Política do programa para desenvolvedores

(em vigor a partir de 1º de dezembro de 2021, salvo indicação em contrário)

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 a seguir.

Conteúdo restrito

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. Isso inclui, mas não se limita a apps que promovem pedofilia ou interação inadequada com menores (por exemplo, apalpar ou acariciar).

Além disso, não são permitidos apps que têm conteúdo interessante para crianças, mas apresentam temas adultos, incluindo, mas não se limitando àqueles que exibem violência excessiva, sangue e imagens relacionadas ou que retratam ou incentivam atividades perigosas e nocivas. Também não permitimos apps que promovem uma visão negativa da própria imagem ou do corpo, incluindo aqueles que retratam cirurgia plástica, perda de peso e outras modificações estéticas à aparência física de uma pessoa para fins de entretenimento.

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.

Conteúdo inadequado

Início da vigência: 1.º de dezembro de 2021

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

Conteúdo sexual e linguagem obscena

Não são permitidos apps que contenham ou promovam conteúdo sexual ou linguagem obscena, incluindo pornografia ou qualquer conteúdo ou serviço com o objetivo de satisfação sexual. Apps ou conteúdos que aparentam promover atos sexuais em troca de remuneração também não são permitidos. O conteúdo com nudez talvez seja permitido se for principalmente para fins educacionais, documentais, científicos ou artísticos, e não apenas uma exposição sem justificativa.

Mesmo se tiver conteúdo que viole esta política e estiver indisponível em outras regiões, um app poderá ser disponibilizado para os usuários de uma região específica caso o conteúdo seja considerado apropriado nesse local.

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 sexual ou posições sexualmente sugestivas em que há pessoas nuas, desfocadas ou seminuas e/ou em que a roupa seria inadequada em um contexto público apropriado
- Imagens, animações ou ilustrações de atos sexuais ou poses sexualmente sugestivas ou a representação sexual das partes do corpo
- Conteúdo que retrata ou funciona como acessório sexual, guias sexuais, temas sexuais ilegais e fetiches
- Conteúdo obsceno ou linguagem obscena, incluindo, entre outros, palavrões, insultos, texto explícito, palavras-chave de conteúdo adulto/sexual na página "Detalhes do app" ou no app
- Conteúdo que retrata, descreve ou incentiva a bestialidade

- Apps que promovam entretenimento relacionado a sexo, serviços de acompanhantes ou outras atividades que possam ser interpretadas como realização de atos sexuais em troca de remuneração, incluindo, mas não se limitando a, serviços de namoro ou encontros sexuais compensados em que seja necessário ou esteja implícito que um participante dará dinheiro, presentes ou apoio financeiro a outro participante, como "sugar dating"
- Apps que degradam ou objetificam pessoas, como os que alegam despir ou permitir ver através das roupas, mesmo que estejam rotulados como apps de entretenimento ou brincadeira

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.

Apps com conteúdo educacional, documental, científico ou artístico (EDSA, na sigla em inglês) relacionado a nazistas podem ser bloqueados em determinados países, de acordo com as legislações e regulamentações locais.

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 ou discurso que declara que um grupo protegido é desumano, inferior ou digno de ser odiado.
- Apps que contêm insultos, estereótipos ou teorias sobre um grupo protegido ter características negativas (por exemplo, ser mal-intencionado, corrupto, mau etc.) ou que afirmam, explícita ou implicitamente, que o grupo é considerado uma ameaça.
- Conteúdo ou discurso que incentiva os outros a acreditar que pessoas devem ser odiadas ou discriminadas porque são membros de um grupo protegido.
- Conteúdo que promove símbolos de ódio, como bandeiras, símbolos, insígnias, instrumentos ou comportamentos associados a grupos de ódio.

Violência

Não são permitidos apps que retratem ou promovam violência gratuita ou outras atividades perigosas. Apps que retratam violência fictícia no contexto de um jogo, como desenhos animados, caça ou pesca, geralmente 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.

- 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 for postar algum conteúdo relacionado a terrorismo para fins educacionais, documentais, científicos ou artísticos ("EDCA"), forneça informações relevantes sobre o contexto EDCA.

Movimentos e organizações perigosos

Não permitimos que movimentos ou organizações que tenham se envolvido, se preparado ou assumido a responsabilidade por atos de violência contra civis publiquem apps no Google Play para qualquer finalidade, incluindo recrutamento.

Não permitimos apps com conteúdo relacionado a planejamento, preparação ou glorificação da violência contra civis. Caso seu app inclua conteúdo desse tipo para finalidades EDCA, ele deverá ser fornecido com informações relevantes sobre o contexto EDCA.

Eventos sensíveis

Não são permitidos apps que tratem de desastres naturais, atrocidades, crises sanitárias, conflitos, mortes ou outros eventos trágicos com pouca sensibilidade ou que gerem lucro com esses acontecimentos. Apps com conteúdo relacionado a um evento sensível geralmente serão permitidos se forem relevantes para fins educacionais,

documentais, científicos ou artísticos (EDSA, na sigla em inglês) ou tiverem o objetivo de alertar os usuários ou conscientizar sobre esse evento.

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
- Aparência de estar lucrando com um evento trágico sem benefício perceptível para as vítimas
- Apps que violem o artigo sobre requisitos para apps relacionados ao coronavírus 2019 (COVID-19)

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 que converta uma arma de fogo em 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 forneçam 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 em arma automática, ou de acionamento automático simulado.

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 contenham THC (tetra-hidrocanabinol), incluindo óleos de CBD com THC.

Tabaco e bebidas alcoólicas

Não permitimos apps que facilitem a venda de tabaco (incluindo cigarros eletrônicos e canetas vaporizadoras) ou incentivem o uso ilegal ou inadequado de álcool ou tabaco.

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 a situação social, sexual, profissional, intelectual ou atlético.
- Retratar o uso excessivo de bebidas alcoólicas de maneira favorável, incluindo a representação de consumo excessivo, compulsivo ou de competições.

Serviços financeiros

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, o cronograma de quitação, 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, empréstimos peer-to-peer e com alienação da propriedade.
- Não estão incluídos: hipotecas, financiamentos para automóveis, linhas de crédito rotativo (como cartões de crédito ou linhas de crédito pessoal).

Os apps que oferecem empréstimo pessoal, incluindo, mas não se limitando a, apps que oferecem empréstimos de maneira direta, geradores de leads e aqueles que conectam consumidores a credores terceirizados, precisam ter a categoria "Finanças" no Play Console e 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 o valor inicial e todas as taxas aplicáveis
- Uma Política de Privacidade que divulgue de forma abrangente o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis do usuário

Não são permitidos apps de empréstimo pessoal que exijam quitação em até 60 (sessenta) dias a partir da data de emissão. Definimos esse serviço como "empréstimo pessoal de curto prazo".

Empréstimos pessoais com APRs altas

Nos Estados Unidos, não são permitidos apps de concessão de empréstimo pessoal em que a taxa percentual anual (APR) 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.

Requisitos adicionais para apps de empréstimo pessoal na Índia e na Indonésia

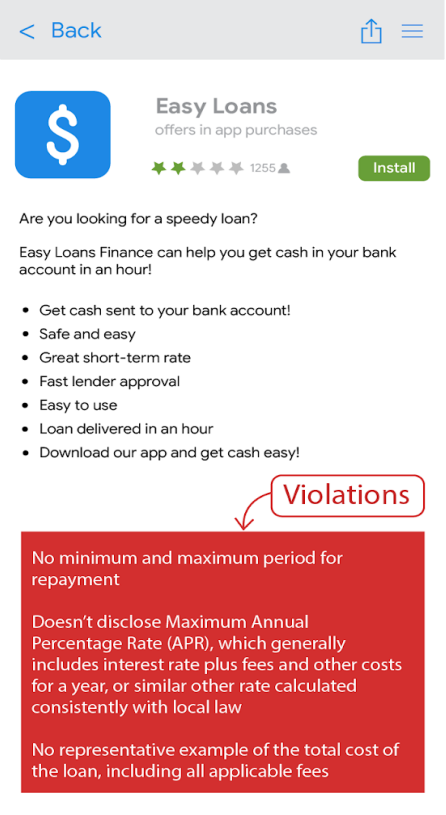
Os apps de empréstimo pessoal na Índia e na Indonésia precisam passar pelas comprovações adicionais dos requisitos de qualificação abaixo.

1. Índia
   - Preencha a declaração de app de empréstimo pessoal para a Índia e forneça a documentação de apoio necessária. Exemplo:
     - Se você tiver uma licença pelo Reserve Bank of India (RBI) para fornecer empréstimos pessoais, precisará enviar uma cópia dela para nossa análise.
     - Se você não tiver envolvimento direto em atividades de empréstimo de dinheiro e apenas fornecer uma plataforma para facilitar essas operações para empresas financeiras não bancárias registradas (NBFCs, na sigla em inglês) ou bancos aos usuários, precisará informar isso de maneira explícita na declaração.

- O nome da conta de desenvolvedor precisa refletir o nome registrado da empresa, conforme fornecido na declaração.

2. Indonésia
   - Permitimos somente apps de empréstimo pessoal licenciados ou registrados pela Autoridade de Serviços Financeiros (Otoritas Jasa Keuangan, "OJK") da Indonésia.
     - Preencha a declaração de app de empréstimo pessoal para a Indonésia e forneça a documentação de apoio da OJK.
     - O nome da conta de desenvolvedor precisa refletir o nome registrado da empresa, conforme fornecido na declaração.

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.



Jogos de azar

Permitimos apps de jogos de azar com dinheiro real, anúncios relacionados a esses tipos de jogos, programas de fidelidade com resultados gamificados e apps de fantasy games diários que atendam a determinados requisitos.

Apps de jogos de azar

Sujeito a restrições e conformidade com todas as políticas do Google Play, permitimos apps que viabilizem ou facilitem jogos de azar on-line nos seguintes países da tabela abaixo, desde que o desenvolvedor conclua o processo de inscrição para apps de jogos de azar distribuídos no Google Play, seja um operador governamental aprovado e/ou registrado como um operador licenciado pela autoridade governamental adequada no país especificado e forneça uma licença operacional válida no país especificado para o tipo de jogos de azar on-line que quer oferecer.

Só permitimos apps de jogos de azar licenciados ou autorizados que tenham os tipos de produtos de jogos de azar on-line a seguir. Consulte a tabela abaixo para ver os tipos específicos de produtos de jogos de azar permitidos em cada país:

- Jogos de cassino on-line
- Apostas esportivas
- Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas)
- Loterias
- Fantasy games diários

Austrália

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Apostas esportivas (incluindo fantasy games diários, quando legal) • Loterias

Bélgica

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias (somente de operadores governamentais)

Brasil

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Apostas esportivas (apenas corridas de cavalos) • Loterias (permissão limitada a apps aprovados publicados pela Caixa Econômica Federal)

Canadá

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line (somente de operadores governamentais) • Apostas esportivas (somente de operadores governamentais) • Loterias (somente de operadores governamentais)

Colômbia

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias (somente de operadores governamentais)

Dinamarca

Resumo	Detalhes

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas (incluindo fantasy games diários, quando legal) • Loterias

Finlândia

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line (somente de operadores governamentais) • Apostas esportivas (somente de operadores governamentais) • Loterias (somente de operadores governamentais)

França

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas) • Loterias (somente de operadores governamentais)

Alemanha

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Apostas esportivas • Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas) • Loterias (somente de operadores governamentais ou contratados afiliados)

Irlanda

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias (somente de operadores governamentais ou beneficentes)

Japão

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Apostas esportivas (corridas de cavalo, barco a motor, bicicleta e motocicleta e loterias esportivas somente de operadores governamentais) • Loterias (somente de operadores governamentais)

México

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias • Fantasy games diários

Nova Zelândia

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Apostas esportivas (somente de operadores governamentais) • Loterias (somente de operadores governamentais)

Noruega

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas (somente de operadores governamentais) • Loterias

Romênia

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias (somente de operadores governamentais)

Espanha

Resumo	Detalhes

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas (incluindo fantasy games diários, quando legal) • Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas) • Loterias (somente de operadores governamentais)

Suécia

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas • Loterias (somente de operadores governamentais)

Reino Unido

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos: • Jogos de cassino on-line • Apostas esportivas (incluindo fantasy games diários, quando legal) • Loterias

Estados Unidos

Resumo	Detalhes
Permitidos com limitações	Sujeitos aos requisitos de inscrição e licenciamento na seção "Apps de jogos de azar", os apps com os seguintes tipos de produtos de jogos de azar são permitidos em certos estados onde são legais e devidamente licenciados: • Jogos de cassino on-line • Apostas esportivas • Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas) • Loterias Se um estado ou produto de jogos de azar para um estado não estiver disponível no formulário de inscrição, o Google Play não permite a distribuição no momento. Dependendo do estado, os fantasy games diários (DFS, na sigla em inglês) podem ser regulamentados como jogos de azar nos EUA, e todos os apps desse tipo publicados nos Estados Unidos estão sujeitos aos requisitos para apps de DFS abaixo.

Para se qualificarem, os apps precisam atender 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 legislações e padrões do setor aplicáveis dos países em que é distribuído.
- O desenvolvedor precisa ter uma licença de jogos de azar válida para cada país ou estado/território em que o app é distribuído.
- O desenvolvedor não pode oferecer um tipo de jogos de azar que exceda o escopo da licença.
- O app precisa impedir que usuários menores de idade façam uso dele.
- O app precisa impedir o acesso e o uso em países, estados/territórios ou áreas geográficas não cobertos pela licença de jogos de azar fornecida ao 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 "AO" (Adult Only, "somente adultos") ou equivalente pela Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês).
- O app e página "Detalhes do app" correspondente precisam mostrar informações claras sobre a participação responsável em jogos de azar.

Outros apps de jogos com dinheiro real, concursos e torneios

Para todos os outros apps que não atendem aos requisitos de qualificação de apps de jogos de azar mencionados acima, não permitimos conteúdo ou serviços que permitam ou facilitem a participação dos usuários em jogos de azar ou o uso de dinheiro real (incluindo itens no aplicativo comprados em dinheiro) para receber um prêmio de valor monetário real. Isso inclui, entre outros, cassinos on-line, apostas esportivas, loterias e jogos que aceitam dinheiro ou oferecem prêmios em dinheiro ou outros itens de valor real (exceto os programas permitidos nos requisitos dos programas de fidelidade gamificados descritos abaixo).

Exemplos de violações

- Jogos que aceitam dinheiro em troca de uma oportunidade de ganhar um prêmio físico ou monetário
- Apps que têm elementos ou recursos de navegação (por exemplo, itens de menu, guias, botões, WebViews etc.) com uma "call-to-action" para apostar ou participar de jogos, concursos ou torneios que usam dinheiro real, como apps que convidam os usuários com palavras como "APOSTE!", "INSCREVA-SE!" ou "CONCORRA!" em um torneio para ter a chance de ganhar um prêmio em dinheiro
- Apps que aceitam ou gerenciam apostas, moedas no app, ganhos ou depósitos para apostar em ou ganhar um prêmio físico ou monetário

Programas de fidelidade gamificados

Quando for permitido por lei e não houver requisitos adicionais de licenciamento de jogos ou jogos de azar, permitimos programas de fidelidade que recompensam os usuários com prêmios reais ou o equivalente monetário, de acordo com os seguintes requisitos de qualificação da Play Store:

Para todos os apps (jogos e outros):

- Os benefícios, as cortesias ou as recompensas do programa de fidelidade precisam ser claramente complementares e subordinados a qualquer transação monetária qualificada no app (em que a transação monetária qualificada precisa ser uma transação separada real para fornecer produtos ou serviços independentes do programa de fidelidade) e não podem estar sujeitos a compras ou vinculados a modos de troca que violem as restrições da Política de jogos de azar com dinheiro real, jogos e concursos.
  - Por exemplo, nenhuma parte da transação monetária qualificada poderá representar uma tarifa ou um prêmio para participar do programa de fidelidade, e a transação monetária qualificada não poderá resultar na compra de bens ou serviços acima do preço normal.

