Política do Programa para programadores

(em vigor a partir de 5 de março de 2025, salvo indicação em contrário)

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

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

Conteúdo restrito

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

Negligência infantil

As apps que não proíbem os utilizadores de criar, carregar ou distribuir conteúdos que facilitem a exploração ou o abuso de crianças estão sujeitas a remoção imediata do Google Play. Tal abrange todos os materiais relativos a abuso sexual infantil. Para denunciar conteúdos num produto Google que possam explorar uma criança, clique em **Denunciar abuso** . Se encontrar conteúdos noutro local da Internet, contacte diretamente as autoridades competentes do seu país .

Proibimos o uso de apps que coloquem crianças em perigo. Isto inclui, entre outros, o uso de apps para promover comportamentos predatórios em relação a crianças, como:

- Interação imprópria segmentada para uma criança (por exemplo, apalpar ou acariciar).
- Aliciamento e sedução de menores (por exemplo, tornar-se amigo de uma criança online para facilitar o contacto sexual, tanto online como offline, e/ou trocar imagens de cariz sexual com essa criança).
- Sexualização de um menor (por exemplo, imagens que retratem, incentivem ou promovam o abuso sexual de crianças ou a representação de crianças de uma forma que possa resultar na exploração sexual de crianças).
- Extorsão sexual (por exemplo, ameaçar ou chantagear uma criança através de um acesso real ou alegado a imagens de cariz íntimo da criança).
- Tráfico de crianças (por exemplo, publicidade ou aliciamento de uma criança para exploração sexual comercial).

Tomaremos as medidas necessárias que podem incluir o envio de uma denúncia para o Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC, National Center for Missing & Exploited Children), se tomarmos conhecimento da existência de conteúdos com materiais relativos a abuso sexual infantil. Se suspeitar que uma criança se encontra em risco ou foi sujeita a abuso, exploração ou tráfico, contacte as autoridades locais e uma organização de segurança infantil listada aqui .

Além disso, não são permitidas apps que sejam atrativas para crianças, mas que contenham temas para adultos, incluindo, entre outras:

- Apps com violência excessiva, sangue e violência gráfica.
- Apps que representem ou incentivem atividades prejudiciais e perigosas.

Da mesma forma, não permitimos apps que promovam uma imagem corporal ou auto-imagem negativa, incluindo apps que retratem, para efeitos de entretenimento, cirurgia plástica, perda de peso

e outros ajustes estéticos ao aspeto físico de uma pessoa.

Política de Normas de Segurança Infantil

O Google Play exige que as apps sociais e de encontros estejam em conformidade com a política de Normas de Segurança para Crianças.

Estas apps têm de:

- **Ter Normas Publicadas:** a sua app tem de proibir explicitamente o abuso e exploração sexual infantil (AESI) em normas acessíveis publicamente, como os Termos de Utilização da sua app, as regras da comunidade ou qualquer outra documentação da Política do Utilizador disponível publicamente.
- **Oferecer um mecanismo na app para feedback dos utilizadores:** tem de se autocertificar de que oferece um mecanismo na app para os utilizadores enviarem feedback, preocupações ou denúncias.
- **Resolver CSAM:** tem de se autocertificar de que a sua app toma as medidas adequadas, incluindo, entre outras, a remoção de CSAM, depois de obter conhecimento efetivo da existência deste tipo de material, de acordo com as suas normas publicadas e as leis relevantes.
- **Estar em conformidade com as leis de segurança infantil:** tem de se autocertificar de que a sua app está em conformidade com as leis e regulamentos de segurança infantil aplicáveis, incluindo, entre outros, a existência de um processo para denunciar CSAM confirmado ao National Center for Missing and Exploited Children ou à sua autoridade regional relevante.
- **Disponibilizar um ponto de contacto de segurança infantil:** a sua app tem de disponibilizar um ponto de contacto designado para receber potenciais notificações do Google Play sobre conteúdo de AESI encontrado na sua app ou plataforma. Este representante deve estar preparado para falar sobre os seus procedimentos de aplicação e revisão, e para tomar medidas, se necessário.

Saiba mais aqui sobre estes requisitos e como estar em conformidade no nosso artigo do Centro de Ajuda.

Conteúdo impróprio

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

Conteúdos de natureza sexual e linguagem obscena

Não permitimos apps que incluam ou promovam conteúdos de natureza sexual ou linguagem obscena, incluindo pornografia ou quaisquer conteúdos ou serviços que pretendam ser sexualmente gratificantes. Não permitimos apps ou conteúdos de apps que aparentem promover ou solicitar um ato sexual em troca de compensação. Não permitimos apps que incluam ou promovam conteúdos associados a comportamento sexualmente predatório ou distribuam conteúdos de natureza sexual não consensuais. Pode ser permitido conteúdo com nudez se o objetivo principal for educativo, documental, científico ou artístico e não for despropositado.

As apps de catálogo (apps que apresentam títulos de livros/vídeos como parte de um catálogo de conteúdos mais vasto) podem distribuir títulos de livros (incluindo livros eletrónicos e audiolivros) ou vídeos com conteúdos de natureza sexual, desde que sejam cumpridos os seguintes requisitos:

- Os títulos de livros/vídeos com conteúdos de natureza sexual representam uma pequena fração do catálogo geral da app
- A app não promove ativamente títulos de livros/vídeos com conteúdos de natureza sexual. No entanto, estes títulos podem ser apresentados em recomendações baseadas no histórico do utilizador ou durante promoções gerais de preços
- A app não distribui títulos de livros/vídeos com conteúdos de negligência infantil, pornografia ou quaisquer outros conteúdos de natureza sexual definidos como ilegais pela lei aplicável

- A app protege os menores, restringindo o acesso a títulos de livros/vídeos com conteúdos de natureza sexual

Se uma app incluir conteúdos que violem esta política, mas que sejam considerados apropriados numa determinada região, a app pode estar disponível para os utilizadores nessa região, mas permanecerá indisponível para os utilizadores noutras regiões.

Seguem-se alguns exemplos de violações comuns:

- Representações de nudez de cariz sexual ou posições sexualmente sugestivas em que o sujeito está nu, desfocado ou minimamente vestido e/ou em que o vestuário não seja aceitável num contexto público adequado.
- Representações, animações ou ilustrações de atos sexuais, poses com conotações sexuais ou a representação sexual de partes do corpo.
- Conteúdo que represente brinquedos sexuais, guias sexuais, temas sexuais ilegais e fetiches.
- Conteúdo que seja provocador ou obsceno, incluindo, entre outros, conteúdo que possa conter linguagem obscena, insultos, texto explícito ou palavras-chave para adultos/sexuais na Ficha da loja ou app.
- Conteúdo que represente, descreva ou incentive a bestialidade.
- Apps que promovam entretenimento associado a sexo, serviços de acompanhantes ou outros serviços que possam ser interpretados como disponibilização ou solicitação de atos sexuais em troca de compensação, incluindo, entre outros, encontros em troca de compensação ou acordos de cariz sexual onde seja esperado que um dos participantes forneça dinheiro, presentes ou apoio financeiro ao outro participante (encontros com pessoas mais velhas movidos por interesses financeiros) ou esteja implícito que tal irá acontecer.
- Apps que rebaixem ou tratem pessoas como objetos, tais como apps que afirmam despir as pessoas ou ver através do vestuário, mesmo que identificadas como apps de entretenimento ou de partidas.
- Conteúdos ou comportamentos que tentem ameaçar ou explorar as pessoas de forma sexual, tais como fotos tiradas em público sem o consentimento das pessoas, câmaras ocultas, conteúdos de natureza sexual não consensuais criados através de tecnologia deepfake ou semelhante, ou conteúdos com agressões.

Incitação ao ódio

Não são permitidas apps que promovam violência ou incitem ao ódio contra pessoas ou grupos de pessoas com base na raça, etnia, religião, deficiência, idade, nacionalidade, estatuto de veterano, orientação sexual, género, identidade de género, casta, estatudo de imigração ou qualquer outra caraterística associada a discriminação ou marginalização sistémica.

As apps que incluem conteúdo EDSA (educativo, documental, científico ou artístico) relacionado com nazis podem ser bloqueadas em determinados países, em conformidade com as leis e os regulamentos locais.

Seguem-se alguns exemplos de violações comuns:

- Conteúdo ou discurso que afirme que um grupo protegido é desumano, inferior ou passível de ser alvo de ódio.
- Apps que contenham insultos de ódio, estereótipos ou teorias acerca de um grupo protegido com caraterísticas negativas (por exemplo, malicioso, corrupto, demoníaco, etc.), ou que declare de forma explícita ou implícita que o grupo é uma ameaça.
- Conteúdo ou discurso que tente encorajar outros a acreditar que as pessoas devem ser odiadas ou discriminadas por serem membros de um grupo protegido.
- Conteúdo que promova símbolos de ódio, como bandeiras, símbolos, insígnias, artigos ou comportamentos associados a grupos de ódio.

Violência

Não são permitidas apps que retratem ou promovam violência gratuita ou outras atividades perigosas. Geralmente, são permitidas apps que representem violência fictícia no contexto de um jogo, como desenhos animados, caça ou pesca.

Seguem-se alguns exemplos de violações comuns:

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

Extremismo violento

A Google não permite que organizações terroristas, ou outras organizações ou movimentos perigosos que se tenham envolvido em atos de violência contra civis, se tenham preparado para estes ou reivindicado a responsabilidade destes, publiquem apps no Google Play seja para que fim for, incluindo recrutamento.

Também não são permitidas apps com conteúdo relacionado com extremismo violento ou conteúdo relacionado com o planeamento, a preparação ou a glorificação da violência contra civis, nomeadamente conteúdo que promova atos terroristas, incite à violência ou festeje ataques terroristas. Se publicar conteúdos relacionados com extremismo violento para fins educativos, documentais, científicos ou artísticos, tenha o cuidado de indicar um contexto EDSA relevante.

Eventos sensíveis

Não são permitidas apps que tirem partido ou que não revelem sensibilidade em relação a um evento sensível com impacto social, cultural ou político significativo, tais como emergências civis, desastres naturais, emergências de saúde pública, conflitos, mortes ou outros eventos trágicos. Geralmente, são permitidas apps com conteúdo relacionado com um acontecimento sensível se esse conteúdo tiver valor EDSA (educativo, documental, científico ou artístico), ou quiser alertar ou sensibilizar os utilizadores para o evento sensível.

Seguem-se alguns exemplos de violações comuns:

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

Bullying e assédio

Não são permitidas apps que incluam ou promovam ameaças, assédio ou bullying.

Seguem-se alguns exemplos de violações comuns:

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

Produtos perigosos

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

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

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

Marijuana

Não são permitidas apps que promovam a venda de marijuana ou produtos de marijuana, independentemente da sua legalidade.

Seguem-se alguns exemplos de violações comuns:

- Permitir que os utilizadores encomendem marijuana através de uma funcionalidade de compras na app.
- Auxiliar os utilizadores na entrega ou recolha de marijuana.
- Facilitar a venda de produtos com THC (tetra-hidrocanabinol), incluindo produtos como óleos de CBD que contenham THC.

Tabaco e álcool

Não são permitidas apps que facilitem a venda de tabaco ou de produtos de contenham tabaco (tais como cigarros eletrónicos, vaporizadores e bolsas de nicotina) ou que incentivem o consumo ilegal ou impróprio de álcool, tabaco ou nicotina.

