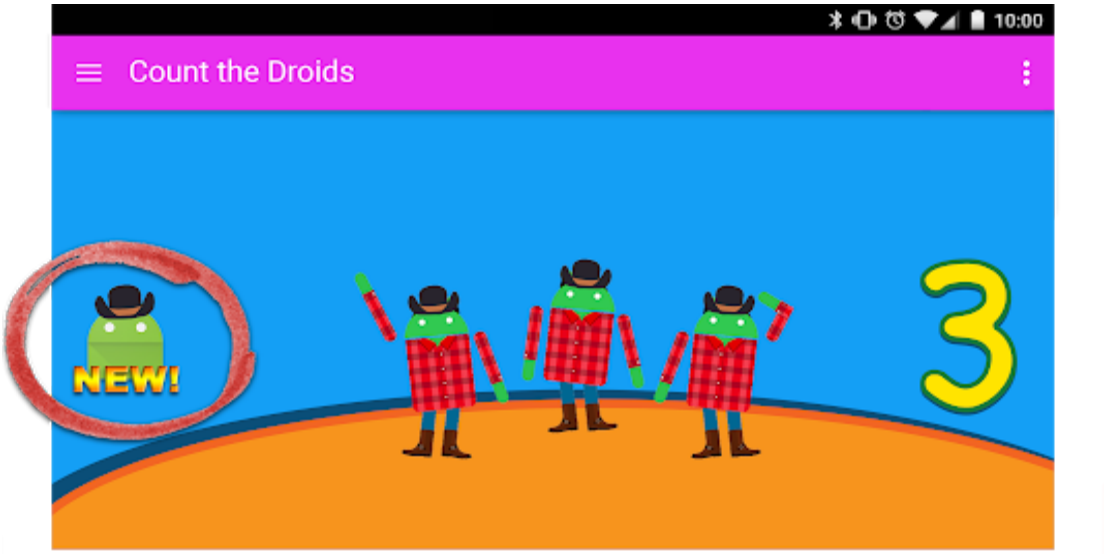
Anúncios que ocupam a maior parte da tela do dispositivo sem fornecer ao usuário uma maneira clara de dispensá-los, conforme descrito no exemplo abaixo:



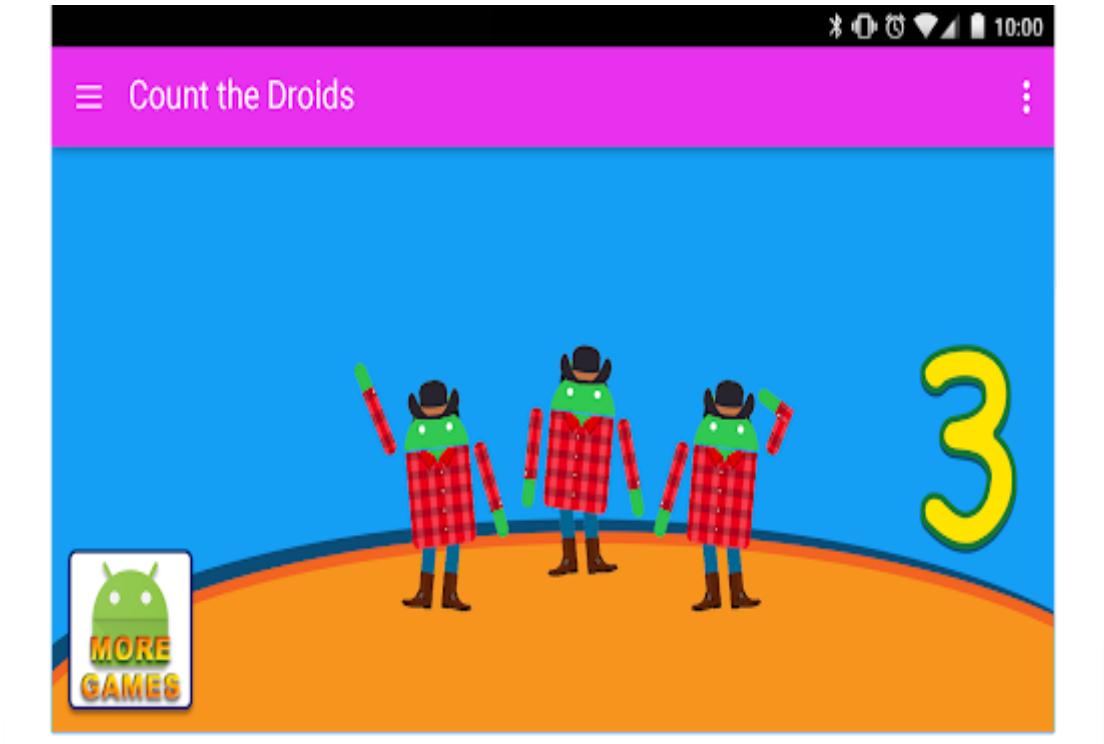
Anúncios de banner que mostram várias ofertas, conforme mostrado no exemplo abaixo:



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



Botões ou anúncios que promovem outras páginas "Detalhes do app" do Google Play, mas que podem ser confundidos com o conteúdo do app, conforme mostrado no exemplo abaixo:



Veja alguns exemplos de conteúdo impróprio de anúncios que não devem ser exibidos para crianças.