Para apps de jogos :

- Os pontos de fidelidade ou as recompensas com benefícios, cortesias ou prêmios associados a uma transação monetária qualificada só podem ser concedidos e resgatados de forma fixa, em que a proporção é documentada de forma visível no app e também dentro das regras oficiais disponíveis publicamente para o programa. Além disso, o ganho de benefícios ou o valor de resgate **não** poderá ser apostado, concedido nem multiplicado de acordo com o desempenho no jogo ou em resultados baseados em probabilidades.

Para apps que não são de jogos:

- Os pontos de fidelidade ou as recompensas poderão ser vinculados a um concurso ou a resultados com base em probabilidades, desde que atendam aos requisitos indicados abaixo. Os programas de fidelidade com benefícios, cortesias ou recompensas associados a uma transação monetária qualificada precisam:
  - publicar as regras oficiais para o programa no app;
  - para programas que envolvam sistemas de recompensas variáveis, aleatórias ou baseadas em probabilidades, divulgar nos termos oficiais do programa 1) as chances dos programas que usam probabilidades fixas para determinar as recompensas e 2) o método de seleção (por exemplo, as variáveis usadas para determinar a recompensa) de todos os programas;
  - especificar um número fixo de vencedores, prazo fixo de inscrição e data de concessão do prêmio, por promoção, de acordo com os termos oficiais de um programa que oferece sorteios, prêmios ou outras promoções de estilo semelhante;
  - documentar todas as proporções fixas de acréscimo e resgate de pontos ou recompensas de fidelidade de maneira visível no app e nos termos oficiais do programa.

Tipo do app com programa de fidelidade	**Programas de fidelidade gamificados e prêmios variáveis**	**Recompensas de fidelidade com base em uma proporção/programação fixa**	**Termos e Condições do programa de fidelidade**	**Termos e Condições precisam divulgar as chances ou os métodos de seleção dos programas de fidelidade baseados em probabilidades**
Jogo	Não permitidos	Permitidas	Obrigatórios	N/A (apps de jogos não contêm elementos baseados em probabilidades nos programas de fidelidade)
Outros	Permitidos	Permitidas	Obrigatórios	Sim

Anúncios de jogos de azar ou jogos, concursos e torneios com dinheiro real em apps distribuídos pelo Google Play

Permitimos apps com anúncios que promovem jogos de azar e jogos, concursos e torneios com dinheiro real caso atendam aos seguintes requisitos:

- O app, o anúncio e os anunciantes precisam obedecer a todas as legislações e padrões do setor aplicáveis nos locais em que o anúncio for exibido.
- O anúncio precisa atender a todos os requisitos locais de licenciamento aplicáveis a 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.
- Se você promover um app de jogos de azar (conforme definido acima), o anúncio precisará mostrar claramente informações sobre como participar de jogos de azar de maneira responsável na página de destino, na página "Detalhes do app" ou no próprio app.
- O app não pode ter conteúdo de jogos de azar simulados (por exemplo, apps sociais de cassino ou caça-níqueis virtuais).
- O app não pode ter funções de suporte para jogos de azar nem para jogos, loterias ou torneios com dinheiro real (por exemplo, funcionalidades que ajudem com apostas, pagamentos, acompanhamento de placares/desempenho/prognósticos esportivos ou gerenciamento de fundos de jogos de azar).
- O conteúdo do app não pode promover ou direcionar os usuários a serviços de jogos de azar ou jogos, loterias ou torneios com dinheiro real.

Somente os apps que atendem a todos esses requisitos na seção listada (acima) podem incluir anúncios de jogos de azar e jogos, loterias ou torneios com dinheiro real. Os "Apps de jogos de azar" (conforme definido acima) ou os

"Apps de fantasy games diários" (conforme definido abaixo) aceitos que atendem aos requisitos de 1 a 6 acima podem incluir anúncios de jogos de azar ou de jogos, loterias ou torneios com dinheiro real.

Exemplos de violações

- Um app criado para usuários menores de idade exibe um anúncio que promove serviços de jogos de azar.
- Um jogo de cassino simulado promove ou direciona os usuários para cassinos com dinheiro real.
- Um app dedicado ao acompanhamento de prognósticos esportivos contém anúncios de jogos de azar integrados com links para um site de apostas esportivas.
- Apps com anúncios de jogos de azar que violam nossa política de anúncios enganosos, como anúncios exibidos aos usuários na forma de botões, ícones ou outros elementos interativos no app.

Apps de fantasy sport diário (DFS, na sigla em inglês)

Os apps de fantasy sports diários (DFS, na sigla em inglês), definidos conforme a lei local aplicável, só serão permitidos se cumprirem com os seguintes requisitos:

- O app 1) é distribuído apenas nos Estados Unidos ou 2) está qualificado de acordo com os requisitos para apps de jogos de azar e o processo de inscrição mencionados acima para países diferentes dos EUA.
- O desenvolvedor precisa passar pelo processo de inscrição para DFS e ser aceito para distribuir o app no Google Play.
- O app precisa estar em conformidade com todas as legislações e padrões do setor aplicáveis aos países em que é distribuído.
- O app precisa impedir que usuários menores de idade apostem ou façam transações monetárias por meio dele.
- 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 "AO" (Adult Only, "somente adultos") ou equivalente pela Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês).
- O app e a página "Detalhes do app" precisam mostrar informações claras sobre a participação responsável em jogos de azar.
- O app precisa obedecer a todas as legislações 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 em cada estado ou território dos EUA que exija isso para apps de fantasy sport diário.
- O app precisa impedir o uso em estados ou territórios dos EUA em que o desenvolvedor não tem a licença necessária para apps de fantasy sport diário.
- O app precisa impedir o uso em estados ou territórios dos EUA em que apps de fantasy sports diários são ilegais.

Atividades ilícitas

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.

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 upload de UGC;
- definir o que são conteúdos e comportamentos questionáveis (de maneira compatível com as Políticas do programa para desenvolvedores do Google Play) e proibi-los nos Termos de Uso ou nas políticas 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;
  - no caso de apps de transmissão ao vivo, o UGC questionável precisa ser removido o mais próximo possível do tempo real;
  - no caso de apps de realidade aumentada (RA), a moderação de UGC (incluindo o sistema de denúncias no app) precisa considerar o UGC de RA questionável (por exemplo, uma imagem de RA sexualmente explícita) e o local confidencial de ancoragem do RA (por exemplo, conteúdo de RA ancorado em um área restrita, como uma base militar ou uma propriedade privada em que a ancoragem de RA pode causar problemas para o proprietário);
- disponibilizar um sistema fácil de usar no app para denunciar UGCs problemáticos e tomar medidas contra esses UGCs quando apropriado;
- 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 questionável
- Apps com UGC 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

Substâncias não aprovadas

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 .

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.

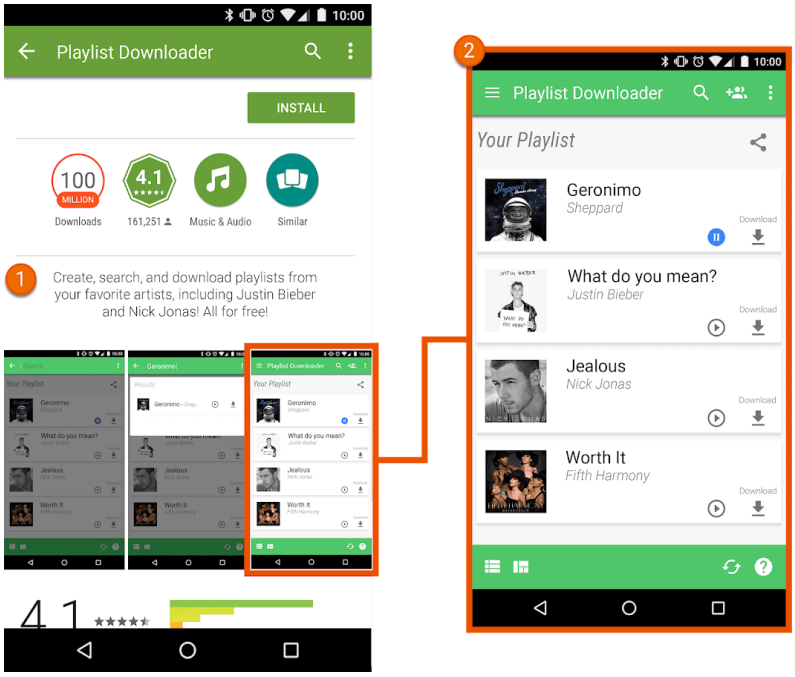
- Arte da capa de álbuns de música, videogames e livros
- Imagens de publicidade para filmes, programas de TV e jogos de video game.
- Pôsteres ou imagens de quadrinhos, desenhos animados, filmes, clipes musicais ou programas de TV.
- Logotipos de times profissionais ou de universidades.
- Fotos tiradas 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 e sensíveis de usuários, consulte os requisitos adicionais na seção "Dados pessoais e sensíveis do usuário" abaixo. Além dessas exigências do Google Play, é preciso seguir os requisitos prescritos pelas legislações de privacidade e proteção de dados aplicáveis. Se você inclui código de terceiros (por exemplo, SDKs) no seu app, é necessário garantir que o código esteja em conformidade com as Políticas do programa para desenvolvedores do Google Play.

Dados pessoais e sensíveis do usuário

Os dados pessoais e sensíveis de usuários incluem, entre outros, informações de identificação pessoal, financeiras e de pagamento; dados de autenticação; agenda; contatos; localização do dispositivo ; dados de SMS e chamadas; inventário de outros apps no dispositivo; conteúdo do microfone e da câmera; e outros dados sensíveis de uso ou do dispositivo. Caso seu app lide com dados pessoais e sensíveis de usuários, você precisa:

- limitar o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis coletados 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 no Google Play). O compartilhamento de dados pessoais e sensíveis de usuários inclui o uso de SDKs ou outros serviços de terceiros que fazem com que dados sejam transferidos para terceiros. Apps que estendem o uso de dados pessoais e sensíveis do usuário para veiculação de anúncios precisam estar em conformidade com nossa política de Anúncios ;
- lidar com todos os dados pessoais ou sensíveis de usuários de maneira segura, incluindo a transmissão desses dados por criptografia moderna (por exemplo, HTTPS);
- usar uma solicitação de permissões de execução sempre que disponível, antes de acessar os dados controlados por permissões do Android ;
- não vender dados pessoais e sensíveis do usuário.

Requisito de consentimento e divulgação em destaque

Nos casos em que os usuários não esperam que dados pessoais e sensíveis sejam necessários para fornecer ou melhorar recursos ou funcionalidades do app que estejam em conformidade com a política (por exemplo, a coleta de dados ocorre em segundo plano no app), 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 e sensíveis de usuários.

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

- precisa apresentar a caixa de diálogo de consentimento de uma maneira clara e inequívoca;
- 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 da divulgação para outra tela (por exemplo, tocar na tela para sair ou pressionar os botões home ou "Voltar");
- não pode usar mensagens que expiram ou são dispensadas automaticamente como modo de receber o consentimento do usuário.

Para atender aos requisitos da política, recomendamos que você use o modelo de divulgação em destaque a seguir quando necessário:

- "[O app] coleta/transmite/sincroniza/armazena [tipo de dados] para ativar ["recurso"], [em qual contexto]."
- *Exemplo: "O Fitness Funds coleta dados de local para ativar o monitoramento de atividades físicas, mesmo quando o app está fechado ou não está em uso, além de veicular publicidade."*
- *Exemplo: "O Call Buddy coleta dados de registro de chamadas de leitura e gravação para ativar o gerenciamento de contatos, mesmo quando o app não está em uso."*

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 coleta a localização do dispositivo, mas não tem uma divulgação em destaque que explique qual recurso usa esses dados e/ou que indique o uso do app em segundo plano
- Um app que tem uma permissão de execução que solicita acesso aos dados **antes** da divulgação em destaque que especifica para que as informações são usadas
- Um app que acessa o inventário de apps instalados do usuário e não trata esses dados como pessoais ou sensíveis sujeitos aos requisitos da Política de Privacidade, de tratamento de dados e de consentimento e divulgação em destaque

- Um app que acessa os dados do smartphone ou dos contatos de um usuário e não trata esses dados como pessoais ou sensíveis e sujeitos aos requisitos da Política de Privacidade, de tratamento de dados e de divulgação e consentimento em destaque
- Um app que registra a tela do usuário e não trata esses dados como pessoais ou sensíveis sujeitos a essa política
- Um app que coleta a localização do dispositivo e não divulga de maneira detalhada o uso desses dados nem obtém o consentimento de acordo com os requisitos acima
- Um app que coleta permissões restritas em segundo plano, inclusive para fins de rastreamento, pesquisa ou marketing, e não divulga de forma abrangente seu uso nem obtém consentimento de acordo com os requisitos acima

:

Restrições de acesso a dados pessoais e sensíveis

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 e sensíveis 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, assim como outras divulgações no app, explique os dados do usuário que o app coleta e transmite, como eles são usados e com quem são compartilhados.
O público-alvo do seu app inclui crianças.	Seu app não pode incluir um SDK que não foi aprovado para uso em serviços feitos para crianças. Acesse Como criar apps para crianças e famílias para ver a linguagem e os requisitos completos da política.
Seu app coleta ou vincula identificadores de dispositivo persistentes (por exemplo, IMEI, IMSI, número de série do chip etc.).	Identificadores de dispositivo persistentes não podem ser vinculados a outros dados pessoais e sensíveis de usuários ou identificadores de dispositivo reconfiguráveis, exceto em casos de • telefonia vinculada a uma identidade do chip (por exemplo, chamada de Wi-Fi vinculada à conta da operadora); • apps de gerenciamento de dispositivos corporativos que usam o modo proprietário do dispositivo. Esses usos precisam ser divulgados com destaque aos usuários, conforme especificado na política de Dados do usuário . Consulte este recurso para identificadores únicos alternativos. Acesse a política de Anúncios para ver diretrizes adicionais sobre o ID de publicidade do Android.

Seção "Segurança dos dados"

Todos os desenvolvedores precisam ter uma seção de segurança de dados clara e precisa em cada app, detalhando a coleta, o uso e o compartilhamento de dados do usuário. O desenvolvedor é responsável pela precisão do marcador e por manter as informações atualizadas. Quando relevante, essa seção precisa ser consistente com as divulgações feitas na Política de Privacidade do app.

Consulte este artigo para ver mais informações sobre como preencher a seção "Segurança dos dados".

Política de Privacidade

Todos os apps precisam ter uma Política de Privacidade no campo apropriado no Play Console e no próprio app. A Política de Privacidade e as divulgações no app precisam descrever de maneira detalhada como o app acessa, coleta, usa e compartilha os dados do usuário, sem se limitar aos dados divulgados na seção "Segurança dos dados". Isso precisa incluir:

- informações sobre o desenvolvedor e um ponto de contato de privacidade ou mecanismo para o envio de consultas;
- a divulgação dos tipos de dados pessoais e sensíveis dos usuários que o app acessa, coleta, usa e compartilha, além de qualquer grupo com que esses dados são compartilhados;

- procedimentos seguros de tratamento de dados pessoais e sensíveis de usuários;
- a política de retenção e exclusão de dados do desenvolvedor;
- uma indicação clara do tipo de política (por exemplo, colocar "Política de Privacidade" no título).

A entidade (desenvolvedor ou empresa) nomeada na página "Detalhes do app" precisa aparecer na Política de Privacidade ou o app precisa estar nomeado nela. Apps que não acessam dados pessoais e sensíveis de usuários também precisam enviar uma Política de Privacidade.

Sua política precisa estar disponível de forma não editável em um URL ativo (PDFs são proibidos).

Uso do ID definido pelo app

O Android apresentará um novo ID para oferecer compatibilidade com casos de uso essenciais, como análise e prevenção de fraudes. Os termos para o uso desse ID estão disponíveis abaixo.

- **Uso**: o ID definido pelo app não pode ser usado para personalização e avaliação de anúncios.
- **Associação com informações de identificação pessoal ou outros identificadores**: o ID do conjunto de apps não pode ser conectado a outros identificadores do Android (por exemplo, AAID) ou a dados pessoais e sensíveis para fins publicitários.
- **Transparência e consentimento**: a coleta e o uso do ID definido pelo app e o compromisso com estes termos precisam ser divulgados aos usuários em uma notificação de privacidade legalmente adequada, incluindo na sua Política de Privacidade. É necessário receber o consentimento legalmente válido dos usuários quando necessário. Para saber mais sobre nossos padrões de privacidade, consulte a política de Dados do usuário .