Informações adicionais

- Não é permitido descrever nem encorajar a utilização ou a venda de álcool ou tabaco a menores.
- Não é permitido afirmar que o consumo de tabaco pode melhorar a vida social, sexual, profissional, intelectual ou atlética.
- Não é permitido promover o consumo excessivo de álcool de forma favorável, incluindo a representação favorável do seu consumo excessivo, exagerado ou como forma de competição.
- Não são permitidos anúncios, promoções nem a apresentação proeminente de produtos de tabaco (inclui anúncios, faixas, categorias e links para sites de venda de tabaco).
- Podemos permitir a venda limitada de produtos de tabaco em apps de entrega de comida/mercearia em determinadas regiões e sujeita a salvaguardas de restrição de idade (como a verificação de identidade na entrega).
- Podemos permitir a venda de produtos comercializados como auxiliares de cessação de nicotina sujeita a salvaguardas de restrição de idade.

Serviços financeiros

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

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

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

Todas as apps que incluam funcionalidades financeiras têm de preencher o Formulário de declaração de funcionalidades financeiras na Play Console.

Opções binárias

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

Empréstimos pessoais

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

- Exemplos: empréstimos pessoais, empréstimos de ordenado, empréstimos coletivos, empréstimos com garantia automóvel
- Exemplos não incluídos: hipotecas, crédito automóvel e linhas de crédito rotativo (como cartões de crédito e linhas de crédito pessoal)

As apps que fornecem empréstimos pessoais, incluindo, entre outras, as apps que oferecem empréstimos diretamente, geram leads e ligam os consumidores a credores de terceiros, têm de ter a categoria de apps definida como "Finanças" na Play Console e divulgar as seguintes informações nos respetivos metadados:

- O período mínimo e máximo para o reembolso
- A taxa anual efetiva (TAE) máxima, que geralmente inclui a taxa de juro, bem como taxas e outros custos durante um ano, ou qualquer outra taxa semelhante calculada em conformidade com a legislação local
- Um exemplo representativo do custo total do empréstimo, incluindo o capital e todas as taxas aplicáveis
- Uma política de privacidade que divulgue de forma abrangente o acesso, a recolha, a utilização e a partilha de dados pessoais e confidenciais do utilizador, sujeitos às restrições descritas nesta política

Não são permitidas apps que promovam empréstimos pessoais que requeiram o pagamento na totalidade em 60 dias ou menos a contar da data de emissão do empréstimo (denominados "empréstimos pessoais a curto prazo").

Serão consideradas exceções a esta política as apps de empréstimos pessoais que operem em países nos quais determinados regulamentos permitam expressamente tais práticas de empréstimo a curto prazo ao abrigo dos enquadramentos legais estabelecidos. Nestes casos raros, as exceções serão avaliadas de acordo com as diretrizes regulamentares e as leis locais aplicáveis do respetivo país.

Temos de conseguir estabelecer uma ligação entre a sua conta de programador e as licenças ou documentação fornecidas para comprovar a sua capacidade de conceder empréstimos pessoais. Podem ser necessários documentos ou informações adicionais para confirmar que a sua conta está em conformidade com todas as leis e regulamentos locais.

As apps de empréstimos pessoais, apps cujo objetivo principal é facilitar o acesso a empréstimos pessoais (por exemplo, facilitadores ou geradores de leads), as apps de empréstimos complementares (calculadoras de empréstimos, guias de empréstimos, etc.) e as apps de acesso ao salário ganho (EWA) estão proibidas de aceder a dados confidenciais, como fotos e contactos. As seguintes autorizações são proibidas:

- Read_external_storage
- Read_media_images

- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

As apps que utilizam APIs ou informações confidenciais estão sujeitas a restrições e requisitos adicionais. Consulte a Política de autorizações para ver informações adicionais.

Empréstimos pessoais associados a uma TAE elevada

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

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

Requisitos específicos do país

As apps de empréstimos pessoais que segmentam os países indicados têm de estar em conformidade com requisitos adicionais e fornecer documentação complementar como parte da declaração de funcionalidades financeiras na Play Console. Mediante pedido ao Google Play, tem de fornecer mais informações ou documentos relacionados com a sua conformidade com os requisitos de licenciamento e regulamentares aplicáveis.

1. **Índia**
   - Se possuir uma licença do Reserve Bank of India (RBI) para fornecer empréstimos pessoais, tem de enviar uma cópia da mesma para que a possamos rever.
   - Se não participar diretamente em atividades de empréstimos e apenas disponibilizar uma plataforma para facilitar os empréstimos por empresas financeiras não bancárias registadas (NBFCs) ou bancos aos utilizadores, tem de refletir este facto com precisão na declaração.
     - Além disso, os nomes de todas as NBFCs registadas e de todos os bancos têm de ser divulgados de forma destacada na descrição da sua app.
2. **Indonésia**
   - Se a sua app estiver envolvida na atividade de serviços de empréstimos baseados em tecnologias da informação de acordo com o Regulamento OJK n.º 77/POJK.01/2016 (e as respetivas alterações periódicas), tem de enviar uma cópia da sua licença válida para a podermos rever.
3. **Filipinas**
   - Todas as empresas de financiamento e empréstimos que disponibilizem empréstimos através de plataformas de empréstimos online (OLP) têm de obter um número de registo SEC e o número do certificado da AC (autoridade de certificação) da Comissão de Valores Imobiliários das Filipinas (PSEC).
     - Além disso, tem de divulgar o nome da empresa, o número de registo da PSEC e o certificado da AC (autoridade de certificação) para operar uma empresa de financiamento/empréstimos na descrição da sua app.
   - As apps envolvidas em atividades de financiamento coletivo baseadas em empréstimos, como empréstimos ponto a ponto (P2P) ou conforme definido ao abrigo das regras e regulamentos que regem o financiamento coletivo (Regras de FC), têm de processar transações através de intermediários de FC registados na PSEC.
4. **Nigéria**

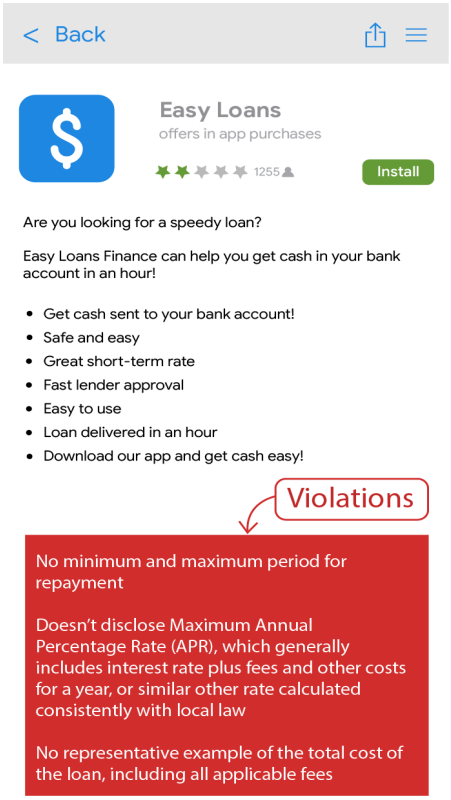
- A Digital Money Lenders (DML) tem de aceitar e preencher o REGULAMENTO PROVISÓRIO LIMITADO, O QUADRO DE REGISTO E AS DIRETRIZES DE EMPRÉSTIMO DIGITAL de 2022 (que podem ser alterados periodicamente) da Comissão Federal de Proteção do Consumidor e da Concorrência (FCCPC) da Nigéria e obter uma carta de aprovação validável da FCCPC.
- Os Agregadores de empréstimos têm de facultar documentação e/ou uma certificação relativa aos serviços de empréstimo digitais, bem como detalhes de contacto de cada DML parceiro.

5. **Quénia**
   - Os fornecedores de crédito digital (DCPs) devem preencher o processo de registo do DCP e obter uma licença do Banco Central do Quénia (CBK). Tem de fornecer uma cópia da sua licença do CBK como parte da sua declaração.
   - Se não participar diretamente em atividades de empréstimos e apenas disponibilizar uma plataforma para facilitar os empréstimos por DCPs registados aos utilizadores, tem de refletir este facto com precisão na declaração e fornecer uma cópia da licença do DCP dos respetivos parceiros.
   - Atualmente, só aceitamos declarações e licenças de entidades publicadas no diretório de fornecedores de crédito digital no Website oficial do CBK.

6. **Paquistão**
   - Cada credor que seja uma empresa financeira não bancária (NBFC) só pode publicar uma app de empréstimos digitais (DLA). Os programadores que tentem publicar mais do que uma DLA por NBFC correm o risco de encerramento da respetiva conta de programador e quaisquer outras contas associadas.
   - Tem de enviar um comprovativo da aprovação da SECP (Securities and Exchange Commission of Pakistan) para prestar ou facilitar serviços de empréstimos digitais no Paquistão.

7. **Tailândia**
   - As apps de empréstimos pessoais que segmentam a Tailândia, com taxas de juro iguais ou superiores a 15%, têm de receber uma licença válida do Bank of Thailand (BoT) ou do Ministério das Finanças (MoF). Os programadores têm de facultar documentação que comprove a respetiva capacidade de fornecer ou facilitar empréstimos pessoais na Tailândia. Esta documentação deve incluir:
     - Uma cópia da respetiva licença emitida pelo Bank of Thailand para operar como fornecedor de empréstimos pessoais ou uma organização nanofinanceira.
     - Uma cópia da respetiva licença comercial de serviços financeiros Pico emitida pelo Ministério das Finanças para operar como credor Pico ou Pico-plus.

Segue-se um exemplo de uma violação comum:



Jogos de azar a dinheiro real, jogos e concursos

Permitimos apps de jogos de azar a dinheiro real, anúncios relacionados com jogos de azar a dinheiro real, programas de fidelidade com gamificação e apps de daily fantasy sports que cumpram determinados requisitos.

Apps de jogos de azar

Sujeito às restrições e à conformidade com todas as Políticas do Google Play, permitimos apps que permitam ou facilitem jogos de azar online em determinados países, desde que o programador conclua o processo de candidatura relativo a apps de jogos de azar distribuídas no Google Play, seja um operador governamental aprovado e/ou esteja registado como um operador licenciado junto da autoridade governamental que regula os jogos de azar adequada no país especificado e forneça uma licença de funcionamento válida no país especificado para o tipo de produto de jogos de azar online que pretende oferecer.

Permitimos apenas apps de jogos de azar autorizadas ou com licença válida com os seguintes tipos de produtos de jogos de azar online:

- Jogos de casino online
- Apostas desportivas
- Corridas de cavalos (onde forem regulamentadas e licenciadas em separado das apostas desportivas)
- Lotarias
- Daily fantasy sports

As apps elegíveis têm de cumprir os seguintes requisitos:

- O programador tem de concluir o processo de candidatura com êxito para distribuir a app no Google Play;
- A app tem de estar em conformidade com todas as leis e normas da indústria aplicáveis a cada país no qual é distribuída;

- O programador precisa de uma licença válida de jogos de azar para cada país ou estado/território no qual a app é distribuída;
- O programador não pode oferecer um tipo de produto de jogos de azar que exceda o âmbito da respetiva licença de jogos de azar;
- A app tem de impedir que os utilizadores menores utilizem a mesma;
- A app tem de impedir o acesso e a utilização em países, estados/territórios ou áreas geográficas não abrangidos pela licença de jogos de azar fornecida pelo programador;
- A app NÃO pode ser adquirida como uma app paga no Google Play, nem usar a Faturação em apps do Google Play;
- A transferência e a instalação da app têm de ser gratuitas a partir da Google Play Store;
- A app tem de incluir a classificação AA (Apenas adultos) ou equivalente da IARC; e
- A app e a ficha da app têm de apresentar claramente informações acerca de jogos de azar responsáveis.