- Conteúdo de mídia impróprio: são anúncios de programas de TV, filmes, álbuns de música ou qualquer outro meio de comunicação que não sejam apropriados para crianças.
- Videogames e software para download impróprios: são anúncios de videogames e software para download que não sejam apropriados para crianças.
- Substâncias controladas ou prejudiciais: são anúncios de bebidas alcoólicas, tabaco, substâncias controladas ou prejudiciais.
- Jogos de azar: são anúncios de simulações de jogos de azar, competições ou promoções de sorteios, mesmo com participação gratuita.
- Conteúdo adulto e sexualmente sugestivo: são anúncios com conteúdo sexual e para maiores.
- Namoro ou relacionamentos: são anúncios de sites de namoro ou de relacionamento para adultos.
- Conteúdo violento: são anúncios que apresentam conteúdo violento e imagens inadequadas para crianças.

SDKs de anúncios

Somente SDKs de anúncios certificados pelo Google Play podem ser usados para veicular anúncios para crianças. Os apps do Programa Feito para Família precisam usar somente SDKs de anúncios certificados pelo Google Play. Para apps que não segmentam somente crianças, SDKs de anúncios não certificados poderão ser usados se uma tela neutra de informações de idade for exibida no app, e a veiculação de anúncios será feita somente para usuários identificados como adultos.

Consulte a página da Política do Programa de Anúncios para Famílias para saber mais sobre esses requisitos e ver a lista atual de SDKs de anúncios aprovados.

Se você usar a AdMob, consulte a Central de Ajuda da plataforma para mais detalhes sobre os produtos dela.

É sua responsabilidade garantir que o app atenda a todos os requisitos relacionados a anúncios, compras no aplicativo e conteúdo comercial. Entre em contato com seus fornecedores de SDK de anúncios para saber mais sobre as políticas de conteúdo e práticas relacionadas.

Compras no app

O Google Play autenticará novamente todos os usuários antes de fazer qualquer compra no aplicativo em apps que participam do programa Feito para Família. Essa medida busca garantir que um adulto financeiramente responsável, e não as crianças, esteja aprovando as compras.

Restrição

É sempre melhor evitar uma violação da política do que solucioná-la. No entanto, quando uma ocorre, temos o compromisso de explicar aos desenvolvedores como os apps deles podem voltar a estar em conformidade com nossas políticas. Entre em contato com nossa equipe se você identificar alguma violação ou tiver dúvidas sobre como solucioná-la.

Cobertura da política

Nossas políticas aplicam-se a qualquer conteúdo que o app do desenvolvedor exibe ou a que se vincula, incluindo quaisquer anúncios exibidos aos usuários e quaisquer conteúdos gerados por usuários que o app hospeda ou a que se vincula. Da mesma forma, essas políticas se aplicam a qualquer conteúdo da conta de desenvolvedor que for exibido publicamente no Google Play, incluindo o nome do desenvolvedor e a página de destino do site de desenvolvedor listado.

Não permitimos apps que possibilitam a instalação de outros apps nos dispositivos. Apps que fornecem acesso a outros apps, jogos ou software sem instalação, incluindo experiências e recursos fornecidos por terceiros, precisam garantir que todo o conteúdo fornecido esteja em conformidade com as políticas do Google Play. Além disso, esse material estará sujeito a análises adicionais de acordo com as políticas.

Os termos definidos usados nessas políticas têm o mesmo significado que aqueles utilizados no Contrato de distribuição do desenvolvedor (DDA). Além de estar em conformidade com essas políticas e o DDA, o conteúdo do app precisa ser classificado de acordo com nossas Diretrizes de classificação de conteúdo.

Apps que possam ser inadequados para o público em geral ou oferecer uma experiência de baixa qualidade para nossos usuários finais possivelmente não estarão qualificados para promoção no Google Play. No entanto, esses apps continuarão disponíveis no Google Play, desde que estejam em conformidade com estas políticas e com o DDA.

O Google se reserva o direito de incluir ou remover apps do Google Play. Podemos agir com base em vários fatores, incluindo padrões de comportamento prejudiciais ou risco alto de abuso. Identificamos o risco de abuso usando vários itens, como o histórico de violações anteriores, o feedback dos usuários e o uso de marcas, personagens e outros materiais conhecidos.

Processo de restrição

Se o app violar qualquer uma de nossas políticas, ele será removido do Google Play, e o desenvolvedor receberá uma notificação por e-mail com o motivo específico da remoção. Violações recorrentes ou graves dessas políticas (como malware, fraude e apps que podem

causar danos ao usuário ou ao dispositivo) ou do Contrato de distribuição do desenvolvedor (DDA, na sigla em inglês) resultarão no encerramento de contas individuais ou relacionadas.

A remoção ou as notificações administrativas podem não contemplar toda e qualquer violação da política presente no app ou no catálogo geral dele. Os desenvolvedores são responsáveis pela resolução de qualquer problema sinalizado relativo às políticas e por garantir, com a devida diligência, que o restante do app também esteja em total conformidade com as políticas. A não resolução dessas violações pode resultar em ações adicionais de restrição, incluindo a remoção permanente do app ou o encerramento da conta.

Gerenciamento e denúncia de violações da política

Se você tiver alguma dúvida ou preocupação em relação a uma remoção ou uma classificação/um comentário de um usuário, consulte os recursos abaixo ou entre em contato com nossa equipe por meio da Central de Ajuda do Google Play. No entanto, não podemos oferecer orientação jurídica ao desenvolvedor. Caso você precise desse tipo de orientação, consulte um advogado.

Verificação de apps e contestações
Como denunciar uma violação de política
Entrar em contato com o Google Play sobre o encerramento de uma conta ou a remoção de um app
Avisos cordiais
Denunciar comentários e apps impróprios
Meu app foi removido do Google Play
Para compreender os encerramentos das contas de desenvolvedor do Google Play

Developer Distribution Agreement