EU-U.S. Privacy Shield (Escudo de Proteção da Privacidade entre os Estados Unidos e a União Europeia) e Swiss-U.S. Privacy Shield (Escudo de Proteção da Privacidade entre os Estados Unidos e a Suíça)

Se você acessar, usar ou tratar 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) .

Você deverá monitorar 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 tratamento de informações pessoais da UE ou tome medidas razoáveis e apropriadas para restabelecer um nível adequado de proteção.

Desde 16 de julho de 2020, o Google não usa mais o EU-U.S. Privacy Shield (Escudo de Proteção da Privacidade entre os Estados Unidos e a União Europeia) para transferir dados pessoais originados no Espaço Econômico Europeu ou no Reino Unido para os Estados Unidos. Saiba mais. Veja outras informações na Seção 9 do Contrato de distribuição do desenvolvedor (DDA, na sigla em inglês).

Permissões

As solicitações de permissões e de APIs que acessam informações sensíveis precisam fazer sentido para os usuários. O app só pode solicitar permissões e APIs que acessam informações sensíveis necessárias para implementar recursos ou serviços atuais promovidos na página "Detalhes do app". Não use permissões ou APIs que acessam informações sensíveis com acesso a dados do usuário ou do dispositivo para finalidades ou recursos não revelados, não implementados ou não permitidos. Dados pessoais ou confidenciais acessados com o uso de permissões ou APIs que acessam informações sensíveis nunca podem ser vendidos.

Solicite permissões e APIs que acessam informações sensíveis para acessar dados de acordo com o contexto (via solicitações incrementais). 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 perigosas , especiais , de assinatura ou conforme documentado abaixo. Elas estão sujeitas aos seguintes requisitos e restrições adicionais:

- Os dados confidenciais do usuário ou do dispositivo acessados com o uso 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, desde que notifique os usuários de forma legalmente adequada. 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.
- É expressamente proibido o uso de permissões em violação às práticas recomendadas de permissões do app para desenvolvedores Android ou às políticas existentes, inclusive o Abuso de privilégios elevados .

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 sensíveis de usuários sujeitos à política de Informações pessoais e sensíveis 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", "Telefone" 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" antes de 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 ficará "corrompido" ou não poderá ser usado. A transferência, o compartilhamento ou o uso licenciado desses dados só pode ocorrer para fornecer os recursos principais ou serviços dentro 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 extrair dados atribuídos às permissões de registro de chamadas ou SMS.

Permissões de localização

A localização do dispositivo é considerada um dado pessoal e sensíveis do usuário, sujeita às políticas de Informações pessoais e sensíveis e Localização em segundo plano 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 em 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, por exemplo, "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 .

Para saber mais sobre os requisitos da política, confira este artigo de ajuda .

Permissão de acesso a todos os arquivos

Os arquivos e atributos de diretório no dispositivo de um usuário são considerados dados pessoais e sensíveis dele e estão sujeitos à política de informações pessoais e sensíveis e aos seguintes requisitos:

- Os apps só podem solicitar acesso ao armazenamento dos dispositivos que seja fundamental para o funcionamento. Eles não podem fazer isso em nome de terceiros para fins não relacionados à funcionalidade principal do app para o usuário.
- Os dispositivos Android com a versão R ou mais recente precisarão da permissão MANAGE_EXTERNAL_STORAGE para gerenciar o acesso no armazenamento compartilhado. Todos os apps direcionados ao R que solicitam acesso amplo ao armazenamento compartilhado ("Acesso a todos os arquivos") precisam passar por uma análise de acesso apropriada antes da publicação. Os apps que podem usar essa permissão precisam solicitar claramente que os usuários ativem a opção "Acesso a todos os arquivos" nas configurações de "Acesso especial ao app". Para saber mais sobre os requisitos do R, confira este artigo de ajuda .

Permissão de visibilidade do pacote (app)

O inventário dos apps instalados consultados em um dispositivo são considerados dados pessoais e sensíveis, sujeitos à política de Informações pessoais e sensíveis e aos seguintes requisitos:

Os apps que têm a finalidade principal de lançar, pesquisar ou interoperar com outros apps podem ter visibilidade do escopo apropriado para outros apps instalados no dispositivo, conforme descrito abaixo:

- **Ampla visibilidade do app**: é a capacidade de um app de ter uma visibilidade extensa (ou "ampla") dos apps instalados ("pacotes") em um dispositivo.
  - Para apps destinados à API de nível 30 ou mais recente , a visibilidade ampla para apps instalados com a permissão QUERY_ALL_PACKAGES é restrita a casos de uso específicos em que o reconhecimento e/ou interoperabilidade com qualquer um ou todos os apps no dispositivo são necessários para que ele funcione.
    - Não será possível usar QUERY_ALL_PACKAGES se o app puder operar com uma declaração de visibilidade do pacote com escopo segmentado . Por exemplo, consultar e interagir com pacotes específicos em vez de solicitar uma visibilidade ampla.
  - O uso de métodos alternativos para aproximar o nível de visibilidade ampla associado à permissão QUERY_ALL_PACKAGES também está restrito à funcionalidade principal do app apresentada para o usuário e à interoperabilidade com todos os apps descobertos por esse método.
  - Consulte este artigo da Central de Ajuda e veja os casos autorizados para o uso da permissão QUERY_ALL_PACKAGES.
- **Visibilidade limitada do app**: quando um app minimiza o acesso aos dados, ao consultar apps específicos usando métodos mais segmentados (em vez de "amplos"). Por exemplo, consultar apps específicos que atendam à declaração do manifesto do app. É possível usar esse método para consultas nos casos em que o app tenha interoperabilidade em conformidade com a política ou gerenciamento desses apps.
- A visibilidade do inventário de apps instalados em um dispositivo precisa estar diretamente relacionada à finalidade ou funcionalidade principal que os usuários acessam no app.

Os dados de inventário de apps consultados nos apps distribuídos no Google Play nunca poderão ser vendidos nem compartilhados para análise ou monetização de anúncios.

API de acessibilidade

A API de acessibilidade não pode ser usada para:

- mudar as configurações do usuário sem permissão, a menos que autorizado pela família ou responsável com um app de controle dos pais ou por administradores autorizados com um software de gerenciamento empresarial;
- impedir que os usuários desativem ou desinstalem apps ou serviços;
- contornar os controles e as notificações de privacidade integrados do Android;
- mudar ou usar a interface do usuário de maneira enganosa ou que viole as Políticas para desenvolvedores do Google Play.

O uso da API de acessibilidade precisa ser documentado na página "Detalhes do app".

Diretrizes para IsAccessibilityTool

Os apps com funcionalidades básicas destinadas a oferecer apoio direto às pessoas com deficiências estão qualificados para usar o **IsAccessibilityTool** e, assim, se autodesignar publicamente como "app de acessibilidade".

Os apps sem qualificação para usar o **IsAccessibilityTool** não podem incorporar o sinalizador e precisam atender aos requisitos de consentimento e divulgação em destaque conforme descrito na política de Dados do usuário já que o recurso relacionado à acessibilidade não é óbvio para o usuário. Consulte o artigo da Central de Ajuda API AccessibilityService para mais informações.

Quando possível, os apps precisam usar APIs e permissões com escopos mais limitados em vez da API de acessibilidade para alcançar a funcionalidade desejada.

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 .

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

Apps ou código de terceiros (por exemplo, SDKs) com linguagens interpretadas (JavaScript, Python, Lua etc.) carregadas em tempo de execução (por exemplo, não empacotadas com o app) não podem permitir possíveis violações das políticas do Google Play.

Não são permitidos códigos que introduzam ou explorem vulnerabilidades de segurança. Confira o Programa de melhoria da segurança dos aplicativos para saber mais sobre os problemas de segurança mais recentes sinalizados para os desenvolvedores.

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 não estão qualificados para a lista de permissões e tentam ignorar o gerenciamento de energia do sistema
- Apps que facilitam serviços de proxy para terceiros, o que só pode ser feito se esse for o objetivo principal do app
- Apps ou código de terceiros (por exemplo, SDKs) que fazem download de código executável (como arquivos dex ou código nativo) de uma fonte que não seja o Google Play
- Apps que instalam outros apps em um dispositivo sem o consentimento prévio do usuário
- Apps que facilitam a distribuição ou instalação de software malicioso ou contêm links para esse tipo de software
- Apps ou código de terceiros (por exemplo, SDKs) contendo um WebView com interface JavaScript adicionada que carrega conteúdo da Web não confiável (por exemplo, URL http://) ou URLs não verificados de fontes não confiáveis (por exemplo, URLs obtidos com intents não confiáveis).

Comportamento enganoso

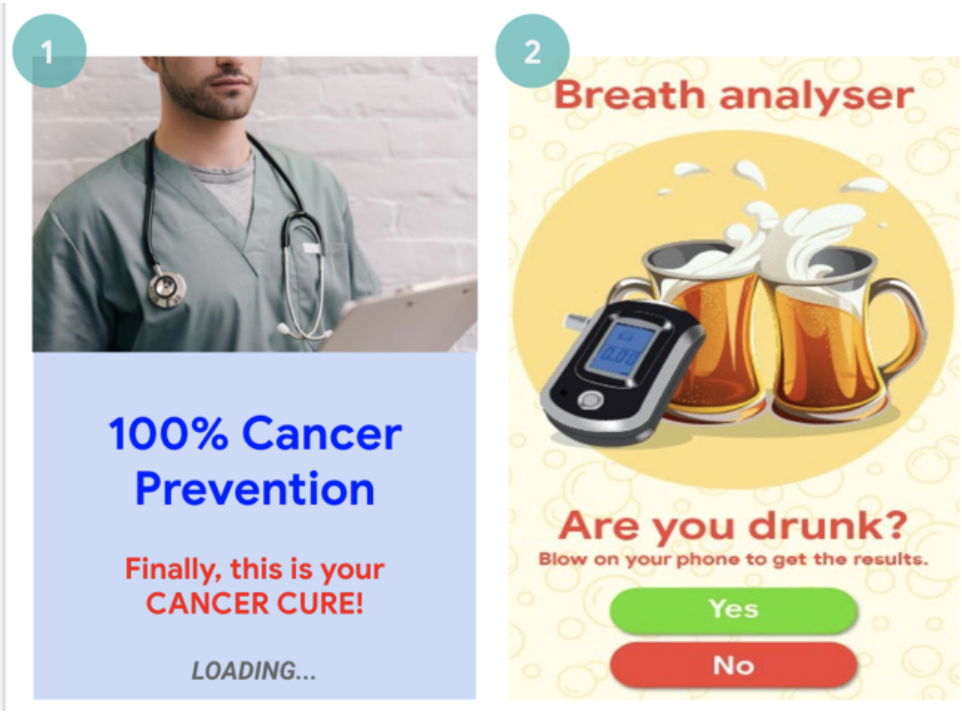
Não são permitidos apps que tentam enganar os usuários ou permitem comportamento desonesto, incluindo, mas não se limitando a, apps com um recurso impossível. Os apps precisam incluir divulgação, descrição e imagens/vídeos precisos de suas funcionalidades em todos os metadados. Os apps não podem tentar imitar a funcionalidade ou os avisos do sistema operacional ou de outros apps. As alterações nas configurações do dispositivo precisam ter o conhecimento e consentimento do usuário e ser reversíveis por ele.

Declarações enganosas

Apps que contenham informações ou declarações falsas ou enganosas, inclusive 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
- Apps com conteúdos ou recursos médicos ou relacionados à saúde que sejam enganosos ou potencialmente perigosos
- Apps que alegam ter funcionalidades impossíveis de serem implementadas (por exemplo, apps repelentes de insetos), mesmo que sejam representados como pegadinhas, dissimulações, piadas etc.
- Apps categorizados incorretamente, incluindo, mas não se limitando a, classificação ou categoria do app
- 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
- 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



(1) O app faz declarações médicas ou relacionadas à saúde (cura do câncer) que são enganosas.
(2) O app alega ter funções impossíveis de serem implementadas (usar o smartphone como bafômetro).

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 que seja enganoso de alguma forma, incluindo, entre outros, apps que gerem ou facilitem a geração de cédulas de identidade, 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 do app deve atender à expectativa razoável e precisa do usuário.

O download de recursos adicionais do app (por exemplo, de itens em jogos) só poderá ser feito 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.

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

- Apps que imitam outros aplicativos ou sites para induzir os usuários a divulgar informações pessoais ou de autenticação
  - Apps que retratam ou exibem números de telefone, contatos, endereços ou informações que permitam identificar uma pessoa, sejam elas não confirmadas ou reais, de pessoas ou entidades sem o consentimento delas
- Apps com funcionalidade principal diferente com base na região geográfica, nos parâmetros do dispositivo ou em outros dados dependentes do usuário em que essas diferenças não são divulgadas em destaque para o usuário na página "Detalhes do app"
- Apps que mudam significativamente entre as versões sem alertar o usuário (por exemplo, a seção "Novidades") e atualizar a página "Detalhes do app"
- Apps que tentam modificar ou ofuscar o comportamento durante a revisão
- Apps com downloads facilitados por rede de fornecimento de conteúdo (CDN) quando não há uma solicitação ao usuário antes de começar nem é informado o tamanho do download

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 acontecimentos polêmicos ou delicados, 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 não possa 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 manifestação durante um evento politicamente sensível.
- 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.

(1) O app oferece funcionalidades para alterar clipes de mídia para imitar uma transmissão de notícias e adicionar pessoas famosas ou públicas ao clipe sem uma marca d'água.

Declarações falsas

Não são permitidos apps nem contas de desenvolvedor que:

- se façam passar por outra pessoa ou organização ou que deturpem ou ocultem a propriedade ou o objetivo principal;
- se envolvam 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;
- se coordenem com outros apps, sites, desenvolvedores ou contas para ocultar ou fazer declarações falsas sobre a identidade do app ou do desenvolvedor ou outros detalhes relevantes, caso o conteúdo do app se relacione a política, questões sociais ou assuntos de interesse público.

Malware

Nossa política contra malware é simples: o ecossistema Android, inclusive a Google Play Store, e os dispositivos do usuário não podem apresentar comportamentos maliciosos (ou seja, malware). Com base nesse 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 dele ou um dispositivo em risco. Isso inclui aplicativos potencialmente nocivos (PHAs), binários ou modificações do framework que consistem em categorias como cavalos de troia, phishing, apps de spyware, entre outras. É importante destacar que estamos sempre 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 do framework podem ser nocivos e gerar um comportamento malicioso, mesmo que essa não tenha sido a intenção. Eles 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 do framework 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 framework 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 intencionalmente 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 ocultando acordos de divulgação ou mensagens SMS da operadora de telefonia móvel com notificações sobre cobranças ou confirmações de assinaturas.

Alguns códigos, apesar de tecnicamente expor o envio de SMS, também apresenta um comportamento adicional que permite 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, na sigla em inglês) 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 incluir 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 interceptada para evitar que os usuários percebam a transação financeira.

Stalkerware

É um código que coleta e/ou transmite dados de usuário pessoais ou sensíveis de um dispositivo sem o devido consentimento ou aviso e não exibe uma notificação contínua de que isso está acontecendo.

Apps de stalkerware segmentam os usuários de dispositivos, monitorando dados pessoais ou sensíveis e transmitindo ou tornando esses dados acessíveis a terceiros.

Os únicos apps de vigilância aceitáveis são os projetados ou comercializados exclusivamente para o monitoramento dos filhos pelos pais ou para o gerenciamento de empresas, desde que atendam totalmente aos requisitos descritos abaixo. Não é permitido usá-los para monitorar outras pessoas (um cônjuge, por exemplo), mesmo com conhecimento ou permissão delas e independentemente de os apps exibirem uma notificação contínua.