Outras apps de jogos, concursos e torneios a dinheiro real

Relativamente a todas as outras apps que não cumpram os requisitos de elegibilidade das apps de jogos de azar mencionados acima e não estejam incluídas nos "Outros testes-pilotos de jogos a dinheiro real" mencionados abaixo, não permitimos conteúdos ou serviços que autorizem ou facilitem aos utilizadores apostar, arriscar ou participar com dinheiro real (incluindo itens na app comprados com dinheiro) para obter um prémio de valor monetário real. Isto inclui, entre outros, casinos online, apostas desportivas, lotarias e jogos que aceitam dinheiro e oferecem prémios em dinheiro ou outro valor real (exceto programas permitidos ao abrigo dos requisitos dos programas de fidelidade com gamificação descritos abaixo).

Exemplos de violações

- Jogos que aceitam dinheiro em troca de uma oportunidade de ganhar um prémio físico ou monetário.
- Apps com funcionalidades ou elementos de navegação (por exemplo, itens de menu, separadores, botões, WebViews, etc.) que fornecem um "apelo à ação" para apostar, arriscar ou participar em jogos, concursos ou torneios a dinheiro real, tais como apps que convidam os utilizadores a apostarem, registarem-se ou competirem num torneio para se habilitarem a ganhar um prémio em dinheiro.
- Apps que aceitam ou gerem apostas, moedas na app, ganhos ou depósitos para apostar ou obter um prémio físico ou monetário.

Outros testes-pilotos de jogos a dinheiro real

Ocasionalmente, podemos realizar testes-piloto por tempo limitado para determinados tipos de videojogos com dinheiro real em regiões selecionadas. Para obter detalhes, consulte esta página do Centro de Ajuda. O teste-piloto dos jogos de gancho online no Japão terminou a 11 de julho de 2023. A partir de 12 de julho de 2023, as apps de jogos de gancho online podem ser apresentadas no Google Play globalmente, sujeitos à lei aplicável e a determinados requisitos.

Programas de fidelidade com gamificação

Nos casos permitidos por lei e não sujeitos a requisitos de licenciamento de jogos de azar ou jogos adicionais, permitimos programas de fidelidade que recompensem os utilizadores com prémios reais ou um equivalente monetário, sujeito aos seguintes requisitos de elegibilidade da Play Store:

Para todas as apps (jogos e não jogos):

- As vantagens, os benefícios ou os prémios do programa de fidelidade têm de ser claramente complementares e subordinados a qualquer transação monetária elegível na app (em que a transação monetária elegível tem de ser uma transação separada genuína para fornecer bens ou

serviços independentes do programa de fidelidade) e não podem estar sujeitos a compra nem associados a qualquer modo de troca que viole as restrições da Política de Jogos de Azar a Dinheiro Real, Jogos e Concursos.

- Por exemplo, nenhuma parte da transação monetária elegível pode representar uma taxa ou uma aposta para participar no programa de fidelidade e a transação monetária elegível não pode resultar na compra de bens ou serviços acima do preço habitual.

Para apps de jogos :

- Os prémios ou os pontos de fidelidade com vantagens, benefícios ou prémios associados a uma transação monetária elegível apenas podem ser atribuídos e resgatados com base numa relação fixa, na qual a relação está documentada de forma clara na app e também nas regras oficiais do programa disponíveis publicamente. Além disso, os ganhos das vantagens ou o valor de resgate **não** podem ser apostados, atribuídos ou exponenciados pelo desempenho do jogo ou por resultados baseados em hipóteses.

Para apps que não são jogos:

- Os prémios ou os pontos de fidelidade podem ser associados a um concurso ou a resultados baseados em hipóteses, se cumprirem os requisitos indicados abaixo. Os programas de fidelidade com vantagens, benefícios ou prémios associados a uma transação monetária elegível têm de:
  - Publicar regras oficiais do programa na app.
  - Para programas que envolvam sistemas de prémios variáveis, baseados em hipóteses ou aleatórios: divulgar nos termos oficiais para o programa 1) as probabilidades para quaisquer programas de recompensas que utilizem probabilidades fixas para determinar os prémios e 2) o método de seleção (por exemplo, variáveis utilizadas para determinar o prémio) para todos os outros programas.
  - Especificar um número fixo de vencedores, um prazo de participação fixo e uma data de atribuição do prémio, por promoção, nos termos oficiais de um programa com sorteios, apostas ou outras promoções semelhantes.
  - Documentar de forma clara qualquer relação fixa para o resgate e a acumulação de prémios de fidelidade ou pontos de fidelidade na app, bem como nos termos oficiais do programa.

Tipo de app com programa de fidelidade	**Prémios variáveis e gamificação de fidelidade**	**Prémios de fidelidade com base numa relação/agenda fixa**	**Termos de Utilização do programa de fidelidade obrigatórios**	**Os Termos de Utilização têm de divulgar as probabilidades ou o método de seleção de qualquer programa de fidelidade baseado em hipóteses**
Jogo	Não permitidos	Permitidos	Obrigatório	N/A (as apps de jogos não podem ter elementos baseados em hipóteses em programas de fidelidade)
Não jogo	Permitidos	Permitidos	Obrigatório	Obrigatório

Anúncios de jogos de azar ou jogos, concursos e torneios a dinheiro real em apps distribuídas no Google Play

Permitimos apps com anúncios que promovam jogos de azar, jogos, concursos e torneios a dinheiro real se cumprirem os seguintes requisitos:

- A app e o anúncio (incluindo os anunciantes) têm de estar em conformidade com todas as normas da indústria e leis aplicáveis em todas as localizações nas quais o anúncio é apresentado;
- O anúncio tem de cumprir todos os requisitos de licenciamento de anúncios locais aplicáveis para todos os serviços e produtos relacionados com jogos de azar que estão a ser promovidos;

- A app não deve apresentar um anúncio de jogos de azar a indivíduos com menos de 18 anos;
- A app não pode estar inscrita no programa Concebido para Famílias;
- A app não se pode destinar a indivíduos com menos de 18 anos;
- Se anunciar uma app de jogos de azar (conforme definido acima), o anúncio tem de apresentar claramente informações acerca de jogos de azar responsáveis na respetiva página de destino, na própria ficha da app anunciada ou na app;
- A app não pode fornecer conteúdo de jogos de azar simulado (por exemplo, apps de casinos sociais ou apps com slot machines virtuais);
- A app não pode ter suporte a jogos de azar ou jogos, lotarias ou torneios a dinheiro real nem funcionalidades associadas (por exemplo, funcionalidades que ajudem a fazer apostas, pagamentos, monitorização de resultados desportivos/probabilidades/desempenho ou gestão de fundos de participação);
- O conteúdo da app não pode promover nem direcionar os utilizadores para serviços de jogos de azar ou jogos, lotarias ou torneios a dinheiro real

Apenas as apps que cumpram todos estes requisitos na secção listada (acima) podem incluir anúncios de jogos de azar ou jogos, lotarias ou torneios a dinheiro real. As apps de jogos de azar aceites (conforme definido acima) ou as apps de daily fantasy sport aceites (conforme definido abaixo) que cumpram os requisitos 1 a 6 acima podem incluir anúncios de jogos de azar ou jogos, lotarias ou torneios a dinheiro real.

Exemplos de violações

- Uma app concebida para utilizadores menores de idade e que apresenta um anúncio que promove serviços de jogos de azar.
- Um jogo de casino simulado que promove ou direciona os utilizadores para casinos a dinheiro real.
- Uma app dedicada ao acompanhamento de probabilidades desportivas que inclui anúncios de jogos de azar integrados com links para um site de apostas desportivas.
- Apps com anúncios de jogos de azar que violam a nossa Política de Anúncios Enganadores, como anúncios apresentados aos utilizadores como botões, ícones ou outros elementos interativos na app.

Apps de daily fantasy sports (DFS)

Apenas são permitidas apps de daily fantasy sports (DFS), conforme definido pela lei local aplicável, se cumprirem os seguintes requisitos:

- A app é 1) distribuída apenas nos Estados Unidos ou 2) elegível ao abrigo dos requisitos e processo de candidatura relativos a apps de jogos de azar mencionados acima em países que não sejam os EUA;
- O programador tem de concluir com êxito o processo de candidatura a DFS e ser aceite para distribuir a app no Google Play;
- A app tem de estar em conformidade com todas as normas da indústria e leis aplicáveis em todos os países nos quais é distribuída;
- A app tem de impedir os utilizadores menores de participarem em transações monetárias na app;
- A app NÃO pode ser adquirida como uma app paga no Google Play, nem utilizar a Faturação em apps do Google Play;
- A transferência e a instalação da app têm de ser gratuitas a partir da Play Store;
- A app tem de incluir a classificação AA (Apenas adultos) ou equivalente da IARC;
- A app e a ficha da app têm de apresentar claramente informações acerca de jogos de azar responsáveis;
- A app tem de cumprir todas as normas da indústria e leis aplicáveis em qualquer estado ou território dos EUA em que é distribuída;

- O programador precisa de uma licença válida para cada estado ou território dos EUA em que seja obrigatória uma licença para apps de daily fantasy sports;
- A app tem de impedir a utilização em estados ou territórios dos EUA nos quais o programador não possui uma licença obrigatória para apps de daily fantasy sports; e
- A app tem de impedir a utilização em estados ou territórios dos EUA onde as apps de daily fantasy sports não são legais.

Atividades ilegais

Não são permitidas apps que facilitem ou promovam atividades ilegais.

Seguem-se alguns exemplos de violações comuns:

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

Conteúdo gerado pelo utilizador

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

As apps que incluam ou apresentem UGC, incluindo apps que são navegadores ou clientes especializados para direcionar os utilizadores para uma plataforma de UGC, têm de implementar uma moderação de UGC robusta, eficaz e contínua que:

- Exija que os utilizadores aceitem os termos de utilização e/ou a política do utilizador da app para poderem criar ou carregar UGC;
- Defina comportamentos e conteúdo censurados (de modo a cumprir as Políticas do Programa para Programadores do Google Play) e que os proíba nos termos de utilização ou nas políticas do utilizador da app;
- Realize uma moderação de UGC, na medida do que for razoável e consistente com o tipo de UGC alojado pela app. Isto inclui a disponibilização de um sistema na app para denunciar e bloquear UGC e utilizadores censuráveis, bem como a tomada de medidas contra UGC e utilizadores quando apropriado. Experiências de UGC diferentes podem exigir esforços de moderação diferentes. Por exemplo:
  - As apps com UGC que identifiquem um conjunto específico de utilizadores através de meios como a validação de utilizadores ou o registo offline (por exemplo, apps usadas exclusivamente numa empresa ou escola específica, etc.) têm de disponibilizar uma funcionalidade na app para denunciar conteúdo e utilizadores.
  - As funcionalidades de UGC que permitam a interação do utilizador individual com utilizadores específicos (por exemplo, mensagens diretas, etiquetagens, menções, etc.) têm de disponibilizar uma funcionalidade na app para bloquear utilizadores.
  - As apps que disponibilizem acesso a UGC acessível publicamente, como apps de redes sociais e apps de blogues, têm de implementar uma funcionalidade na app para denunciar utilizadores e conteúdo, bem como para bloquear utilizadores.
  - No caso de Apps de realidade aumentada, a moderação do UGC (incluindo o sistema de denúncias na app) tem de ter em conta tanto o UGC de realidade aumentada censurável (por exemplo, uma imagem de realidade aumentada sexualmente explícita) e a localização de ancoragem de realidade aumentada confidencial (por exemplo, conteúdo de realidade aumentada ancorado a uma área restrita, como uma base militar ou uma propriedade privada na qual a ancoragem de realidade aumentada possa causar problemas ao proprietário).

- Forneça salvaguardas para evitar que a rentabilização na app incentive comportamentos censuráveis dos utilizadores.

Conteúdos de natureza sexual fortuitos

Os conteúdos de natureza sexual são considerados "fortuitos" se aparecerem numa app de UGC que (1) dá acesso a conteúdos essencialmente de natureza não sexual e (2) não promove nem recomenda ativamente conteúdos de natureza sexual. Os conteúdos de natureza sexual definidos como ilegais pela lei aplicável e os conteúdos de perigo para as crianças não são considerados "fortuitos" e não são permitidos.

As apps de UGC podem incluir conteúdos de natureza sexual fortuitos se todos os requisitos seguintes forem cumpridos:

- Esses conteúdos estão ocultados por predefinição através de filtros que requerem, pelo menos, duas ações do utilizador para serem completamente desativados (por exemplo, através de um anúncio intercalar de ocultação ou ocultados por predefinição, a menos que a "Pesquisa segura" esteja desativada).
- As crianças, conforme definido na Política para Famílias, estão explicitamente proibidas de aceder à sua app através de sistemas de filtragem de idade, como um ecrã de idade neutro ou um sistema apropriado, conforme definido pela lei aplicável.
- A sua app fornece respostas precisas ao questionário de classificação de conteúdo relativo ao UGC, conforme exigido pela Política de Classificações de Conteúdo.

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

Seguem-se alguns exemplos de violações comuns:

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

Serviços e conteúdo de saúde

Não são permitidas apps que exponham os utilizadores a conteúdos e serviços prejudiciais para a saúde.

Se a sua app possuir ou promover conteúdos e serviços de saúde, tem de garantir que a mesma está em conformidade com todas as leis e regulamentos aplicáveis.

Apps de saúde

Se a sua app acede a dados de saúde e é uma app de saúde ou oferece funcionalidades relacionadas com saúde, tem de agir em conformidade com as Política para Programadores do Google Play existentes, incluindo Privacidade, Logro e Abuso, bem como Eventos sensíveis, além dos requisitos abaixo:

- **Declaração da Play Console:**
  - Aceda à página Conteúdo da app (Política > Conteúdo da app) na Play Console e selecione a categoria ou as categorias às quais a sua app pertence.

- **Política de Privacidade e requisitos de divulgação destacada:**
  - A sua app tem de publicar um link da Política de Privacidade no campo designado na Play Console e um texto ou link da Política de Privacidade na própria app. Certifique-se de que a sua Política de Privacidade está disponível num URL ativo, acessível e sem perímetro virtual (sem PDFs) e não é editável (conforme a Secção segurança dos dados).
  - Em conjunto com eventuais divulgações na app, a Política de Privacidade da sua app tem de divulgar de modo abrangente o acesso, a recolha, a utilização e a partilha de dados pessoais e confidenciais do utilizador sem se limitar aos dados divulgados na Secção segurança dos dados acima. Para funcionalidades ou dados regulados por autorizações perigosas ou de tempo de execução , a app tem de cumprir todos os requisitos de divulgação destacada e consentimento aplicáveis.
  - As autorizações que não sejam necessárias para que a app de saúde execute a respetiva funcionalidade essencial não devem ser pedidas, e as autorizações não usadas têm de ser removidas. Para ver a lista de autorizações consideradas como estando no âmbito de dados confidenciais relacionados com a saúde, consulte o artigo Categorias de apps de saúde e informações adicionais.
  - Se a sua app não for uma app principalmente de saúde, mas tiver funcionalidades relacionadas com a saúde e aceder a dados de saúde, continua a estar no âmbito da Política de Apps de Saúde. Deve ser clara para o utilizador a ligação entre a funcionalidade essencial da app e a recolha de dados relacionados com a saúde (por exemplo, seguradoras, apps de jogos que recolham dados de atividade de um utilizador como forma de avançar a jogabilidade, etc.) A Política de Privacidade da app tem de refletir esta utilização limitada.
- **Requisitos adicionais:**
  Se a sua app de saúde se qualificar para uma das seguintes designações, tem de agir em conformidade com os requisitos relevantes e selecionar a categoria adequada na Play Console:
  - **Apps de saúde afiliadas ao governo:** se tiver autorização do governo ou de uma organização de cuidados de saúde reconhecida para desenvolver e distribuir uma app em afiliação com estes, tem de enviar um comprovativo da elegibilidade através do formulário de aviso prévio.
  - **Apps de rastreio de contactos/estado de saúde:** se a sua app for uma app de rastreio de contactos e/ou estado de saúde, selecione "Prevenção de doenças e saúde pública" na Play Console e faculte as informações necessárias através do formulário de aviso prévio acima.
  - **Apps de investigação em seres humanos:** as apps que realizam investigações em seres humanos relacionadas com a saúde têm de cumprir todas as regras e regulamentos, incluindo, entre outros, a obtenção do consentimento informado dos participantes ou, no caso de menores, dos respetivos pais ou tutores. As apps de investigação na área da saúde também devem ser aprovadas junto de um conselho de revisão institucional (IRB) e/ou comité de ética independente semelhante, salvo isenção em contrário. A prova dessa aprovação tem de ser facultada mediante pedido.
  - **Apps de dispositivos médicos ou SaMD:** as apps que sejam consideradas como sendo dispositivos médicos ou SaMDs precisam de ter e manter uma carta de autorização ou outra documentação de aprovação que tenha sido facultada por uma autoridade reguladora ou um organismo responsável pela administração e conformidade da app de saúde. É necessário facultar um comprovativo de tal autorização ou aprovação no momento do pedido.

Dados da Saúde Connect

Os dados acedidos através das autorizações da Saúde Connect são considerados como dados pessoais e confidenciais do utilizador sujeitos à Política de Dados do Utilizador e a requisitos adicionais .

Medicamentos com receita médica

Não são permitidas apps que facilitem a venda ou a compra de medicamentos sem receita médica.

Substâncias não aprovadas

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

Seguem-se alguns exemplos de violações comuns:

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

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

Desinformação sobre saúde

Não são permitidas apps que contêm declarações de saúde enganosas que contradizem o consenso médico existente ou que podem causar danos aos utilizadores.

Seguem-se alguns exemplos de violações comuns:

- Declarações enganosas sobre vacinas, tais como que as vacinas podem alterar o ADN de uma pessoa.
- Defesa de tratamentos nocivos e não aprovados.
- Defesa de outras práticas nocivas para a saúde, tais como a terapia de conversão.

Funcionalidades médicas

Não permitimos apps que incluam funcionalidades médicas ou relacionadas com a saúde que sejam enganadoras ou potencialmente prejudiciais. Por exemplo, não são permitidas apps que reivindicam ter uma funcionalidade de oximetria que se baseia exclusivamente em apps. As apps de oximetria têm de ser suportadas por hardware externo, acessórios ou sensores de smartphones dedicados concebidos para suportar a funcionalidade de oximetria. Estas apps suportadas também têm de conter exclusões de responsabilidade nos metadados a declarar que não se destinam a utilização médica, que são apenas concebidas para fins gerais de fitness e bem-estar, e que não constituem um dispositivo médico, bem como divulgar devidamente o modelo de hardware/modelo do dispositivo compatível.

Pagamentos - serviços clínicos

As transações que envolvam serviços clínicos regulamentados não devem usar o sistema de faturação do Google Play. Para mais informações, consulte Compreender a Política de Pagamentos do Google Play .

Conteúdo baseado em blockchain

À medida que a tecnologia de blockchain continua a evoluir rapidamente, visamos oferecer uma plataforma para os programadores prosperarem com inovação e criarem experiências mais avançadas e envolventes para os utilizadores.

Para efeitos da presente política, a Google define o conteúdo baseado em blockchain como sendo ativos digitais convertidos em tokens protegidos numa blockchain. Se a sua app tiver conteúdo baseado em blockchain, tem de agir em conformidade com estes requisitos.

Câmbios de criptomoedas e softwares de carteira

A compra, a posse ou a troca de criptomoedas deve ser realizada através de serviços certificados em jurisdições reguladas.

Também tem de agir em conformidade com os regulamentos aplicáveis de todos os países ou regiões que a sua app segmente e evitar publicar a sua app onde os seus produtos e serviços são proibidos. O Google Play pode pedir-lhe que faculte informações ou documentos adicionais relativos à sua conformidade com os requisitos regulamentares ou de licenciamento.

Mineração de criptomoedas

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

Requisitos de transparência para a distribuição de ativos digitais convertidos em tokens

Se a sua app vender ou permitir que os utilizadores ganhem ativos digitais convertidos em tokens, tem de declarar isto através do formulário de declaração Funcionalidades financeiras na página Conteúdo da app na Play Console.

Quando criar um produto na app, tem de indicar nos detalhes deste que representa um ativo digital convertido em token. Para obter orientações adicionais, veja o artigo Crie um produto na app.

Não pode promover nem destacar potenciais ganhos provenientes de atividades de jogo ou negociação.

Requisitos adicionais para a gamificação de NFTs (tokens não fungíveis)

Conforme exigido pela Política de Jogos de Azar a Dinheiro Real, Jogos e Concursos do Google Play, as apps de jogos de azar que integram os ativos digitais convertidos em tokens, como os NFTs, devem concluir o processo de candidatura.

Relativamente a todas as outras apps que não cumpram os requisitos de elegibilidade para apps de jogos de azar e não estejam incluídas nos Outros testes-pilotos de jogos a dinheiro real, não deve ser aceite algo de valor monetário em troca de uma possibilidade de obter um NFT de valor desconhecido. Os NFTs comprados por utilizadores devem ser consumidos ou usados no jogo para melhorar a experiência de um utilizador ou ajudar os utilizadores a progredir no jogo. Os NFTs não podem ser usados para apostar ou arriscar em troca da oportunidade de ganhar prémios de valor monetário do mundo real (incluindo outros NFTs).

Seguem-se alguns exemplos de violações comuns:

- As apps que vendem pacotes de NFTs sem divulgar os respetivos conteúdos e valores dos NFTs.
- Jogos sociais de casino em que se paga para jogar, como slot machines, que recompensam com NFTs.

Conteúdo gerado pela IA

À medida que os modelos de IA generativa são disponibilizados de forma mais abrangente aos programadores, pode incorporá-los nas suas apps para aumentar a interação e melhorar a experiência do utilizador. O Google Play quer ajudar a garantir que o conteúdo gerado pela IA é seguro

para todos os utilizadores e que o feedback dos utilizadores é incorporado para permitir uma inovação responsável.