Os apps distribuídos na Play Store que não são de stalkerware e que monitoram ou rastreiam o comportamento de um usuário em um dispositivo precisam obedecer aos seguintes requisitos:

- Eles não podem se apresentar aos usuários como soluções de vigilância secreta ou de espionagem.
- Eles não podem usar técnicas de cloaking ou ocultar o comportamento de rastreamento nem tentar enganar os usuários sobre essa funcionalidade.
- Eles precisam obrigatoriamente apresentar aos usuários uma notificação contínua sempre que estiverem em execução, com um ícone que identifique o app facilmente.
- Os apps e as páginas "Detalhes do app" no Google Play não podem fornecer meios de ativar nem acessar funcionalidades que violem esses termos, como links a um APK não compatível hospedado fora da plataforma.
- 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.

Negação de serviço (DoS, na sigla em inglês)

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 contra 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 download de PHAs 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, conseguindo privilégios elevados ou alterando ou desabilitando 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 são 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 não executam outras 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 permita comportamentos classificados em uma das outras categorias de malware. Por exemplo, se um app permitir o carregamento dinâmico de código, e o código carregado dinamicamente extrai mensagens de texto, o app será classificado como malware "backdoor".

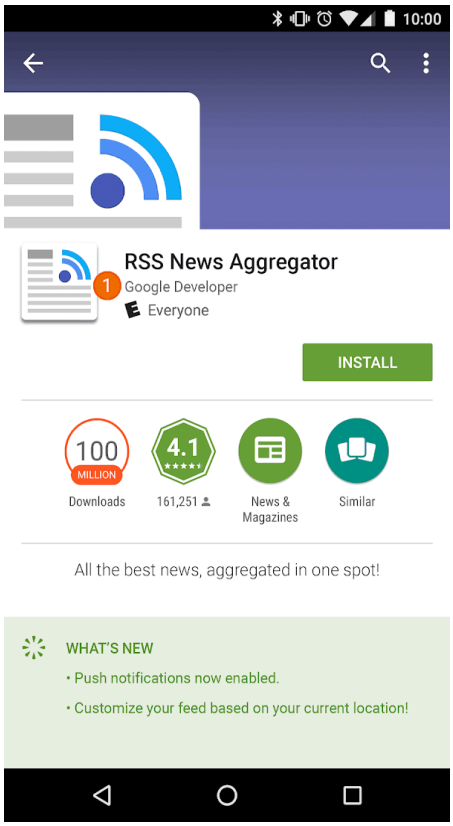
Porém, se um app permitir a execução arbitrária de código, mas não tivermos motivos para acreditar que esse código tenha sido adicionado com o objetivo de realizar um comportamento malicioso, o app será considerado vulnerável, e não malware "backdoor". Nesse caso, será solicitado que o desenvolvedor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

Falsificação de identidade

Não permitimos apps que enganem os usuários ao se passarem por outra pessoa (por exemplo, outro desenvolvedor, empresa, entidade) ou outro app. Não insinue que seu app está relacionado ou autorizado por uma pessoa sem a permissão dela. Tenha cuidado para não usar ícones, descrições, títulos ou elementos no app que possam enganar os usuários sobre o relacionamento do app com outra pessoa ou outro 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.

- Desenvolvedores que indicam falsamente uma relação com outra empresa ou desenvolvedor:



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 .

Mobile Unwanted Software

No Google, acreditamos que, se o foco está no usuário, todo o resto é consequência. Nos princípios de software e na política de software indesejado, apresentamos recomendações gerais para softwares que proporcionam uma ótima experiência ao usuário. Essa política se baseia na política de software indesejado do Google e descreve os princípios do ecossistema Android e da Google Play Store. Qualquer software que viole tais princípios é potencialmente prejudicial para a experiência do usuário. Nós tomaremos as medidas para proteger esses usuários.

Conforme mencionado na política de software indesejado, descobrimos que a maioria dos softwares indesejados tem uma ou mais das mesmas características básicas:

- São enganosos, prometem um valor que não é fornecido.
- Tentam enganar os usuários para que estes os instalem ou aproveitam a instalação de outro programa.
- Não informam ao usuário todas as suas funções principais e significativas.
- Afetam o sistema do usuário de formas inesperadas.
- Coletam ou transmitem informações particulares sem o conhecimento dos usuários.
- Coletam ou transmitem informações particulares sem um tratamento seguro (por exemplo, transmissão por HTTPS).
- Agrupam-se com outro software e sua presença não é divulgada.

Em dispositivos móveis, o software é um código na forma de um app, binário, modificação de framework etc. Para evitar softwares prejudiciais ao ecossistema de software ou à experiência do usuário, tomaremos medidas em relação ao código que viola esses princípios.

A seguir, desenvolvemos a política de software indesejado para estender sua aplicabilidade a softwares para dispositivos móveis. Do mesmo modo, continuaremos refinando a política de software indesejado para dispositivos móveis para lidar com novos tipos de abuso.

Comportamento transparente e divulgações claras

Todos os códigos precisam cumprir as promessas feitas ao usuário. Os apps precisam fornecer todas as funcionalidades informadas. Os apps não podem confundir os usuários.

- Os apps precisam ser claros sobre a função e os objetivos.
- Explique de forma explícita e clara ao usuário quais alterações serão feitas pelo app no sistema. Permita que os usuários analisem e aprovem todas as opções e mudanças significativas da instalação.
- O software não pode deturpar o estado do dispositivo para o usuário, por exemplo, alegando que o sistema está em estado crítico de segurança ou infectado com vírus.
- Não use atividades inválidas criadas para aumentar o tráfego de anúncios e/ou as conversões.
- Não permitimos apps que enganem os usuários ao se passarem por outra pessoa (por exemplo, outro desenvolvedor, empresa, entidade) ou outro app. Não insinue que seu app está relacionado ou autorizado por uma pessoa sem a permissão dela.

Exemplos de violação:

- Fraude de anúncio
- Engenharia social

Proteção dos dados do usuário

Divulgue com clareza e transparência o acesso, o uso, a coleta e o compartilhamento de dados pessoais e confidenciais do usuário. As aplicações dos dados do usuário precisam estar de acordo com todas as políticas relevantes sobre o assunto, quando aplicáveis, e é necessário tomar todas as precauções para proteger esses dados.

- Dê aos usuários a oportunidade de concordar com a coleta de dados antes de começar a coletá-los e enviá-los do dispositivo, incluindo dados sobre contas de terceiros, e-mail, número de telefone, apps instalados, arquivos, localização e outros dados pessoais e confidenciais que o usuário não espera que sejam coletados.
- Os dados pessoais e confidenciais do usuário coletados precisam ser tratados de maneira segura, inclusive por meio de criptografia moderna (por exemplo, por HTTPS).
- O software, incluindo apps para dispositivos móveis, só pode transmitir dados pessoais e confidenciais do usuário para os servidores, já que eles estão relacionados à função do app.

Exemplos de violação:

- Coleta de dados (confira a seção sobre spyware)
- Abuso de permissões restritas

Exemplos de políticas de dados do usuário:

- *Política de dados do usuário do Google Play*
- *Política de dados do usuário dos requisitos do GMS*
- *Política de dados do usuário do serviço de APIs do Google*

Não prejudique a experiência em dispositivos móveis

A experiência do usuário precisa ser simples, fácil de entender e se basear em escolhas claras feitas pelo usuário. Ela precisa apresentar uma proposta de valor clara para o usuário e não interromper a experiência divulgada ou esperada.

- Não exiba anúncios aos usuários de maneiras inesperadas que prejudiquem ou interfiram na usabilidade das funções do dispositivo nem os exiba fora do ambiente do app acionador sem que eles sejam facilmente dispensáveis e tenham o consentimento e a atribuição adequados.
- Os apps não podem interferir em outros apps nem na usabilidade do dispositivo.
- A desinstalação, quando aplicável, precisa ser clara.
- O software para dispositivos móveis não pode imitar solicitações do SO do dispositivo ou de outros apps. Não suprima alertas de outros apps ou do sistema operacional para o usuário, especialmente aqueles que informam sobre alterações no SO.

Exemplos de violação:

- Anúncios invasivos
- Uso não autorizado ou imitação de funcionalidade do sistema

---

Componente de download hostil

Em vigor a partir de 2 de fevereiro de 2022

É um código que não é um software indesejado, mas faz download de outro software indesejado para dispositivos móveis (MUwS, na sigla em inglês).

Ele pode ser um componente de downloads hostil se:

- há razões para acreditar que ele foi criado para espalhar MUwS e que fez ou contém um código que poderia fazer o download de MUwS e instalá-los; ou
- pelo menos 5% dos downloads de app feitos por ele são de MUwS com um limite mínimo de 500 observados (ou seja, 25 downloads de MUwS 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 software sejam iniciados por usuários que deram consentimento.

Fraude de anúncios

A fraude de anúncios é estritamente proibida. As interações de anúncios geradas com a finalidade de fazer uma rede de publicidade acreditar que o tráfego é do interesse autêntico do usuário são fraudes de anúncios, uma forma de

tráfego inválido. A fraude de anúncios pode ser realizada por desenvolvedores que implementam anúncios de maneiras não permitidas, como exibir anúncios ocultos, clicar automaticamente em anúncios, alterar ou modificar informações e se aproveitar de outras ações não humanas (indexadores, bots etc.) ou atividade humana projetada para produzir tráfego de anúncios inválidos. O tráfego inválido e a fraude de anúncios são prejudiciais para os anunciantes, os desenvolvedores e os usuários, além de gerar perda de confiança em longo prazo no ecossistema de anúncio para dispositivos móveis.

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.

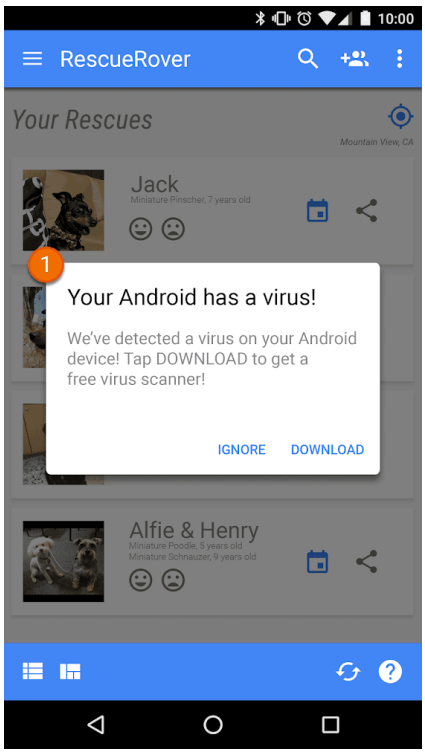
- Um app que renderiza anúncios que não são visíveis para o usuário
- Um app que gera cliques em anúncios automaticamente sem a intenção do usuário ou que produz tráfego de rede equivalente para fornecer créditos de cliques de maneira fraudulenta
- Um app que envia cliques falsos de atribuição de instalação para receber pagamentos por instalações que não se originaram na rede do remetente
- Um app que exibe anúncios pop-up quando o usuário não está na interface do app
- Declarações falsas do inventário de anúncios por um app, por exemplo, um app que comunica a redes de publicidade que está em execução em um dispositivo iOS quando, na verdade, está em um dispositivo Android; um app que declara incorretamente o nome do pacote que está sendo monetizado

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, como quando um app de uma companhia aérea notifica os usuários sobre promoções especiais ou quando um jogo notifica os usuários sobre as próprias promoções.

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 ver mais exemplos relacionados, consulte a política de anúncios.

Social Engineering

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

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

Início da vigência: 18.º de dezembro de 2021

1. Os desenvolvedores que cobram pelo download de apps no Google Play precisam usar o sistema de faturamento da plataforma como forma de pagamento dessas transações.
2. Os apps distribuídos no Google Play que solicitam ou aceitam pagamento pelo acesso a recursos ou serviços, incluindo funcionalidades do app, conteúdos ou produtos digitais (coletivamente, "compras no app") precisam usar o sistema de faturamento do Google Play para essas transações, a menos que as Seções 3 ou 8 sejam aplicáveis.

   Exemplos de recursos ou serviços de apps que exigem o uso do sistema de faturamento do Google Play incluem, entre outros, compras no app de:

   - itens (como moedas virtuais, vidas extras, mais tempo de jogo, itens complementares, personagens e avatares);
   - serviços por assinatura (como de exercícios físicos, jogos, encontros, educação, música, vídeo, upgrades e outros conteúdos);
   - conteúdo ou funcionalidades do app (como uma versão sem anúncios de um app ou novos recursos indisponíveis na versão gratuita);
   - software e serviços em nuvem (como serviços de armazenamento de dados, software de produtividade empresarial e software de gerenciamento financeiro).

3. O sistema de faturamento do Google Play não pode ser usado quando:
   a. o pagamento é principalmente:
      - para a compra ou a locação de produtos físicos (como mantimentos, roupas, utensílios domésticos, eletrônicos);
      - para a compra de serviços físicos (como serviços de transporte, limpeza, passagem aérea, academia, entrega de comida, ingressos para eventos ao vivo);
      - uma remessa referente a uma fatura de cartão de crédito ou de serviços públicos (como serviços de cabo e telecomunicações);

   b. para transferências de pessoa para pessoa, leilões on-line e doações isentas de tributos;
   c. para conteúdo ou serviços que facilitam jogos de azar on-line, conforme descrito na seção Apps de jogos de azar da política Jogos de azar com dinheiro real, jogos e concursos;
   d. o pagamento refere-se a qualquer categoria de produto considerada inaceitável de acordo com as Políticas de conteúdo da Central de pagamentos do Google.

      Observação: em alguns mercados, oferecemos o Google Pay para apps que vendem produtos e/ou serviços físicos. Para saber mais, acesse a Página do desenvolvedor do Google Pay.

4. Além das condições descritas nas seções 3 e 8, os apps não podem levar usuários a formas de pagamento que não sejam o sistema de faturamento do Google Play.Essa proibição inclui, entre outras opções, direcionar os usuários a outras formas de pagamento via:
   - páginas "Detalhes do app" no Google Play;
   - promoções no app relacionadas a conteúdo comprável;

- WebViews, botões, links, mensagens, anúncios ou outras calls-to-action no app;
- fluxos da interface do usuário no app, incluindo os de inscrição ou de criação de contas, que levam os usuários a outra forma de pagamento fora do sistema de faturamento do Google Play.

5. As moedas virtuais no app só poderão ser usadas dentro do app ou jogo em que foram compradas.
6. Os desenvolvedores precisam informar os usuários de maneira clara e precisa sobre os termos e os preços do app ou sobre os recursos ou assinaturas no app oferecidos para compra. Os preços no app precisam corresponder aos preços exibidos na interface de faturamento do Google Play voltada para o usuário. 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.
7. Os apps e jogos que oferecem mecanismos para receber itens virtuais aleatórios de uma compra, incluindo, entre outros, "loot boxes", precisam divulgar claramente as chances de receber esses itens antes e perto de efetuarem o pagamento.
8. A menos que as condições descritas na Seção 3 sejam aplicáveis, os desenvolvedores de apps distribuídos no Google Play em smartphones e tablets que solicitem ou aceitem pagamentos de usuários na Coreia do Sul para acessar compras no app poderão oferecer aos usuários um sistema de faturamento em app adicional para essas transações se preencherem o formulário de declaração para sistemas de faturamento em apps adicionais e aceitarem os termos e requisitos do programa.

Observação: para ver os cronogramas e as Perguntas frequentes sobre esta política, acesse nossa Central de Ajuda.

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:

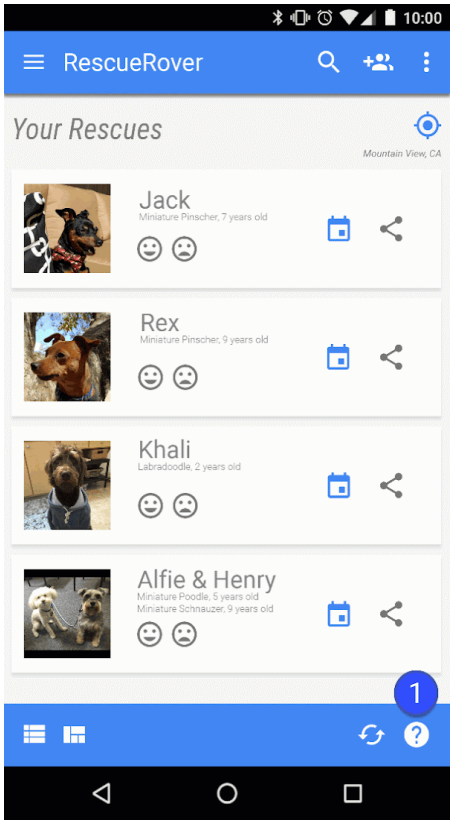
- O uso ou coleta de dados de local do dispositivo com base em permissão para fins publicitários precisa estar claro para o usuário e documentado na Política de Privacidade obrigatória do app. Isso inclui links para as Políticas de Privacidade relevantes da rede de publicidade que abordem o uso desse 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 estar claro para o usuário qual app veicula cada anúncio.