Conteúdo gerado pela IA

O conteúdo gerado pela IA é conteúdo criado por modelos de IA generativa com base em comandos do utilizador. Alguns exemplos de conteúdo gerado pela IA incluem:

- Bots de chat de IA generativa de conversação de texto para texto, em que a interação com o bot de chat é uma funcionalidade central da app
- Imagem gerada pela IA com base em texto, imagem ou comandos de voz

Para garantir a segurança dos utilizadores e, de acordo com a Abrangência das Políticas do Google Play, as apps que geram conteúdo através da IA têm de estar em conformidade com as Políticas para Programadores do Google Play existentes, inclusive através da proibição e prevenção de conteúdo restrito, por exemplo, conteúdo que facilite a exploração ou o abuso de crianças e conteúdo que permite comportamento enganador.

As apps que geram conteúdo através da IA têm de conter funcionalidades de denúncia ou sinalização por utilizadores na app que permitam aos utilizadores denunciar ou sinalizar conteúdo ofensivo aos programadores sem terem de sair da app. Os programadores devem usar os relatórios dos utilizadores para informar a filtragem e a moderação de conteúdo nas respetivas apps.

Propriedade intelectual

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

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

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

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

Se possuir documentação escrita que comprove a sua autorização para utilizar a propriedade intelectual de terceiros na sua app ou Ficha da loja (por exemplo, nomes, logótipos e recursos gráficos de marcas), contacte a equipa do Google Play antes do envio para garantir que a sua app não é rejeitada devido a uma violação de propriedade intelectual.

Utilização não autorizada de conteúdo protegido por direitos de autor

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

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

Seguem-se alguns exemplos de violações comuns:

- Capas de álbuns de música, de videojogos e de livros.
- Imagens de marketing de filmes, de televisão ou de videojogos.

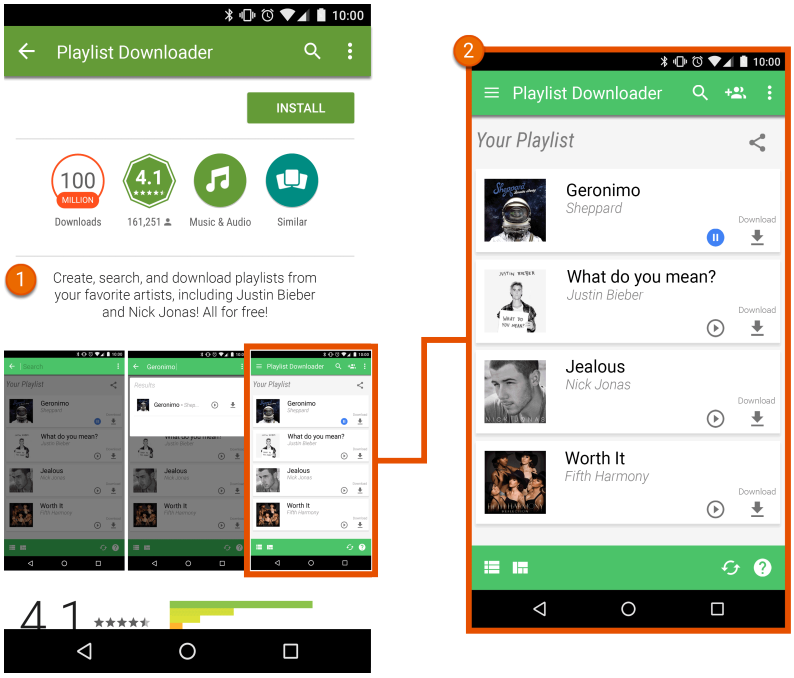
- Ilustrações ou imagens de livros de banda desenhada, de desenhos animados, de vídeos de música ou de televisão.
- Logótipos de equipas desportivas profissionais e universitárias.
- Fotos retiradas de contas de redes sociais de figuras públicas.
- Imagens profissionais de figuras públicas.
- Reproduções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

Encorajamento à violação de direitos de autor

Não são permitidas apps que induzam ou encorajem a violação de direitos de autor. Antes de publicar a sua app, verifique se esta está de alguma forma a encorajar a violação de direitos de autor e obtenha aconselhamento jurídico se necessário.

Seguem-se alguns exemplos de violações comuns:

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



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

Violação de marca comercial

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

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

Contrafação

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

Privacidade, logro e abuso de dispositivos

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

Dados do utilizador

Tem de ser transparente no modo como processa os dados do utilizador (por exemplo, as informações recolhidas sobre ou de um utilizador, incluindo as informações do dispositivo). Isso significa divulgar o acesso, recolher, usar, processar e partilhar dados do utilizador a partir da sua app e limitar a utilização dos dados às finalidades divulgadas em conformidade com a política. Tenha em atenção que qualquer processamento de dados pessoais e confidenciais do utilizador está também sujeito aos requisitos adicionais na secção "Dados pessoais e confidenciais do utilizador" abaixo. Estes requisitos do Google Play são adicionais a quaisquer requisitos estabelecidos por leis de privacidade e proteção de dados aplicáveis.

Se incluir código de terceiros (por exemplo, um SDK) na sua app, tem de assegurar que o código usado na app e as práticas de terceiros referentes aos dados do utilizador a partir da sua app estão em conformidade com as Políticas do Programa para Programadores do Google Play, as quais incluem requisitos de divulgação e utilização. Por exemplo, tem de assegurar que os fornecedores do SDK não vendem dados pessoais e confidenciais do utilizador a partir da sua app. Este requisito aplica-se independentemente de os dados do utilizadores serem transferidos depois de serem enviados para um servidor ou ao incorporar código de terceiros na sua app.

Dados do utilizador pessoais e confidenciais

Os dados pessoais e confidenciais do utilizador incluem, entre outros, informações de identificação pessoal, informações de pagamento e financeiras, informações de autenticação, lista telefónica, contactos, localização do dispositivo, dados relacionados com chamadas e SMS, dados de saúde, dados da Saúde Connect, inventário de outras apps no dispositivo, microfone, câmara, bem como outros dados de utilização ou confidenciais do dispositivo. Se a sua app processar dados pessoais e confidenciais do utilizador, tem de:

- Limitar o acesso, a recolha, a utilização e a partilha de dados pessoais e confidenciais do utilizador adquiridos através da app para a funcionalidade da app e do serviço, bem como para as finalidades em conformidade com a política esperadas de forma razoável pelo utilizador:
  - As apps que expandem a utilização de dados pessoais e confidenciais do utilizador para publicação de anúncios têm de estar em conformidade com a Política de Anúncios do Google Play.
  - Também pode transferir os dados consoante o necessário para fornecedores de serviços ou por motivos legais, como cumprir um pedido governamental válido, uma lei aplicável ou como parte de um processo de fusão ou aquisição mediante o aviso legalmente adequado aos utilizadores.

- Processar todos os dados pessoais e confidenciais do utilizador de forma segura, incluindo a transmissão através de criptografia moderna (por exemplo, por HTTPS).
- Utilizar um pedido de autorizações de tempo de execução sempre que estiver disponível, antes de aceder a dados bloqueados por autorizações do Android .
- A venda de dados pessoais e confidenciais do utilizador não é permitida.
  - "Venda" significa a troca ou a transferência de dados pessoais e confidenciais do utilizador para terceiros para consideração monetária.
    - Uma transferência de dados pessoais e confidenciais do utilizador iniciada pelo utilizador (por exemplo, quando o utilizador está a usar uma funcionalidade da app para transferir um ficheiro para terceiros ou quando o utilizador opta por usar uma app de estudo de investigação para uma finalidade dedicada) não é considerada venda.

Divulgação destacada e requisito de consentimento

Em casos em que o acesso, a recolha, a utilização ou a partilha de dados pessoais e confidenciais do utilizador da app possam não estar dentro da expetativa razoável do utilizador do produto ou da funcionalidade em questão (por exemplo, se a recolha de dados ocorrer em segundo plano quando o utilizador não está a interagir com a app), tem de cumprir os seguintes requisitos:

Divulgação destacada: tem de fornecer uma divulgação na app do acesso, da recolha, da utilização e da partilha de dados. A divulgação na app:

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

Consentimento e autorizações de tempo de execução: os pedidos de consentimento do utilizador e de autorização de tempo de execução na app têm de ser imediatamente precedidos por uma divulgação na app que cumpra o requisito desta política. O pedido de consentimento da app:

- Tem de apresentar a caixa de diálogo de consentimento de forma clara e inequívoca;
- Tem de requerer uma ação afirmativa do utilizador (por exemplo, tocar para aceitar ou selecionar uma caixa de verificação);
- Não deve interpretar a navegação para fora da divulgação (incluindo tocar para sair ou premir o botão Anterior ou página inicial) como consentimento;
- Não deve usar mensagens com opção para ignorar automaticamente ou com validade como forma de obter consentimento do utilizador; e
- Tem de ser concedido pelo utilizador antes de a app conseguir iniciar a recolha ou o acesso aos dados pessoais e confidenciais do utilizador.

As apps que dependam de outras bases legais para processar dados pessoais e confidenciais do utilizador sem consentimento, como um interesse legítimo ao abrigo do RGPD (Regulamento Geral sobre a Proteção de Dados) da União Europeia, têm de cumprir todos os requisitos legais aplicáveis e fornecer divulgações adequadas aos utilizadores, incluindo divulgações na app, conforme exigido ao abrigo desta política.

Para cumprir os requisitos da política, é recomendável seguir o formato do exemplo abaixo para a divulgação destacada quando exigida:

- "[Esta app] recolhe/transmite/sincroniza/armazena [tipo de dados] para ativar ["funcionalidade"], [em que circunstâncias].

- *Exemplo: "A Fitness Funds recolhe dados de localização para ativar a monitorização de fitness mesmo quando a app está fechada ou não está a ser usada, sendo igualmente usada para suportar publicidade".*
- *Exemplo: "O Call Buddy recolhe dados de registo de chamadas de escrita e leitura para permitir a organização de contactos mesmo quando a app não está a ser usada".*

Se a sua app integrar código de terceiros (por exemplo, um SDK) concebido para recolher dados pessoais e confidenciais do utilizador por predefinição, tem de, num prazo de duas semanas após a receção de um pedido do Google Play (ou, se o pedido do Google Play tiver um período mais longo, dentro desse período), fornecer provas suficientes que demonstrem que a sua app cumpre os requisitos de divulgação destacada e consentimento desta política, incluindo o acesso, a recolha, a utilização ou a partilha de dados através do código de terceiros.

Seguem-se alguns exemplos de violações comuns:

- Uma app que recolhe a localização do dispositivo, mas não tem uma divulgação destacada a explicar que funcionalidade usa estes dados e/ou indica a utilização da app em segundo plano.
- Uma app que tenha uma autorização de tempo de execução a pedir o acesso a dados antes da divulgação destacada que especifica a finalidade da utilização dos dados.
- Uma app que aceda ao inventário de apps instaladas de um utilizador e não trate estes dados como dados pessoais ou confidenciais sujeitos aos requisitos de Política de Privacidade, processamento de dados, divulgação destacada e consentimento mencionados anteriormente.
- Uma app que aceda aos dados do telemóvel ou da agenda telefónica de um utilizador e não trate estes dados como dados pessoais ou confidenciais do utilizador sujeitos aos requisitos de Política de Privacidade, processamento de dados, divulgação destacada e consentimento mencionados acima.
- Uma app que grave o ecrã do utilizador e não trate estes dados como dados pessoais ou confidenciais sujeitos a esta política.
- Uma app que recolha a localização do dispositivo e não divulgue a respetiva utilização de forma abrangente nem obtenha consentimento em conformidade com os requisitos acima.
- Uma app que use autorizações restritas em segundo plano na app, incluindo para fins de monitorização, pesquisa ou marketing, e não divulgue a respetiva utilização de forma abrangente nem obtenha consentimento em conformidade com os requisitos acima.
- Uma app com um SDK que recolha dados pessoais e confidenciais do utilizador, e não trate destes dados em conformidade com esta Política de Dados do Utilizador e os requisitos de divulgação destacada e consentimento, acesso e processamento de dados (incluindo venda não permitida).

Consulte este artigo para obter mais informações sobre o requisito de divulgação destacada e consentimento.

Restrições de acesso a dados pessoais e confidenciais

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

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

	Conceber apps para crianças e famílias para obter os requisitos e a linguagem da política completa.
A sua app recolhe ou associa identificadores de dispositivos permanentes (por exemplo, IMEI, IMSI, número de série do SIM, etc.)	Os identificadores de dispositivos permanentes não podem estar associados a outros dados pessoais e confidenciais do utilizador nem a identificadores de dispositivos redefiníveis, exceto para finalidades de • Telefonia associadas à identidade do SIM (por exemplo, chamadas Wi-Fi associadas à conta do operador); e • Apps de gestão de dispositivos empresariais que utilizem o modo de proprietário do dispositivo. Estas utilizações têm de ser divulgadas de forma proeminente aos utilizadores, conforme especificado na Política de Dados do Utilizador . Consulte este recurso para obter identificadores únicos alternativos. Leia a Política de Anúncios para obter diretrizes adicionais relativas ao ID de publicidade Android.

Secção Segurança dos dados

Todos os programadores têm de elaborar uma Secção Segurança dos dados clara e precisa para cada app que detalhe a recolha, a utilização e a partilha dos dados do utilizador. O programador é responsável pela exatidão da etiqueta e por manter estas informações atualizadas. Quando tal for relevante, a secção tem de ser consistente com as divulgações efetuadas na política de privacidade da app.

Consulte este artigo para obter informações adicionais sobre como elaborar a Secção Segurança dos dados.

Política de privacidade

Todas as apps têm de publicar um link da política de privacidade no campo designado na Play Console e um texto ou link da política de privacidade na própria app. Em conjunto com eventuais divulgações na app, a política de privacidade tem de divulgar de modo abrangente a forma como a app acede, recolhe, usa e partilha os dados do utilizador sem se limitar aos dados divulgados na Secção segurança dos dados. Isto tem de incluir:

- Informações do programador e um ponto de contacto de privacidade ou um mecanismo para enviar perguntas.
- A divulgação dos tipos de dados pessoais e confidenciais do utilizador que a app usa, recolhe ou aos quais acede e com que partes estes são partilhados.
- Procedimentos seguros para o processamento de dados pessoais e confidenciais do utilizador.
- A política de retenção e eliminação de dados do programador.
- Etiquetagem clara como uma Política de Privacidade (por exemplo, listada como "Política de Privacidade" no título).

A entidade (por exemplo, programador ou empresa) nomeada na Ficha da loja da sua app no Google Play tem de aparecer na Política de Privacidade ou a app tem de ser nomeada na Política de Privacidade. As apps que não acedem a dados pessoais e confidenciais do utilizador têm, todavia, de enviar uma política de privacidade.

Certifique-se de que a política de privacidade está disponível num URL ativo, acessível ao público e sem perímetro virtual (sem PDFs) e de que não é editável.

Requisito de eliminação de contas

Se a sua app permite que os utilizadores criem uma conta na sua app, também tem de permitir que os utilizadores solicitem a eliminação da respetiva conta. Os utilizadores têm de ter uma opção facilmente detetável para iniciar a eliminação da conta da app dentro e fora da app (por exemplo, ao visitar o seu Website). Um link para este recurso Web tem de ser introduzido no campo do formulário URL designado na Play Console.

Ao apagar uma conta da app com base na solicitação de um utilizador, também tem de apagar os dados do utilizador associados à respetiva conta da app. O "bloqueio" ou a desativação temporária da conta da app não se qualifica como a eliminação da conta. Se precisar de reter determinados dados por razões legítimas, como segurança, prevenção de fraudes ou conformidade regulamentar, tem de informar os utilizadores de forma clara sobre as suas práticas de retenção de dados (por exemplo, na sua política de privacidade).

Para saber mais sobre os requisitos de políticas de eliminação de contas, consulte este artigo do Centro de Ajuda. Para obter informações adicionais sobre a atualização do seu formulário de Segurança dos dados, visite este artigo.

Utilização do ID de conjunto de apps

O Android apresentará um novo ID para suportar exemplos de utilização essenciais como estatísticas e a prevenção de fraudes. Seguem-se os Termos de Utilização deste ID.

- **Utilização**: o ID de conjunto de apps não pode ser utilizado para a personalização de anúncios nem para a medição de anúncios.
- **Associação a informações de identificação pessoal ou outros identificadores:** o ID de conjunto de apps não pode ser associado a nenhum identificador do Android (por exemplo, AAID) nem a quaisquer dados pessoais e confidenciais para fins publicitários.
- **Transparência e consentimento:** a recolha e a utilização do ID de conjunto de apps e o compromisso para com os presentes termos devem ser divulgados aos utilizadores através de uma notificação de privacidade juridicamente adequada, incluindo a sua política de privacidade. Tem de obter um consentimento legalmente válido dos utilizadores nos casos em que tal seja obrigatório. Para saber mais acerca das nossas normas de privacidade, analise a nossa Política de Dados do Utilizador .

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

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

- Cumprir todas as leis, diretivas, normas e regras aplicáveis em matéria de privacidade, segurança de dados e proteção de dados;
- Aceder, utilizar ou processar as Informações pessoais da UE apenas para fins compatíveis com a autorização obtida junto da pessoa a quem as referidas informações dizem respeito;
- Implementar medidas organizacionais e técnicas adequadas para proteger as Informações pessoais da UE contra perda, utilização indevida e acesso, divulgação, alteração e destruição não autorizada ou ilegal; e
- Assegurar o mesmo nível de proteção exigido pelos Princípios do Privacy Shield (Escudo de Proteção da Privacidade) .

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

Desde 16 de julho de 2020 que a Google não aplica o EU-U.S. Privacy Shield (Escudo de Proteção da Privacidade UE-EUA) para transferir dados pessoais provenientes do Espaço Económico Europeu ou do Reino Unido para os Estados Unidos. (Saiba mais.)Pode encontrar mais informações na secção 9 do DDA.

Autorizações e APIs com acesso a informações confidenciais

Os pedidos de autorização e APIs (interface de programação de aplicações) com acesso a informações confidenciais devem ser compreensíveis pelos utilizadores. Apenas pode solicitar as autorizações e APIs com acesso a informações confidenciais necessárias para implementar as funcionalidades ou os serviços atuais na sua app que sejam promovidos na sua ficha do Google Play. Não pode usar autorizações ou APIs com acesso a informações confidenciais que dão acesso aos dados do utilizador ou dispositivo para funcionalidades ou finalidades não divulgadas, não implementadas ou não autorizadas. Os dados pessoais ou confidenciais acedidos através de autorizações ou APIs com acesso a informações confidenciais nunca podem ser vendidos nem partilhados numa venda facilitada.

Peça autorizações e APIs com acesso a informações confidenciais para aceder aos dados em contexto (através de pedidos progressivos) de forma que os utilizadores compreendam os motivos pelos quais a sua app está a pedir a autorização. Use os dados apenas para as finalidades autorizadas pelo utilizador. Se mais tarde quiser usar os dados para outras finalidades, tem de perguntar aos utilizadores e assegurar que concordam com as utilizações adicionais.

Autorizações restritas

Para além do exposto acima, as autorizações restritas são autorizações designadas como Perigosas , Especiais , de Assinatura ou conforme documentado abaixo. Estas autorizações estão sujeitas aos seguintes requisitos e restrições adicionais:

- Os dados do utilizador ou do dispositivo acedidos através de autorizações restritas são considerados dados pessoais e confidenciais do utilizador. São aplicados os requisitos da Política de Dados do Utilizador .
- Respeite as decisões dos utilizadores caso recusem um pedido de Autorização restrita. Os utilizadores não podem ser manipulados nem forçados a consentir qualquer autorização não crítica. Tem de envidar um esforço razoável para integrar os utilizadores que não concederem acesso a autorizações confidenciais (por exemplo, permitir que um utilizador introduza um número de telefone manualmente caso tenha restringido o acesso aos registos de chamadas).
- A utilização de autorizações que violem as Políticas de Software Malicioso do Google Play (incluindo o abuso de privilégios elevados) é expressamente proibida.

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

Autorizações de SMS e de registo de chamadas

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

Autorização restrita	Requisito
Grupo de autorizações do Registo de chamadas (por exemplo, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Tem de estar ativamente registado como o controlador predefinido do Telemóvel ou do Assistente no dispositivo.

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

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

As apps apenas podem utilizar a autorização (e quaisquer dados derivados da autorização) para fornecer a funcionalidade essencial da app aprovada. A funcionalidade essencial é definida como o objetivo principal da app. Isto pode incluir um conjunto de funcionalidades essenciais, que tem de documentar e promover proeminentemente na descrição da app. Sem a funcionalidade essencial, a app é considerada "danificada" ou inutilizável. A transferência, a partilha ou a utilização licenciada destes dados apenas se podem destinar a fornecer funcionalidades ou serviços essenciais na app e a respetiva utilização não pode ser alargada a qualquer outra finalidade (por exemplo, melhorar outras apps ou serviços, publicidade ou marketing). Não pode utilizar métodos alternativos (incluindo outras autorizações, APIs ou origens de terceiros) para derivar os dados atribuídos às autorizações relacionadas com SMS ou registo de chamadas.

Autorizações de acesso à localização

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

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

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

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

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

Para mais informações acerca dos requisitos da política, consulte este artigo de ajuda .

Autorização de acesso a todos os ficheiros

Os atributos de ficheiros e diretório no dispositivo de um utilizador são considerados dados pessoais e confidenciais do utilizador sujeitos à Política de Informações Pessoais e Confidenciais e aos seguintes requisitos:

- As apps apenas devem solicitar acesso ao armazenamento do dispositivo que seja fundamental para que a app funcione e não podem solicitar acesso ao armazenamento do dispositivo em nome de terceiros para qualquer finalidade que não esteja relacionada com funcionalidades centradas no utilizador da app.
- Os dispositivos Android com a versão R ou posterior necessitam da autorização MANAGE_EXTERNAL_STORAGE para gerir o acesso no armazenamento partilhado. Todas as apps destinadas à versão R e que solicitem amplo acesso ao armazenamento partilhado ("Acesso a todos os ficheiros") têm de passar com êxito uma revisão de acesso adequada antes da publicação. As apps com autorização para utilizar esta autorização têm de solicitar claramente aos utilizadores que ativem a opção "Acesso a todos os ficheiros" para a respetiva app nas definições de "Acesso especial a apps". Para obter mais informações acerca dos requisitos da versão R, consulte este artigo de ajuda .