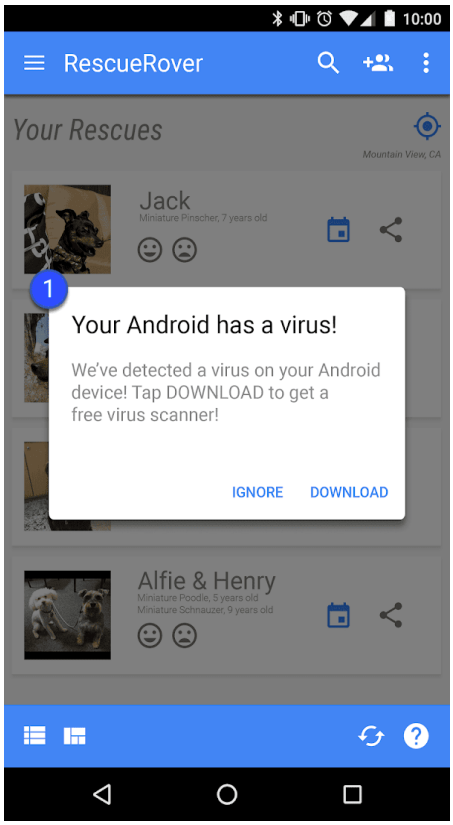
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

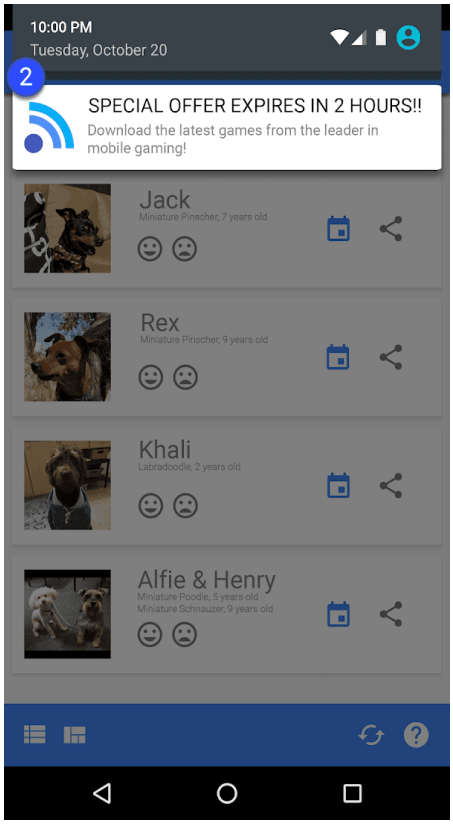
- Anúncios que imitam a interface do usuário de um app:



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

Anúncios invasivos são exibidos aos usuários de maneiras inesperadas, que podem resultar em cliques acidentais ou prejudicar ou interferir na usabilidade das funções do dispositivo.

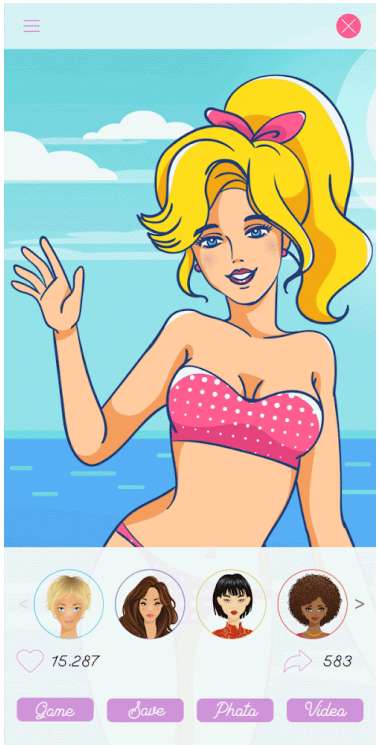
É proibido forçar um usuário a clicar em um anúncio ou enviar informações pessoais para fins publicitários antes de usar o app por completo. Os anúncios intersticiais só podem ser exibidos dentro do app que os veicula. Caso seu app exiba anúncios intersticiais ou outros anúncios que interfiram no uso 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.

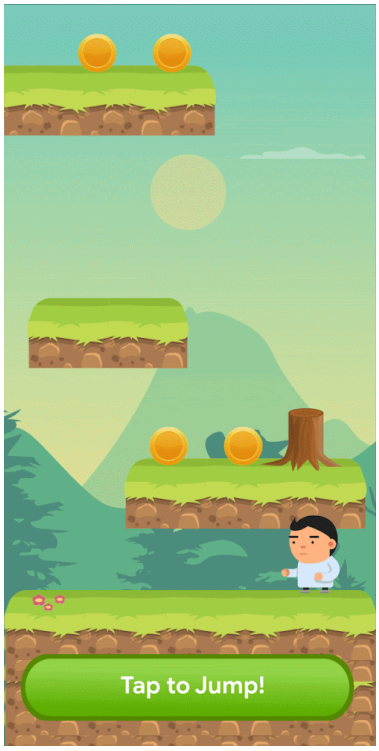
- Anúncios que ocupam a tela inteira ou interferem na utilização normal e não fornecem um meio claro de dispensar o anúncio:

① O anúncio não tem um botão para dispensar.

- Anúncios que forçam o usuário a clicar usando um falso botão "Dispensar" ou que aparecem repentinamente em áreas do app, independentemente do usuário tocar em outra função



- Anúncios que usam um botão "Dispensar" falso



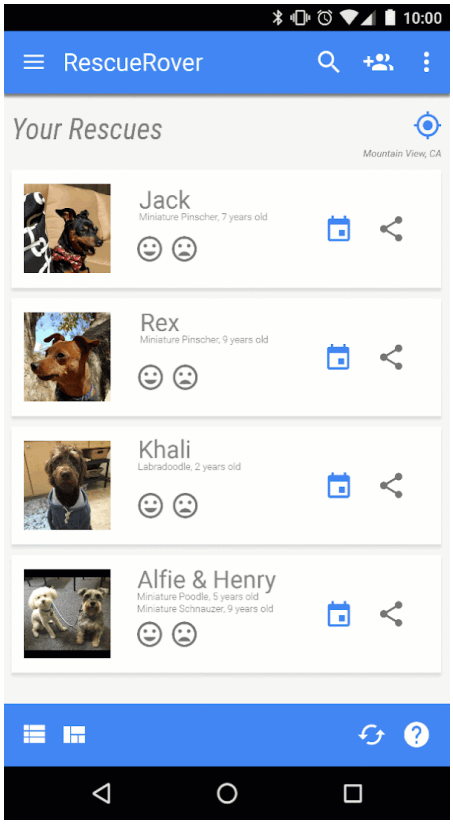
Anúncios que aparecem repentinamente em uma área em que o usuário está acostumado a tocar para funções no app

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.

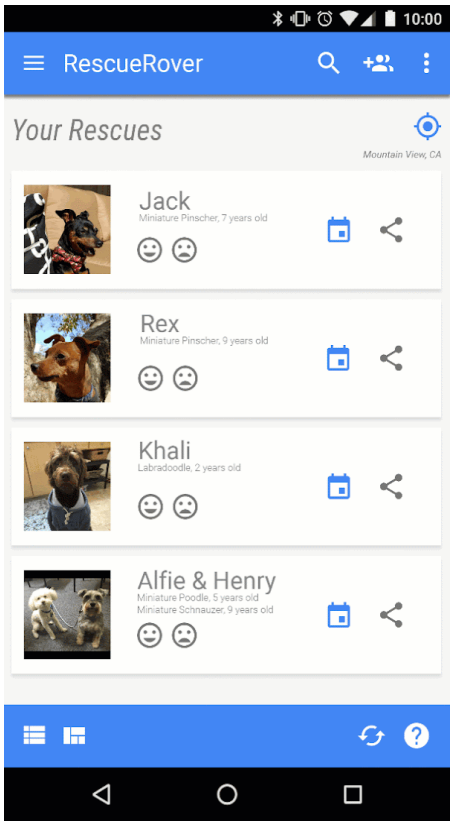
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- 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 home ou por outros recursos projetados especificamente para sair do app:

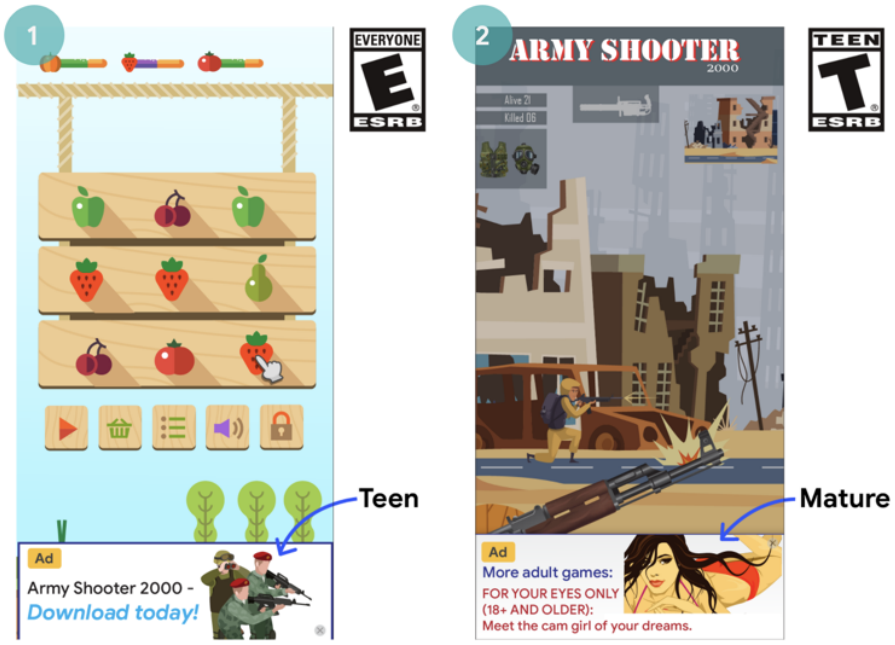


Descrição: O usuário tenta sair do app e navegar até a tela inicial, mas em vez disso, o fluxo esperado é interrompido por um anúncio.

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 O anúncio é inadequado (Adolescente) para o público-alvo do app (maiores de 7 anos).

② O anúncio é inadequado (Adulto) para o público-alvo do app (maiores de 12 anos).

Uso do ID 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 (AAID, na sigla em inglês) 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 ID.
- **Associação a informações de identificação pessoal ou outros identificadores**.
  - Uso de publicidade: o identificador de publicidade pode não estar conectado a identificadores de dispositivo permanentes (por exemplo: endereço MAC, IMEI etc.) para qualquer finalidade publicitária. O identificador de publicidade só pode ser conectado a informações de identificação pessoal com o consentimento explícito do usuário.
  - Uso do Google Analytics: o identificador de publicidade só pode ser conectado a informações de identificação pessoal ou associado a identificadores de dispositivo permanentes (por exemplo: endereço MAC, IMEI etc.) com o consentimento explícito do usuário. Leia a política de Dados do usuário para mais orientações sobre identificadores de dispositivos persistentes.
- **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.
  - 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.
  - Em dispositivos mais novos, quando um usuário exclui o identificador de publicidade do Android, o identificador é removido. Qualquer tentativa de acessar o identificador receberá uma sequência de zeros. Um dispositivo sem um identificador de publicidade não pode ser conectado a dados vinculados ou derivados de um identificador de publicidade anterior.
- **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 a Política do programa para desenvolvedores do Google Play, 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 ID de publicidade (quando disponível em um dispositivo) em vez de outros identificadores de dispositivo para fins publicitários.

Inscrições

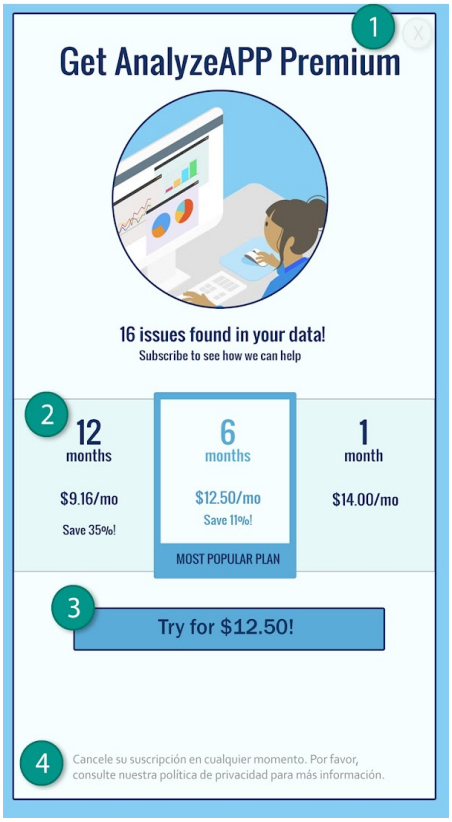
Os desenvolvedores não podem enganar os usuários sobre nenhum serviço ou conteúdo de assinatura oferecido no app. É fundamental fornecer informações claras em qualquer promoção no app ou na tela de apresentação. Não permitimos apps que sujeitem os usuários a experiências de compra enganosas ou manipuladoras (incluindo compras no app ou assinaturas).

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 com mais destaque
- Preços e termos da assinatura que não estão completamente no idioma local
- 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 "Teste gratuito" ou "Teste a assinatura premium gratuitamente por três dias" para uma assinatura com cobrança recorrente automática
- Várias telas no fluxo de compra que levam os usuários a clicar acidentalmente no botão de inscrição

Exemplo 1:



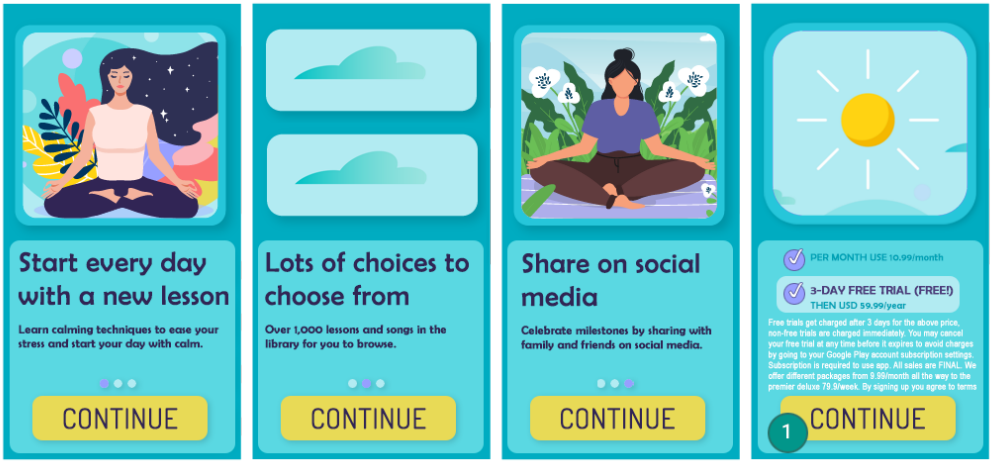
① O botão de dispensar não é claramente visível, e talvez os usuários não entendam que podem acessar recursos sem aceitar a oferta de assinatura.