Autorização de visibilidade de pacotes (app)

O inventário de apps instaladas consultado a partir de um dispositivo é considerado dados pessoais e confidenciais do utilizador sujeitos à Política de Informações Pessoais e Confidenciais e aos seguintes requisitos:

As apps que têm como finalidade principal iniciar, pesquisar ou interoperar com outras apps no dispositivo podem obter visibilidade adequada ao âmbito às mesmas, conforme descrito abaixo:

- **Visibilidade ampla das apps:** a visibilidade ampla refere-se à capacidade de uma app ter uma visibilidade abrangente (ou "ampla") das apps instaladas ("pacotes") num dispositivo.
  - Para as apps que segmentam o nível da API 30 ou posterior , a visibilidade ampla das apps instaladas através da autorização QUERY_ALL_PACKAGES está restrita a exemplos de utilização específicos em que o conhecimento de todas as apps instaladas no dispositivo e/ou a interoperabilidade com as mesmas são necessários para que a app funcione.
    - Não pode utilizar QUERY_ALL_PACKAGES se a sua app funcionar com uma declaração de visibilidade de pacotes com âmbito mais segmentado (por exemplo, consultar e interagir com pacotes específicos em vez de solicitar visibilidade ampla).
  - A utilização de métodos alternativos para se aproximar do nível de visibilidade ampla associado à autorização QUERY_ALL_PACKAGES também está restrita à funcionalidade essencial da app para o utilizador e à interoperabilidade com quaisquer apps detetadas através deste método.
  - Consulte este artigo do Centro de Ajuda para obter exemplos de utilização permitidos da autorização QUERY_ALL_PACKAGES.
- **Visibilidade limitada das apps**: a visibilidade limitada acontece quando uma app minimiza o acesso aos dados ao consultar apps específicas através de métodos mais segmentados (em vez de métodos "amplos"), por exemplo, ao consultar apps específicas que satisfaçam a declaração do manifesto da sua app. Pode utilizar este método para consultar apps em casos em que a sua app tenha interoperabilidade em conformidade com as políticas ou a gestão destas apps.
- A visibilidade do inventário de apps instaladas num dispositivo tem de estar diretamente relacionada com a finalidade principal ou a funcionalidade essencial a que os utilizadores acedem na sua app.

Os dados do inventário de apps consultados a partir de apps distribuídas no Google Play nunca podem ser vendidos nem partilhados para fins de análise ou de rentabilização de anúncios.

API de acessibilidade

Não é possível utilizar a API Accessibility para:

- Alterar as definições dos utilizadores sem a respetiva autorização ou impedir a capacidade de os utilizadores desativarem ou desinstalarem qualquer app ou serviço, a menos que tenha a autorização de um dos pais ou tutor através de uma app de controlo parental ou de administradores autorizados através de um software de gestão empresarial;
- Contornar notificações e controlos de privacidade integrados no Android; ou
- Alterar ou tirar partido da interface do utilizador de uma forma enganadora ou que viole de qualquer outra forma as Políticas para Programadores do Google Play.

A API Accessibility não foi concebida e não pode ser pedida para a gravação de áudio de chamadas remotas.

A utilização da API Accessibility tem de ser documentada na ficha do Google Play.

Diretrizes para o IsAccessibilityTool

As apps cuja funcionalidade principal se destine a apoiar diretamente pessoas com deficiência são elegíveis para utilizar o **IsAccessibilityTool** de forma a classificarem-se publicamente como apps de acessibilidade.

As apps não elegíveis para utilizar o **IsAccessibilityTool** podem não utilizar a sinalização e têm de cumprir os requisitos de divulgação proeminente e consentimento, conforme descrito na Política de Dados do Utilizador , uma vez que a funcionalidade relacionada com a acessibilidade não é óbvia para o utilizador. Consulte o artigo do Centro de Ajuda sobre a API AccessibilityService para mais informações.

As apps têm de utilizar APIs e autorizações com um âmbito mais restrito em detrimento da API Accessibility para obter a funcionalidade desejada.

Autorização Solicitar pacotes de instalação

A autorização REQUEST_INSTALL_PACKAGES permite que uma aplicação peça a instalação de pacotes de apps. Para usar esta autorização, a funcionalidade essencial da sua app tem de incluir:

- O envio ou a receção de pacotes de apps; e
- A permissão de instalação de pacotes de apps por iniciativa do utilizador.

As funcionalidades permitidas incluem:

- Pesquisa ou navegação na Web
- Serviços de comunicação que suportam anexos
- Partilha, transferência ou gestão de ficheiros
- Gestão de dispositivos empresariais
- Cópia de segurança e restauro
- Migração de dispositivo/transferência de telemóvel
- Uma app associada para sincronizar o telemóvel com um dispositivo de vestir ou da IdC (Internet das Coisas), por exemplo, um smartwatch ou uma smart TV

A funcionalidade essencial é definida como o objetivo principal da app. A funcionalidade essencial, bem como outras funcionalidades principais que abrangem esta funcionalidade essencial, têm todas de estar documentadas e promovidas claramente na descrição da app.

A autorização REQUEST_INSTALL_PACKAGES não pode ser usada para realizar atualizações automáticas, modificações ou o agrupamento de outros APKs (Android Application Packages) no ficheiro do recurso, exceto para fins de gestão de dispositivos. Todas as atualizações ou as instalações de pacotes têm de estar em conformidade com a Política de Abuso na Rede e em Dispositivos do Google Play e têm de ser iniciadas e controladas pelo utilizador.

Autorizações da Health Connect by Android

A Saúde Connect é uma plataforma Android que permite que as apps de saúde e fitness armazenem e partilhem os mesmos dados no dispositivo, no âmbito de um ecossistema unificado. Oferece também um lugar único para os utilizadores controlarem as apps que podem ler e escrever dados de saúde e fitness, incluindo registos de saúde. Os registos de saúde podem incluir o histórico médico, diagnósticos, tratamentos, medicamentos, resultados laboratoriais e outros dados clínicos, obtidos junto de instituições ou prestadores de cuidados de saúde, ou através de plataformas de saúde de terceiros compatíveis.

A Saúde Connect é compatível com a leitura e a escrita de vários tipos de dados, como passos, a temperatura corporal e dados do registo de saúde.

Os dados acedidos através das autorizações da Saúde Connect são considerados dados pessoais e confidenciais do utilizador sujeitos à Política de Dados do Utilizador. Se a sua app se qualificar como uma app de saúde ou tiver funcionalidades relacionadas com a saúde e aceder a dados de saúde, incluindo os dados da Saúde Connect, também tem de estar em conformidade com a Política de Apps de Saúde.

Consulte este guia do programador Android sobre como começar a usar a Saúde Connect. Para solicitar acesso aos tipos de dados da Saúde Connect e outras Perguntas frequentes, consulte as Perguntas frequentes sobre os requisitos da política da Saúde Connect.

As apps distribuídas através do Google Play têm de cumprir os seguintes requisitos da política para ler e/ou escrever dados na Saúde Connect.

Acesso e utilização adequados da Health Connect

A Saúde Connect só pode ser usada de acordo com as políticas e os Termos de Utilização aplicáveis, e para exemplos de utilização aprovados, conforme estabelecido na presente política. Isto significa que só pode pedir acesso a autorizações quando a sua aplicação ou serviço satisfizer um dos exemplos de utilização aprovados.

Os exemplos de utilização aprovados incluem: fitness e bem-estar, recompensas, orientações de fitness, bem-estar empresarial, cuidados médicos, investigação na área da saúde e jogos. As aplicações com acesso a estes exemplos de utilização não podem alargar a respetiva utilização para fins não divulgados ou não autorizados.

Apenas as aplicações ou os serviços com uma ou mais funcionalidades concebidas para beneficiar a saúde e o fitness dos utilizadores estão autorizados a pedir acesso às autorizações da Saúde Connect. Por exemplo:

- Aplicações ou serviços que permitem que os utilizadores **registem, comuniquem, monitorizem e/ou analisem diretamente** a respetiva atividade física, sono, bem-estar mental, nutrição, medições de saúde, descrições físicas, registos de saúde e/ou outras descrições e medições relacionadas com a saúde ou o fitness.
- Aplicações ou serviços que permitem que os utilizadores **armazenem a respetiva atividade física, sono, bem-estar mental, nutrição, medições de saúde, descrições físicas**, **registos de saúde** e/ou outras descrições e medições relacionadas com saúde ou fitness no respetivo dispositivo e partilhem os respetivos dados com outras apps no dispositivo que satisfaçam estes exemplos de utilização.
- Aplicações ou serviços que permitem aos utilizadores gerir condições crónicas, tratamentos médicos ou cuidados.

O acesso à Saúde Connect não pode ser usado em violação da presente política ou de outros Termos de Utilização ou políticas aplicáveis da Saúde Connect, inclusive para as seguintes finalidades:

- Não use a Saúde Connect para o desenvolvimento de, ou a incorporação em, aplicações, ambientes ou atividades em que a utilização ou falha da Saúde Connect poderia levar à morte, a lesões pessoais, a danos a indivíduos ou a danos ambientais ou materiais (como criação ou operação de instalações nucleares, controlo de tráfego aéreo, sistemas de apoio à vida ou armamento).

- Não use apps sem interface para aceder aos dados obtidos através da Saúde Connect. As apps têm de apresentar um ícone claramente identificável no tabuleiro de apps, nas definições da app do dispositivo, nos ícones de notificação, etc.
- Não use a Saúde Connect com apps que sincronizam dados entre dispositivos ou plataformas incompatíveis.
- Não use a Saúde Connect para se ligar a aplicações, serviços ou funcionalidades destinadas unicamente a crianças.
- Tome medidas razoáveis e apropriadas para proteger todas as aplicações ou sistemas que usam a Saúde Connect contra acesso, utilização, destruição, perda, alteração ou divulgação não autorizados ou ilegais.

Também é responsável por garantir o cumprimento de quaisquer requisitos regulamentares ou legais que se possam aplicar com base na sua utilização prevista da Saúde Connect e de quaisquer dados da mesma. Por exemplo, se for uma entidade abrangida ou um associado comercial sujeito à Lei de Portabilidade e Responsabilidade dos Seguros de Saúde (HIPAA), tem de agir em conformidade com os requisitos aplicáveis ao seu acesso e utilização das informações da Saúde Connect. Se for um programador sujeito ao Regulamento Geral sobre a Proteção de Dados (RGPD) para utilizadores da UE, tem de cumprir igualmente as suas obrigações ao abrigo do RGPD. Estas leis e regulamentos podem exigir a celebração de contratos adicionais antes da partilha de dados (por exemplo, um Contrato de Parceiro Comercial ou um Contrato de Tratamento de Dados) com as entidades relevantes envolvidas nas suas atividades de tratamento. Também é da responsabilidade dos programadores de apps determinar se as respetivas atividades exigem os referidos contratos. Os programadores têm de facultar provas desse contrato ou conformidade à Google, mediante solicitação.

Exceto conforme explicitamente indicado na etiquetagem ou nas informações fornecidas pela Google relativas a produtos ou serviços Google específicos, a Google não recomenda a utilização nem garante a exatidão de quaisquer dados contidos na Saúde Connect para qualquer utilização ou propósito e, em particular, para utilizações de investigação, saúde ou médicas. A Google renuncia a qualquer responsabilidade associada à utilização de dados obtidos através da Saúde Connect.