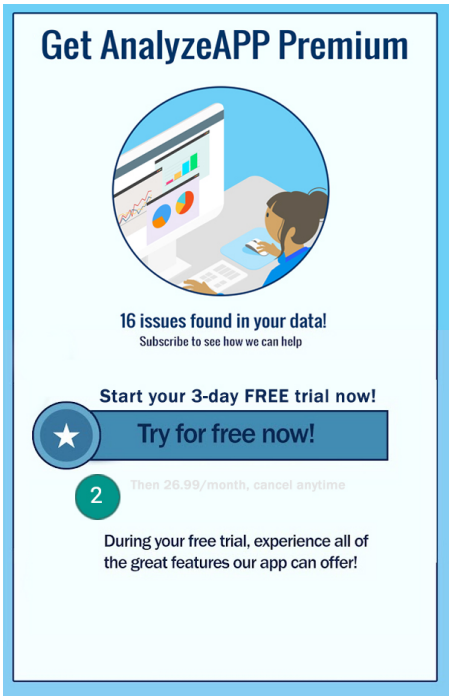
② A oferta exibe somente o custo mensal, e talvez os usuários não entendam que serão cobrados por seis meses ao fazer a assinatura.

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 precisa estar no mesmo idioma dos Termos e Condições para que os usuários a entendam completamente.

Exemplo 2:





① Cliques recorrentes na mesma área de botão fazem com que o usuário clique acidentalmente no botão final de "continuar" para se inscrever.

② O valor que será cobrado dos usuários ao final do período de teste é difícil de ler, de modo que os usuários podem pensar que o plano é gratuito.

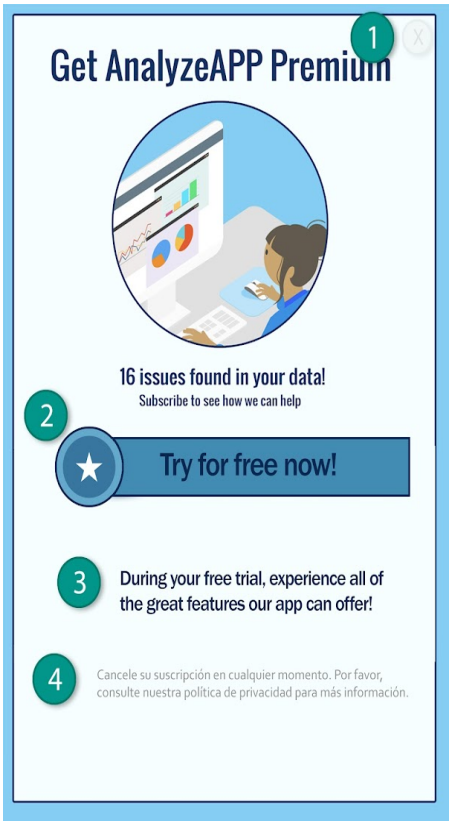
Testes gratuitos e ofertas iniciais

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 o teste gratuito 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 do teste gratuito nem do preço inicial

- Ofertas que não explicam claramente que o usuário será automaticamente inscrito em uma assinatura paga ao final do período de teste
- Ofertas que não demonstram claramente que o usuário pode acessar conteúdo sem um teste (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 no teste gratuito.

② A oferta enfatiza o teste gratuito, e talvez os usuários não entendam que serão cobrados automaticamente no final desse período.

③ A oferta não informa o período de teste, e talvez os usuários não compreendam por quanto tempo terão acesso gratuito ao conteúdo da assinatura.

④ A oferta 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.

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 obedecer às Políticas do programa para desenvolvedores do Google Play.
- Crie um método para classificar seus criativos de anúncios de acordo com os grupos adequados à idade. Os grupos adequados à idade precisam incluir pelo menos grupos para "Todos" e "Adultos". 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 exige que os SDKs de anúncios desativem anúncios personalizados, publicidade com base em interesses e remarketing como parte do tratamento para direcionamento a crianças.
- Permita que os editores selecionem formatos de anúncio que estejam em conformidade com a política de anúncios e monetização para famílias do Google Play e atendam aos requisitos do Programa Aprovado por Professores.
- Quando forem usados lances em tempo real para veicular anúncios a crianças, garanta que os criativos tenham sido revisados e que os indicadores de privacidade sejam propagados aos bidders.
- Forneça ao Google informações suficientes, como as indicadas no formulário de interesse abaixo, para verificar a 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 as informações necessárias às plataformas de mediação 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

Não são permitidos apps que usem ou se beneficiem, direta ou indiretamente, de práticas de promoção (como anúncios) enganosas ou prejudiciais ao ecossistema do desenvolvedor ou aos usuários. As práticas de promoção são consideradas enganosas ou prejudiciais se exibirem comportamento ou conteúdo que viole as Políticas do programa para desenvolvedores.

Exemplos de violações comuns:

- Uso de anúncios enganosos em sites, apps ou outras propriedades, incluindo alertas ou notificações semelhantes àquelas do sistema
- Uso de anúncios sexualmente explícitos para direcionar os usuários à página "Detalhes do app" para download
- 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 via serviços de SMS

É sua responsabilidade garantir que todas as redes de publicidade, afiliados ou anúncios associados com seu app estejam em conformidade com essas políticas.

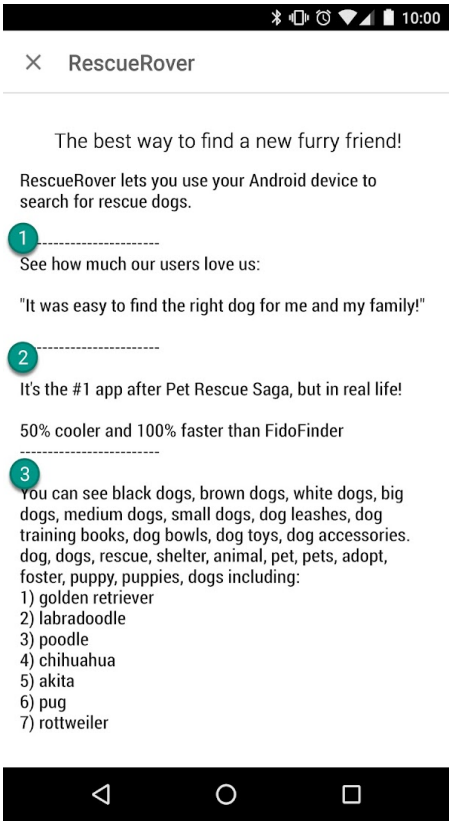
Metadados

Não permitimos apps com metadados enganosos, excessivos, irrelevantes, inadequados, com formatação incorreta ou sem valor descritivo, incluindo, mas não se limitando a, descrição do app, nome do desenvolvedor, título, ícone, capturas de tela e imagens promocionais. Os desenvolvedores precisam descrever claramente o app. Também não permitimos depoimentos de usuários não identificados ou anônimos na descrição do app.

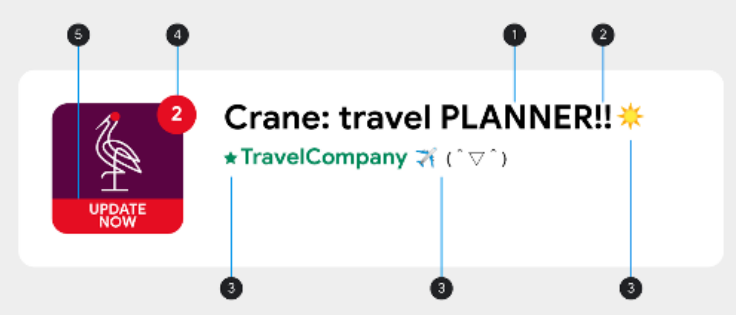
O título, o ícone do app e o nome do desenvolvedor são especialmente úteis para os usuários encontrarem e saberem mais sobre seu app. Não use emojis, emoticons nem caracteres especiais repetidos nesses elementos de metadados. Evite usar TODAS AS LETRAS EM CAIXA ALTA, a menos que isso faça parte da sua marca. Não é permitido o uso de símbolos enganosos nos ícones de apps. Por exemplo: um ponto que indica uma nova mensagem quando não há novas mensagens e símbolos de download/instalação quando o app não está relacionado ao download de conteúdo. O título do seu app precisa ter até 30 (trinta) caracteres.

Além dos requisitos mencionados aqui, Políticas para desenvolvedores específicas ao Google Play podem exigir que você forneça informações adicionais de metadados.

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



① TODAS AS LETRAS EM CAIXA ALTA, a menos que isso faça parte do nome da marca
② Sequências de caracteres especiais irrelevantes para o app
③ Emojis, emoticons (incluindo kaomojis) e caracteres especiais
④ Símbolo enganoso
⑤ Texto enganoso

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 fetichizados, seja real ou ilustração.
- É proibido usar linguagem obscena, vulgar ou outra linguagem imprópria para um público geral 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.

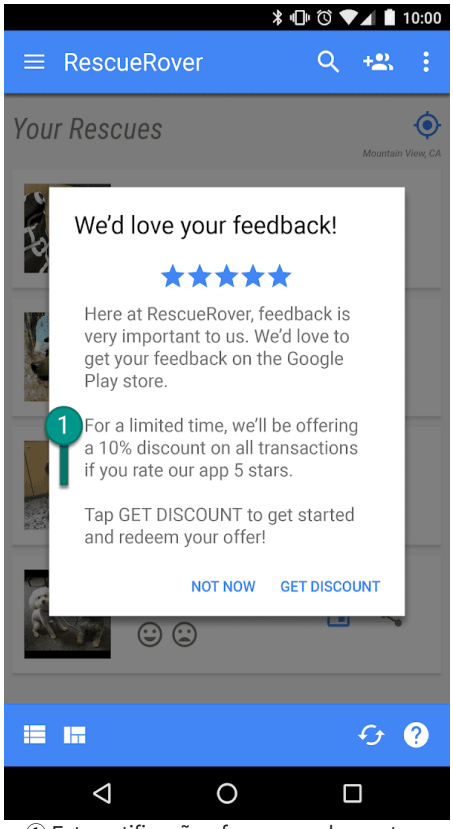
Instalações, notas e avaliações de usuários

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. Instalações, avaliações e notas por incentivo incluem usar textos ou imagens no título, ícone ou nome do desenvolvedor do app que indiquem preço ou outra informação promocional.

Os desenvolvedores não podem adicionar textos ou imagens que indicam o desempenho ou a classificação na loja, ou que sugerem relações com programas já existentes do Google Play no título, no ícone ou no nome do desenvolvedor do app.

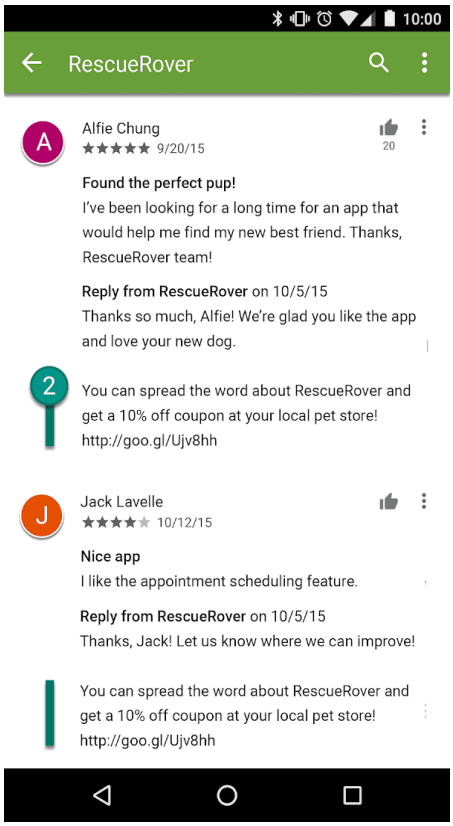
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Pedir que os usuários deem uma 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 RescueRover, oferecendo um cupom.

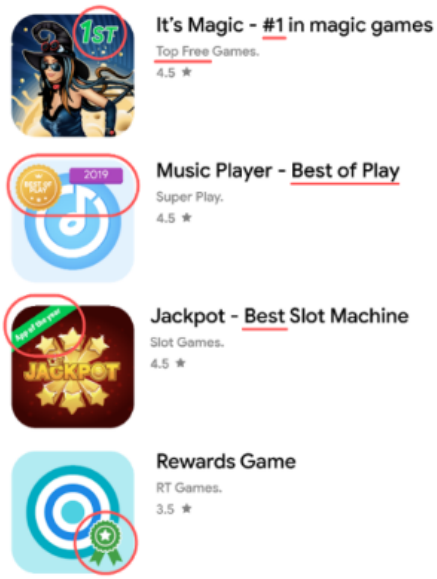
As notas e avaliações são indicadores da qualidade do app. É importante para os usuários que essas informações sejam autênticas e relevantes. Veja algumas práticas recomendadas sobre como responder às avaliações dos

usuários:

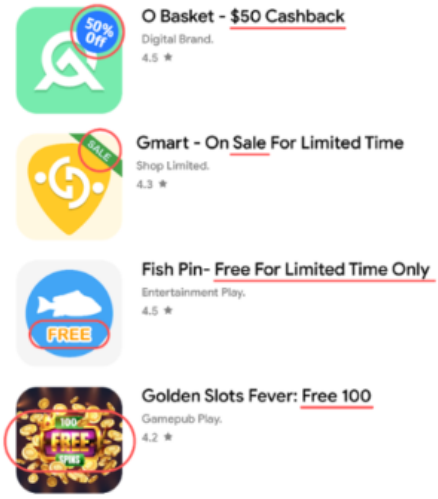
- Mantenha sua resposta focada nas questões levantadas nos comentários dos usuários e não peça uma classificação melhor.
- Inclua referências a recursos úteis, como um endereço de suporte ou uma página "Perguntas frequentes".

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.

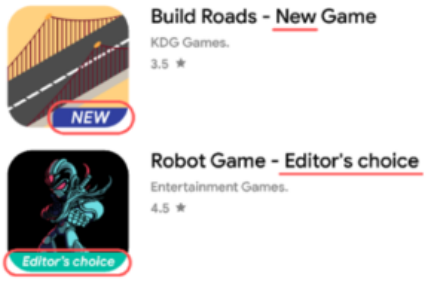
- Imagens ou textos que indicam o desempenho ou a classificação na loja, como "App do ano", "Número 1", "Melhor jogo de 20XX", "Favoritos", ícones de prêmios etc.



- Imagens ou textos que indicam informações promocionais ou de preço, como "10% de desconto", "R$ 50 de reembolso", "gratuito por período limitado" etc.



- Imagens ou textos que indicam programas do Google Play, como "Escolha dos editores", "Novo" etc.



Classificações de conteúdo

As classificações do conteúdo no Google Play são realizadas pela Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês) e foram criadas para ajudar os desenvolvedores a mostrar como os apps foram categorizados de acordo com a região dos usuários. As autoridades regionais da IARC mantêm as diretrizes usadas para determinar o nível de maturidade do conteúdo em um app. Não permitimos apps sem classificação do conteúdo no Google Play.

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.

Notícias

Os apps que se declaram como de notícias no Play Console ("Apps de notícias") precisam atender a todos os requisitos a seguir.

Os Apps de notícias que exigem a compra de uma assinatura precisam oferecer uma prévia do conteúdo no app para os usuários antes da aquisição.

Os Apps de notícias PRECISAM:

- fornecer informações sobre os responsáveis da empresa de notícias e dos colaboradores, incluindo, mas não se limitando a, o site oficial das notícias publicadas no app, dados de contato válidos e verificáveis e o editor original de cada artigo; e
- ter uma página no app ou um site específico que indique claramente que inclui dados de contato, seja fácil de encontrar (por exemplo, um link na parte inferior da página inicial ou na barra de navegação do site) e forneça dados de contato válidos da empresa de notícias, incluindo pelo menos um endereço de e-mail e um número de telefone.

Exibir links para contas de mídia social não é suficiente para atender ao requisito de dados de contato da empresa. Além disso, os apps que têm principalmente conteúdo gerado pelo usuário (por exemplo, apps de mídia social) não podem se declarar como de notícias.

Os Apps de notícias NÃO PODEM:

- ter erros ortográficos e/ou gramaticais significativos;
- ter somente conteúdo estático (por exemplo, de vários meses atrás); e
- ter marketing de afiliados ou receita de publicidade como principal finalidade.

Os apps de notícias *podem* usar anúncios e outras formas de marketing para gerar receita, desde que a finalidade principal do app não seja vender produtos e serviços nem gerar receita de publicidade.

Os apps de notícias que agregam conteúdo de diversas fontes de publicação precisam ser transparentes sobre a fonte do conteúdo no app. Além disso, cada uma dessas fontes precisa atender aos requisitos da política de notícias.

Consulte este artigo para saber as melhores maneiras de fornecer as informações exigidas.

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.

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.

- Quando o usuário pressiona o botão "Compartilhar", o app envia mensagens em nome dele sem que ele possa confirmar o conteúdo e os destinatários:

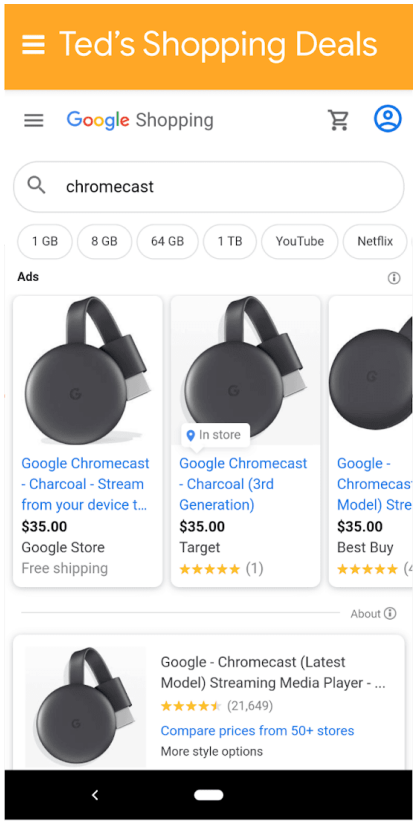
Spam de afiliados e visualizações da Web

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:



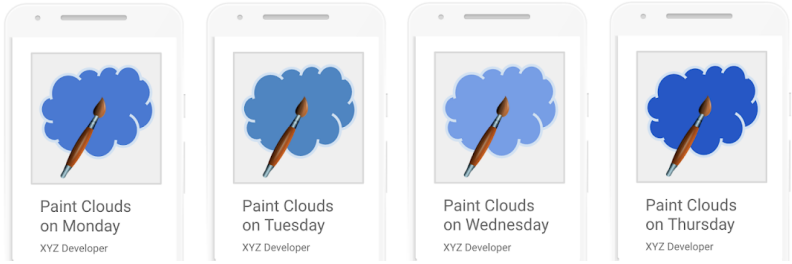
① Este app se chama "Ofertas do Ted", mas ele só fornece um WebView do Google Shopping.

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.



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

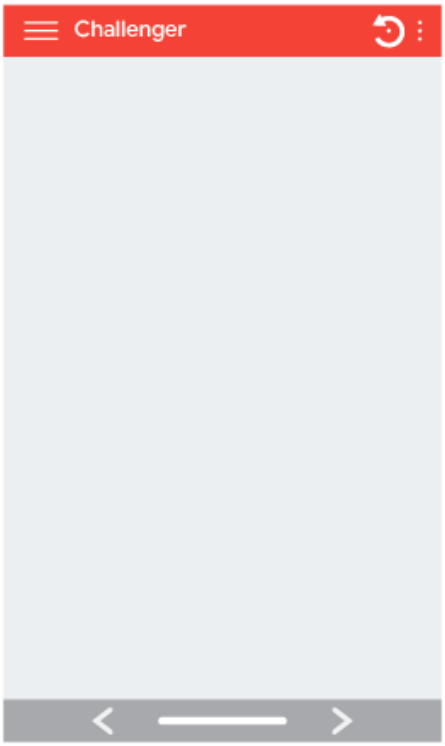
---

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



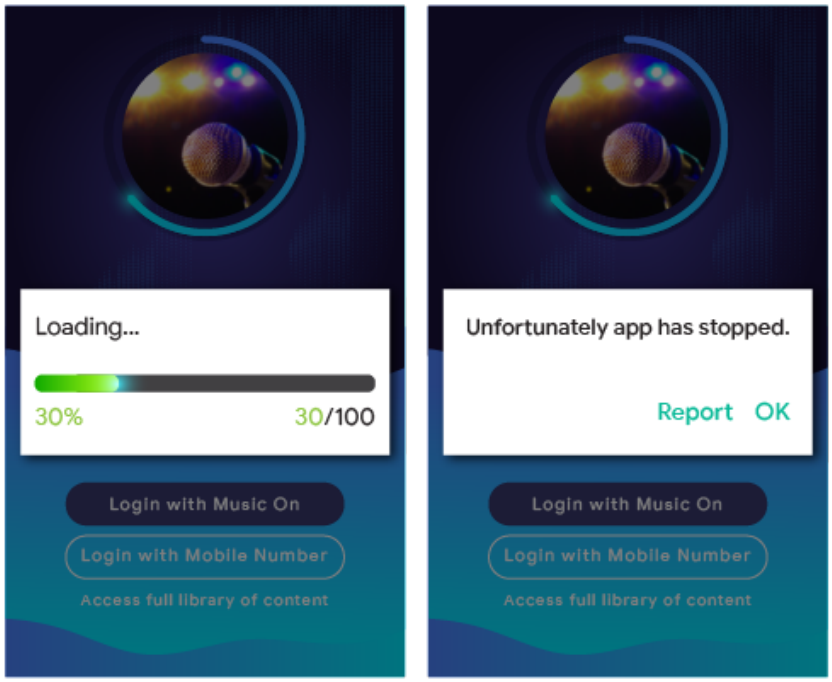
Recursos com problemas

Não permitimos apps com falhas, fechamentos forçados, travamentos ou que funcionem de maneira anormal.

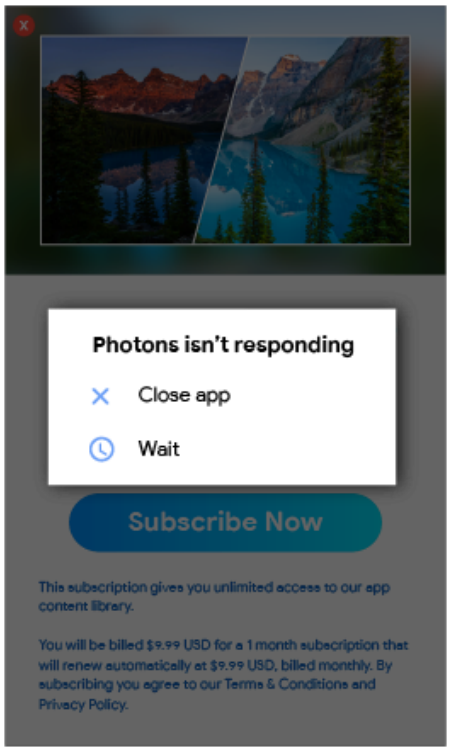
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- 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.

Política de emoji do Android

Em vigor a partir de 2 de fevereiro de 2022

Nossa política de emojis foi desenvolvida para promover uma experiência do usuário consistente e inclusiva em toda a plataforma do Google.

Os apps executados no Android 12 ou versões mais recentes precisam estar em conformidade com a versão mais recente do Unicode em até quatro meses da publicação.

Para manter a conformidade, os desenvolvedores precisam seguir uma das opções:

- Se AppCompat já estiver em uso, confira se o emoji está ativado.
- Use uma biblioteca EmojiCompat em todas as plataformas no app. Isso funcionará com visualizações personalizadas que usam diretamente StaticLayout .
- Atualize o gerenciamento e a fonte/as imagens dos emoji com base na versão mais recente do Unicode.

Use os exemplos de emoji abaixo para testar se o app é compatível com a versão mais recente do Unicode:

Exemplos	Versão do Unicode
🫠 🫆 🫂	13.1
🥲 🫥 🐻‍❄️	13.0
🧑‍🦰 🧑‍🦯 👫	12.1
🦩 🫅🏿 👭	12.0

Consulte este recurso para ver orientações sobre a compatibilidade com emojis adicionais.

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 por conteúdo seguro e de alta qualidade para compartilhar com os filhos. Você pode desenvolver apps específicos para crianças ou seu app pode só 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 app 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. Caso seu app seja direcionado a crianças e usuários mais velhos, você ainda poderá participar do programa Feito para Familia. Todos os apps participantes do programa Feito para Família estarão qualificados para classificação no Programa Aprovado por Professores, mas não podemos garantir que seu app será incluído nesse programa. Se você decidir não participar do programa Feito para Família, 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 se destina a 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 para 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 fortemente que você informe aos usuários existentes do seu app sobre alterações no público-alvo ou se passar a permitir anúncios ou compras no aplicativo. Para fazer isso, use a seção "Novidades" 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

A partir de 1.º de abril de 2022

Se crianças forem 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 para crianças precisa ser apropriado para esse público-alvo.
2. **Funcionalidade do app**: seu app não pode apenas fornecer uma visualização da Web de um site nem ter o objetivo principal de direcionar tráfego para um, mesmo que você tenha a propriedade do site.
   - Sempre buscamos maneiras de disponibilizar novas experiências aos desenvolvedores de apps para crianças. Caso queira participar do nosso piloto do App Confiável da Web para apps educacionais, conte para a gente .
3. **Respostas no Play Console**: você precisa responder com precisão às perguntas sobre seu app no Play Console e atualizar as respostas para que reflitam corretamente qualquer mudança aplicada a ele. Isso inclui, mas não se limita a, divulgação precisa dos elementos interativos do app no questionário de classificação de conteúdo, como os seguintes:
   - Os usuários do seu app podem interagir ou trocar informações.
   - O app compartilha informações fornecidas pelo usuário com terceiros.
   - O app compartilha a localização física do usuário com outras pessoas.
4. **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 publicidade para esses usuários;
   - garantir que os anúncios exibidos para esses usuários não envolvam publicidade com base em interesses (direcionada a usuários individuais com determinadas características e baseada no comportamento de navegação on-line) nem remarketing (publicidade direcionada a usuários individuais e baseada em interação anterior com um app ou site);
   - 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.
5. **Práticas relacionadas a dados**: você precisa divulgar a coleta de todas as informações pessoais e sensíveis de crianças, inclusive por APIs e SDKs chamados ou usados no seu app. As informações sensíveis de crianças

incluem, mas não se limitam a, informações de autenticação, dados do sensor da câmera e do microfone, dados do dispositivo, ID do Android e dados de uso de publicidade. Também é preciso que o app siga estas práticas relacionadas a dados:

- Não é permitido transmitir o identificador de publicidade do Android (AAID, na sigla em inglês), o número de série do chip, o número de série da versão, o BSSID, o MAC, o SSID, o IMEI e/ou o IMSI de crianças ou usuários com idade desconhecida.
- O número de telefone do dispositivo não pode ser solicitado ao TelephonyManager da API do Android.
- Os apps que segmentam somente crianças não podem pedir, coletar, usar nem transmitir a localização.
- Os apps precisam usar o Gerenciador de dispositivos complementar (CDM, na sigla em inglês) ao pedir para usar o Bluetooth, a menos que o app segmente apenas versões de sistema operacional (SO) não compatíveis com CDM.

6. **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 principalmente 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 públicos-alvo mais velhos 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 de crianças. Os apps direcionados a crianças e públicos mais velhos não podem exigir que os usuários façam login ou acessem o conteúdo do app usando APIs ou SDKs que não sejam aprovados para uso em serviços feitos para crianças.
7. **Realidade aumentada (RA)**: se o app usar realidade aumentada, será necessário 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 da família
   - 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. **Recursos e aplicativos sociais**: se o app permitir que os usuários compartilhem ou troquem informações, será necessário divulgar esses recursos com precisão no questionário de classificação do conteúdo no Play Console.
   - Aplicativos sociais: têm como foco principal permitir que os usuários compartilhem conteúdo em formato livre ou se comuniquem com grandes grupos de pessoas. Todos os aplicativos sociais que incluem crianças no público-alvo precisam exibir um lembrete no próprio app sobre segurança on-line e sobre os riscos reais das interações na Internet antes de permitir que usuários dessa faixa etária troquem mídia ou informações em formato livre. Além disso, é preciso exigir o consentimento de um adulto antes de permitir que crianças troquem informações pessoais.
   - Recursos sociais: incluem qualquer funcionalidade adicional do app que permita aos usuários compartilhar conteúdo em formato livre ou se comunicar com grandes grupos de pessoas. Todos os apps que incluem crianças no público-alvo e têm recursos sociais precisam exibir um lembrete no próprio aplicativo sobre segurança on-line e sobre os riscos reais das interações na Internet antes de permitir que usuários dessa faixa etária troquem mídia ou informações em formato livre. Além disso, é preciso oferecer um método para que os adultos gerenciem os recursos sociais de crianças, incluindo ativar/desativar esses recursos ou selecionar diferentes níveis de funcionalidade, entre outros. Também é necessário exigir o consentimento de um adulto antes de ativar recursos que permitem que crianças troquem informações pessoais.
   - O "consentimento de um adulto" é um mecanismo para verificar a idade do usuário sem incentivar as crianças a falsificar essa informação para ter acesso a áreas do app projetadas para adultos. Por exemplo: PIN do adulto, senha, data de nascimento, verificação de e-mail, ID por foto, cartão de crédito ou documento oficial.
   - Aplicativos sociais em que o foco principal é conversar com pessoas desconhecidas não podem ter crianças como público-alvo. Por exemplo: apps do tipo "chat roulette", apps de encontros, salas de chat abertas com foco em crianças etc.
9. **Conformidade legal**: você precisa garantir que o app, incluindo APIs ou SDKs chamados ou usados por ele, obedeça à Lei de Proteção da Privacidade On-line das Crianças (COPPA) dos EUA, ao Regulamento geral de proteção de dados (GDPR) da UE e a 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 têm conteúdo que só é apropriado para adultos
- Apps que implementam APIs com Termos de Serviço que proíbem o uso em apps feitos para crianças
- Apps que exaltam o uso de bebidas alcoólicas, tabaco ou substâncias controladas
- Apps que incluem jogos de azar simulados ou 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 contêm links para sites com conteúdo que viola as Políticas do programa para desenvolvedores do Google Play
- Apps que exibem anúncios destinados a adultos, por exemplo, conteúdo violento, sexual ou de jogos de azar, para crianças (saiba mais sobre as diretrizes do Google Play sobre publicidade, compras no aplicativo e conteúdo comercial para crianças nas políticas de anúncios e monetização para famílias)

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. Esses apps precisam ter a classificação de software de entretenimento (ESRB, na sigla em inglês) "Todos", "Não recomendado para menores de 10 anos" ou equivalente e só podem usar SDKs de anúncios certificados do Google Play . Os apps aceitos no programa Feito para Família precisam estar em conformidade com todos os requisitos do programa. O Google Play pode recusar, remover ou suspender qualquer app considerado inadequado para o programa Feito para Família.

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 contribuição 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, cuidador, príncipe/princesa, bombeiro, policial ou um personagem fictício.

Anúncios e monetização

Se você gera receita com um app destinado a crianças no Google Play, é importante que ele siga os seguintes requisitos da política de anúncios e monetização para famílias.

As políticas abaixo se aplicam a todo tipo de monetização e publicidade, incluindo anúncios, promoções cruzadas (para seus aplicativos e os de terceiros), ofertas de compras no app ou qualquer outro conteúdo comercial (como inserção paga de produto). Toda monetização e publicidade nesses apps precisa obedecer às legislações e regulamentações aplicáveis, inclusive a todas as diretrizes do setor ou de autorregulamentação relevantes.

O Google Play reserva-se o direito de recusar, remover ou suspender apps devido a táticas comerciais excessivamente agressivas.

Requisitos de formato

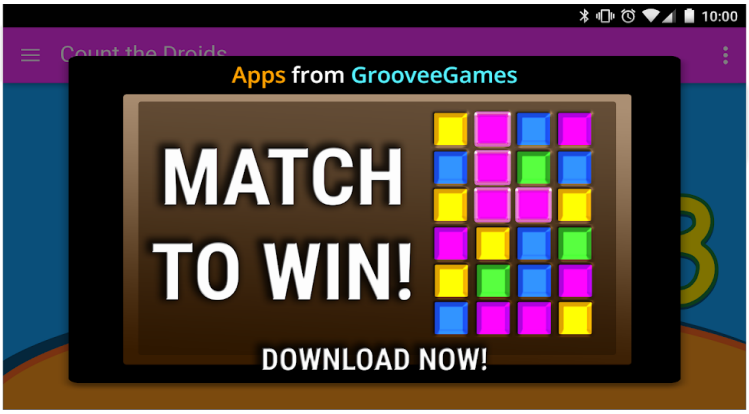
A monetização e a publicidade no app não devem ter conteúdo enganoso nem ser projetadas de maneira que leve a cliques acidentais de crianças. As seguintes ações são proibidas:

- Anúncios e monetização invasivos, como aqueles que ocupam a tela inteira ou interferem no uso normal e não fornecem um meio claro de dispensar o anúncio (por exemplo, paredes de anúncios)
- Monetização e publicidade que interferem no uso normal de apps ou jogos e não podem ser fechadas após cinco segundos
- Monetização e publicidade que não interferem no uso normal do app ou jogo podem persistir por mais de cinco segundos (por exemplo, conteúdo de vídeo com anúncios integrados)
- Publicidade e monetização intersticiais exibidas imediatamente após a inicialização do app
- Vários posicionamentos de anúncio em uma página, por exemplo: mostrar mais de um banner ou anúncio em vídeo ou usar anúncios de banner que exibem diversas ofertas em um canal
- Monetização e publicidade que não podem ser facilmente diferenciadas do conteúdo do app
- Uso de táticas chocantes ou que envolvem a manipulação emocional para incentivar a visualização de anúncios ou as compras no app
- Falta de distinção entre o uso de moedas virtuais no jogo e dinheiro real para fazer compras no app

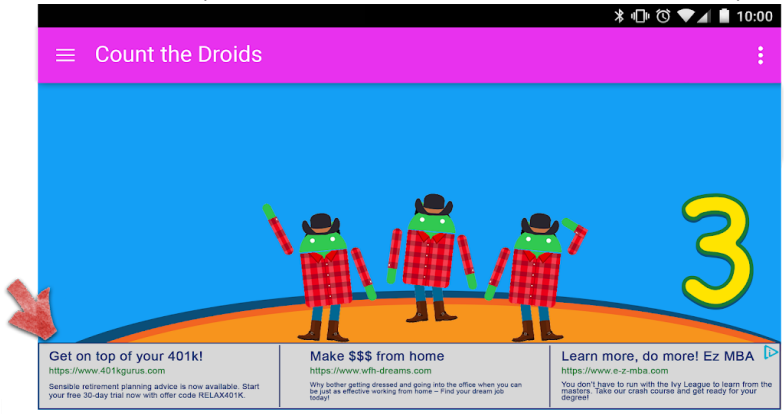
Para que o Google Play continue a ser uma plataforma que promove a segurança e o respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

- Monetização e publicidade que se afastam do dedo do usuário quando ele tenta fechar
- Monetização e publicidade que não fornecem ao usuário uma maneira de fechar a oferta após 5 (cinco) segundos, conforme descrito no exemplo abaixo:

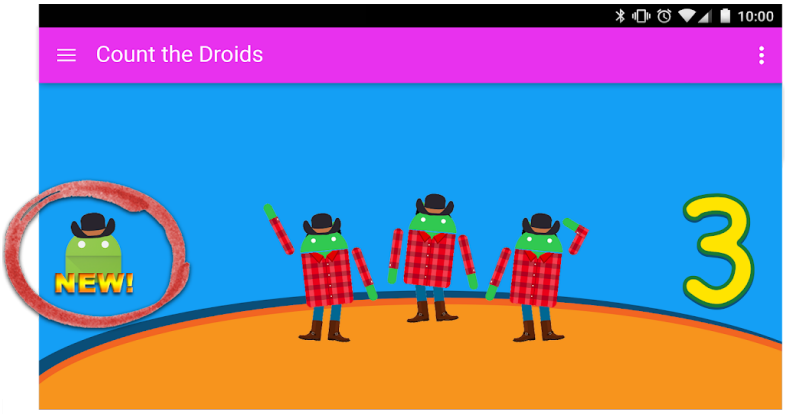
- Monetização e publicidade que ocupam a maior parte da tela do dispositivo sem fornecer ao usuário uma maneira clara de dispensá-lo, conforme descrito no exemplo abaixo:



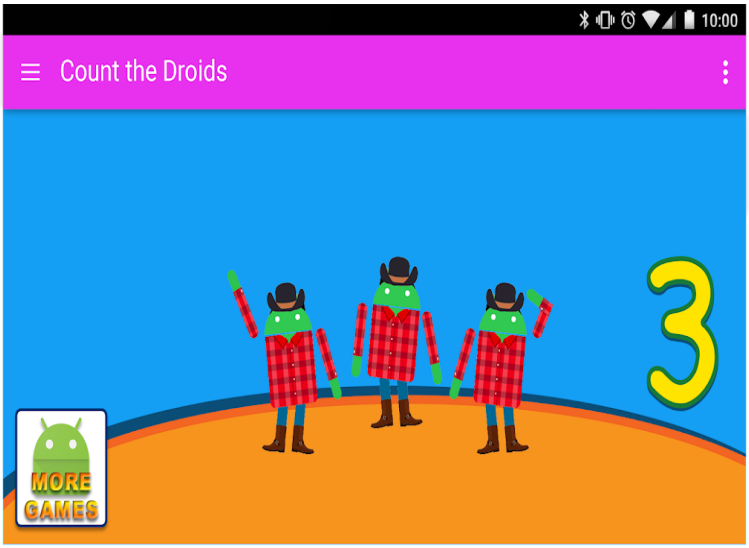
- Anúncios de banner que mostram várias ofertas, conforme mostrado no exemplo abaixo:



- Monetização e publicidade que podem ser confundidas com o conteúdo do app, conforme mostrado no exemplo abaixo:



- Botões, anúncios ou outra monetização 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 podem 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 com conteúdo violento e imagens inadequadas para crianças.

SDKs de anúncios

Se você veicula anúncios no app e o público-alvo dele inclui somente crianças, é necessário usar os SDKs de anúncios certificados do Google Play. Se o público-alvo do app inclui crianças e usuários mais velhos, implemente medidas de triagem de idade, como uma tela neutra de informações de idade. Além disso, garanta que os anúncios exibidos para crianças tenham origem exclusivamente de SDKs de anúncios certificados Google Play. Os apps do Programa Feito para Família precisam usar somente SDKs de anúncios com autocertificação.

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 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 a DDA, o conteúdo do app precisa ser classificado de acordo com nossas Diretrizes de classificação do conteúdo.

Não permitimos apps ou conteúdo que prejudicam a confiança do usuário no ecossistema do Google Play. Ao avaliar a inclusão ou remoção de apps do Google Play, consideramos diversos fatores, incluindo, mas não se limitando a um padrão de comportamento prejudicial ou alto risco de abuso. Identificamos o risco de abuso usando vários itens, como reclamações específicas sobre apps e desenvolvedores, relatórios de notícias, histórico de violações, feedback de usuários e o uso de marcas, personagens e outros recursos conhecidos.

Como funciona o Google Play Protect

O Google Play Protect verifica os apps quando você os instala. Ele também faz verificações periódicas no dispositivo. Se encontrar um app potencialmente nocivo, ele poderá realizar as seguintes ações:

- Enviar uma notificação para você. Para remover o app, toque na notificação e depois em "Desinstalar".
- Desativar o app até que ele seja desinstalado.
- Remover o app automaticamente. Na maioria dos casos, se um app nocivo for detectado, você receberá uma notificação informando que ele foi removido.

Como funciona a proteção contra malware

Para proteger você contra softwares e URLs maliciosos de terceiros, além de outros problemas de segurança, o Google pode receber informações sobre:

- conexões de rede do seu dispositivo;
- URLs potencialmente nocivos;
- sistema operacional e apps instalados no dispositivo por meio do Google Play ou de outras fontes.

Você pode receber um alerta do Google sobre um app ou URL potencialmente perigoso. O app ou URL poderá ser removido ou ter a instalação bloqueada pelo Google se for reconhecido como prejudicial para dispositivos, dados ou usuários.

É possível desativar certas proteções nas configurações do dispositivo. No entanto, talvez o Google continue recebendo informações sobre os apps instalados por meio do Google Play. Além disso, os apps instalados no seu dispositivo de outras fontes poderão ser verificados em busca de problemas de segurança sem o envio de informações ao Google.

Como funcionam os alertas de privacidade

O Google Play Protect enviará um alerta caso um app seja removido da Google Play Store por permitir o acesso às suas informações pessoais para que você possa desinstalá-lo.

Processo de restrição

Se o app violar uma de nossas políticas, as medidas cabíveis serão tomadas, conforme descrito a seguir. Além disso, forneceremos informações relevantes sobre a medida a ser tomada por e-mail, junto com instruções sobre como contestar caso você acredite que nossa ação tenha sido um engano.

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 relativo às políticas e por garantir, com a devida diligência, que o restante do app também esteja em total conformidade com as políticas. Não resolver violações da política em todos os seus apps pode resultar em ações adicionais de restrição.

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 de desenvolvedor do Google Play individuais ou relacionadas.

Ações de restrição

Cada ação de restrição pode afetar o app de uma maneira diferente. Na seção a seguir, há uma descrição de várias ações que a plataforma pode realizar e o impacto delas em um app ou na conta de desenvolvedor do Google Play. Essas informações também são explicadas neste vídeo.

Rejeição

- Um app novo ou uma atualização enviados para revisão não serão disponibilizados no Google Play.
- Se uma atualização de um app for rejeitada, a última versão publicada permanecerá disponível no Google Play.
- Isso não afeta o acesso às instalações do usuário, às estatísticas e às notas do app rejeitado.
- Também não afeta a situação da conta de desenvolvedor do Google Play.

Observação: não tente reenviar um app rejeitado até corrigir todas as violações da política.

Remoção

- O app e as versões anteriores dele serão removidos do Google Play e não estarão mais disponíveis para download.
- Como o app é removido, os usuários não poderão ver a página "Detalhes do app", as instalações do usuário, as estatísticas e as notas do app. Essas informações serão restauradas depois que você enviar uma atualização do app removido em conformidade com a política.
- Talvez os usuários não consigam fazer compras no aplicativo nem utilizar recursos de faturamento em apps até que uma versão em conformidade com a política seja aprovada pelo Google Play.
- As remoções não afetam imediatamente a situação da sua conta de desenvolvedor do Google Play, mas várias remoções podem resultar em suspensão.

Observação: não tente publicar novamente um app removido até corrigir todas as violações da política.

Suspensão

- O app e as versões anteriores dele serão removidos do Google Play e não estarão mais disponíveis para download.
- A suspensão pode ocorrer como resultado de violações graves ou repetidas das políticas, bem como por várias rejeições ou remoções do app.
- Como o app está suspenso, os usuários não poderão ver a página "Detalhes do app", as instalações do usuário, as estatísticas e as notas. Essas informações serão restauradas depois que você enviar uma atualização em conformidade com a política.
- Não é mais possível usar o APK ou pacote de apps do app suspenso.
- Os usuários não poderão fazer compras no aplicativo nem usar recursos de faturamento em apps até que uma versão em conformidade com a política seja aprovada pelo Google Play.
- As suspensões contam como avisos que afetam a situação regular da conta de desenvolvedor do Google Play.Se houver vários avisos, isso poderá resultar no encerramento de contas de desenvolvedor do Google Play individuais e relacionadas.

Observação: não tente publicar novamente um app suspenso, a menos que o Google Play tenha informado que você pode fazer isso.

Visibilidade limitada

- A detecção do app no Google Play é restrita. O app permanecerá disponível no Google Play e poderá ser acessado por usuários com um link direto para a página "Detalhes do app" na Play Store.
- Colocar o app em um estado de visibilidade limitada não afeta a situação da sua conta de desenvolvedor do Google Play.
- Esse estado também não afeta a capacidade dos usuários de ver a página "Detalhes do app", as instalações do usuário, as estatísticas e as notas.

Regiões limitadas

Início da vigência: 1.º de dezembro de 2021

- O download do app no Google Play só está disponível em certas regiões.
- Os usuários de outras regiões não encontrarão o app na Play Store.
- As pessoas que instalaram o app anteriormente poderão continuar a usá-lo nos dispositivos, mas não receberão mais atualizações.
- A limitação de região não afeta a situação da sua conta de desenvolvedor do Google Play.

Encerramento da conta

- Quando a conta de desenvolvedor é encerrada, todos os apps no catálogo dela são removidos do Google Play, e não é possível publicar novos apps. Isso também significa que todas as contas de desenvolvedor do Google Play relacionadas também serão suspensas permanentemente.
- Várias suspensões ou suspensões por graves violações da política também podem resultar no encerramento da conta do Play Console.
- Como os apps na conta encerrada são removidos, os usuários não poderão ver a página "Detalhes do app", as instalações do usuário, as estatísticas e as notas.

Observação: todas as novas contas que você tentar abrir também serão encerradas (sem reembolso da taxa de registro do desenvolvedor). Portanto, não tente se inscrever em uma nova conta do Play Console quando uma das suas outras contas for encerrada.

Contas inativas

Contas inativas são contas de desenvolvedor que não estão ativas ou foram abandonadas. Essas contas não estão em situação regular conforme exigido pelo Contrato de distribuição do desenvolvedor .

As contas de desenvolvedor do Google Play são destinadas a desenvolvedores ativos que publicam e mantêm apps ativamente. Para evitar abusos, fechamos as contas inativas que não são usadas ou não apresentam atividade significativa (por exemplo, de publicação e atualização de apps, acesso a estatísticas ou gerenciamento de páginas "Detalhes do app", entre outras) regularmente.

O encerramento de contas inativas excluirá sua conta e todos os dados associados a ela. A taxa de registro não é reembolsável e será perdida. Antes de encerrarmos sua conta inativa, notificaremos você usando as informações de contato fornecidas para essa conta.

O encerramento de uma conta inativa não impede você de criar uma nova conta no futuro, caso decida publicar no Google Play. Você não poderá reativar a conta, e os apps ou dados anteriores não estarão disponíveis em uma nova conta.

Gerenciamento e denúncia de violações da política

Contestar uma ação de restrição

Em caso de erro e se o app não violar as políticas do programa do Google Play e o Contrato de distribuição do desenvolvedor, todos os apps serão restabelecidos. Se você tiver analisado as políticas com atenção e acreditar que a ação pode ter sido um engano, siga as instruções fornecidas na notificação por e-mail de restrição para contestar nossa decisão.

Recursos adicionais

Se você precisar de mais informações sobre uma ação de restrição ou uma nota/comentário de um usuário, consulte alguns dos recursos abaixo ou entre em contato por meio da Central de Ajuda do Google Play. No entanto, não podemos oferecer orientação jurídica ao desenvolvedor. Se você precisar de orientação jurídica, consulte um advogado.

- Verificação de apps
- 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

---

Requisitos do Play Console

O Google Play quer fornecer experiências de apps seguras e incríveis para nossos usuários e uma grande oportunidade de sucesso para todos os desenvolvedores. Nossa missão é facilitar o processo de disponibilização do seu app para os usuários.

Siga as orientações abaixo ao enviar informações no Play Console para evitar violações comuns que podem retardar o processo de revisão ou gerar uma recusa.

Antes de enviar seu app, faça o seguinte:

- Forneça com precisão todas as informações e metadados do app.
- Verifique se os dados de contato estão atualizados.
- Faça upload da Política de Privacidade do seu app e preencha os requisitos da seção **Segurança dos dados**.
- Forneça uma conta de demonstração ativa, além de informações de login e todos os outros recursos necessários para revisar o app, como credenciais de login, código QR etc.

Como sempre, garanta que o app ofereça uma experiência de usuário estável, envolvente e responsiva e verifique se todos os elementos dele, incluindo redes de publicidade, serviços de análise e SDKs de terceiros, estão em conformidade com as Políticas do programa para desenvolvedores do Google Play . Caso o público-alvo do app inclua crianças, também é preciso estar em conformidade com a Política para famílias .

É sua responsabilidade ler o Contrato de distribuição do desenvolvedor e todas as Políticas do programa para desenvolvedores para garantir que o app esteja em total conformidade.

Developer Distribution Agreement

Precisa de mais ajuda?

Siga as próximas etapas:

Fale conosco

Conte mais sobre o problema para podermos ajudar você