Utilização limitada

Quando usar a Saúde Connect, o acesso e a utilização dos dados têm de respeitar limitações específicas:

- A utilização dos dados deve limitar-se a fornecer ou melhorar o seu exemplo de utilização apropriado ou as funcionalidades visíveis na interface do utilizador da aplicação.
- Os dados do utilizador só podem ser transferidos para terceiros para fins de segurança (por exemplo, para investigar abusos), para estar em conformidade com as leis ou os regulamentos aplicáveis, ou no âmbito de fusões/aquisições. A transferência requer o consentimento explícito do utilizador.
- O acesso humano aos dados do utilizador é restrito, a menos que seja obtido o consentimento explícito do utilizador, para fins de segurança, para estar em conformidade com as leis ou quando agregados para operações internas, de acordo com os requisitos legais.
- **Todas as outras transferências, utilizações ou venda de dados da Saúde Connect são proibidas, incluindo:**
  - A transferência ou venda de dados do utilizador a terceiros, como plataformas de publicidade, corretores de dados ou quaisquer revendedores de informações.
  - A transferência, venda ou utilização de dados do utilizador para publicar anúncios, incluindo publicidade personalizada ou baseada em interesses.
  - A transferência, a venda ou a utilização de dados do utilizador para determinar a solvabilidade ou para fins de empréstimo.
  - A transferência, a venda ou a utilização de dados do utilizador com qualquer produto ou serviço que possa ser qualificado como um dispositivo médico, a menos que a app de dispositivo médico cumpra todos os regulamentos aplicáveis, incluindo a obtenção das autorizações ou aprovações

necessárias dos organismos reguladores relevantes (por exemplo, a FDA dos EUA) para a utilização pretendida dos dados da Saúde Connect, e o utilizador tenha dado o seu consentimento explícito para essa utilização.
- A transferência, a venda ou a utilização de dados do utilizador para qualquer finalidade ou de qualquer forma que envolva Informações de saúde protegidas (conforme definido pela HIPAA), exceto se for iniciado pelo utilizador e em conformidade com os regulamentos da HIPAA.

Âmbito mínimo

Só deve pedir acesso às autorizações necessárias para implementar as funcionalidades ou os serviços do seu produto. Esses pedidos de acesso devem ser específicos e limitados aos dados necessários.

Controlo e aviso transparente e preciso

A Saúde Connect trata dados de saúde e fitness, o que inclui informações pessoais e confidenciais. Os programadores têm de fornecer divulgações claras e acessíveis sobre as respetivas práticas de dados através de uma Política de Privacidade abrangente. Estas divulgações têm de incluir:

- Uma representação com precisão da identidade da aplicação ou do serviço que solicita o acesso aos dados do utilizador.
- Informações claras e precisas que expliquem que tipos de dados estão a ser acedidos, solicitados e/ou recolhidos. Os dados têm de estar relacionados com uma funcionalidade ou uma recomendação orientada para o utilizador oferecida na sua app.
- Uma explicação de como é que os dados vão ser usados e/ou partilhados: se solicitar dados por um motivo, mas os dados também forem usados para uma finalidade secundária, tem de divulgar todos os exemplos de utilização aos utilizadores.
- Documentação de ajuda ao utilizador que explique como é que os utilizadores podem gerir e eliminar os respetivos dados da app e o que acontece aos dados quando uma conta é desativada e/ou eliminada.
- Informações relacionadas com o tratamento de todos os dados pessoais e confidenciais do utilizador de forma segura, incluindo a transmissão através de criptografia moderna (por exemplo, por HTTPS).

Para mais informações sobre os requisitos relativos a apps com ligação à Saúde Connect, consulte este artigo do Centro de Ajuda.

Serviço VPN

O VpnService é uma classe base para aplicações para desenvolver e criar as suas próprias soluções VPN. Apenas as apps que usam o VpnService e têm a VPN como funcionalidade essencial podem criar um túnel seguro ao nível do dispositivo para um servidor remoto. As exceções incluem apps que requerem um servidor remoto para funcionalidades essenciais, como:

- Apps de controlo parental e gestão empresarial.
- Acompanhamento da utilização da app.
- Apps de segurança de dispositivos (por exemplo, antivírus, gestão de dispositivos móveis e firewall).
- Ferramentas relacionadas com redes (por exemplo, acesso remoto).
- Apps de navegação Web.
- Apps de operador que requerem a utilização da funcionalidade de VPN para oferecer serviços de telefonia ou conetividade.

Não é possível usar o VpnService para:

- Recolher dados pessoais e confidenciais do utilizador sem consentimento e divulgação destacada.
- Redirecionar ou manipular o tráfego de utilizadores de outras apps num dispositivo para fins de rentabilização (por exemplo, redirecionar o tráfego de anúncios através de um país diferente do país do utilizador).

As apps que usam o VpnService têm de:

- Documentar a utilização do VpnService na ficha do Google Play, e
- Encriptar os dados do dispositivo para o ponto final do túnel VPN, e
- Cumprir todas as Políticas do Programa para programadores , incluindo as Políticas de Fraude de anúncios , Autorizações e Software malicioso .

Autorização de alarme exato

Vai ser introduzida uma nova autorização, USE_EXACT_ALARM, que fornece acesso à funcionalidade de alarme exato em apps a partir do Android 13 (nível 33 da API de destino).

USE_EXACT_ALARM é uma autorização restrita e as apps só têm de declarar esta autorização se a respetiva funcionalidade essencial suportar a necessidade de um alarme exato. As apps que pedem esta autorização restrita estão sujeitas a verificação e as que não cumprem os critérios do exemplo de utilização autorizado estão proibidas de serem publicadas no Google Play.

Exemplos de utilização autorizados para usar a autorização de alarme exato

A sua app tem de usar a funcionalidade USE_EXACT_ALARM apenas quando a funcionalidade essencial orientada para o utilizador da sua app requer ações precisas, tais como:

- A app é uma app de alarme ou temporizador.
- A app é uma app de calendário que mostra notificações dos eventos.

Se tiver um exemplo de utilização para a funcionalidade de alarme exato que não esteja abrangido acima, deve avaliar se o uso da funcionalidade SCHEDULE_EXACT_ALARM como alternativa é uma opção.

Para mais informações sobre a funcionalidade de alarme exato, consulte estas orientações para programadores .

Autorização de intenção de ecrã inteiro

Para as apps que segmentam o Android 14 (nível 34 da API de destino) e superior, USE_FULL_SCREEN_INTENT é uma autorização de acesso a apps especial . A utilização da autorização USE_FULL_SCREEN_INTENT só é concedida às apps automaticamente se a funcionalidade essencial da app se enquadrar numa das categorias abaixo que requerem notificações de elevada prioridade:

- Definir um alarme
- Receber chamadas ou videochamadas

As apps que pedem esta autorização estão sujeitas a revisão e esta autorização não vai ser automaticamente concedida às apps que não cumprirem os critérios acima. Nesse caso, as apps têm de pedir autorização ao utilizador para usar USE_FULL_SCREEN_INTENT.

Lembre-se de que a utilização da autorização USE_FULL_SCREEN_INTENT tem de estar em conformidade com todas as Políticas para Programadores do Google Play, incluindo as nossas Políticas de Software Indesejável para Dispositivos Móveis, Abuso na Rede e em Dispositivos e Anúncios. As notificações de intenções de ecrã inteiro não podem interferir, perturbar, danificar nem aceder ao dispositivo do utilizador de uma forma não autorizada. Além disso, as apps não devem interferir com outras apps nem com a capacidade de utilização do dispositivo.

Saiba mais sobre a autorização USE_FULL_SCREEN_INTENT no nosso Centro de Ajuda.

Abuso na rede e em dispositivos

Não são permitidas apps que interfiram, perturbem, danifiquem ou acedam de forma não autorizada ao dispositivo do utilizador, outros dispositivos ou computadores, servidores, redes, interfaces de

programação de apps (APIs) ou serviços, incluindo, entre outros, outras apps no dispositivo, qualquer serviço Google ou uma rede de operador autorizado.

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

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

As apps ou o código de terceiros (por exemplo, SDKs) com linguagens interpretadas (JavaScript, Python, Lua, etc.) carregadas no tempo de execução (por exemplo, não fornecidas com a app) não podem permitir potenciais violações das Políticas do Google Play.

Não é permitido código que introduza ou explore vulnerabilidades de segurança. Consulte o Programa de melhoria de segurança de apps para obter mais informações acerca dos problemas de segurança mais recentes sinalizados aos programadores.

Seguem-se alguns exemplos de violações comuns:

Exemplos de violações comuns de abuso na rede e em dispositivos:

- Apps que bloqueiam ou interferem com outra app ao apresentar anúncios.
- Apps de batota em jogos que afetam a jogabilidade de outras apps.
- Apps que facilitam ou fornecem instruções sobre como piratear serviços, software ou hardware, ou contornar proteções de segurança.
- Apps que acedem ou usam um serviço ou uma API de uma forma que viola os respetivos termos de utilização.
- Apps que não são elegíveis para adicionar à lista de autorizações e tentam ignorar a gestão de energia do sistema .
- As apps que facilitam serviços de proxy a terceiros só podem fazê-lo em apps em que seja essa a finalidade principal, centrada no utilizador, da app.
- Apps ou código de terceiros (por exemplo, SDKs) que transferem código executável, como ficheiros dex ou código nativo, proveniente de outras fontes que não o Google Play.
- Apps que instalam outras apps num dispositivo sem o consentimento prévio do utilizador.
- Apps que estabelecem ligação ou facilitam a distribuição ou a instalação de software malicioso.
- Apps ou o código de terceiros (por exemplo, SDKs) que incluam um WebView com interface de JavaScript adicionada que carrega conteúdo Web não fidedigno (por exemplo, um URL http://) ou URLs não validados obtidos de fontes não fidedignas (por exemplo, URLs obtidos de intenções não fidedignas).
- Apps que usam a autorização de intenção de ecrã inteiro para forçar a interação do utilizador com notificações ou anúncios perturbadores.

Utilização de serviços em primeiro plano

A autorização do serviço em primeiro plano garante a utilização adequada dos serviços em primeiro plano orientados para o utilizador. Para apps que segmentem o Android 14 e superior, tem de especificar um tipo de serviço em primeiro plano válido para cada serviço em primeiro plano usado na sua app e declarar a autorização de serviço em primeiro plano adequada para esse tipo. Por exemplo, se o exemplo de utilização da sua app requer a geolocalização do mapa, tem de declarar a autorização FOREGROUND_SERVICE_LOCATION no manifesto da app.

As apps só podem declarar uma autorização de serviço em primeiro plano se a utilização:

- Oferecer uma funcionalidade benéfica para o utilizador e relevante para a funcionalidade essencial da app
- For iniciada pelo utilizador ou for percetível pelo utilizador (por exemplo, áudio da reprodução de uma música, transmissão de conteúdo multimédia para outro dispositivo, notificação do utilizador clara e precisa ou pedido do utilizador para carregar uma foto para a nuvem)
- Puder ser terminada ou parada pelo utilizador
- Não puder ser interrompida nem diferida pelo sistema sem provocar uma experiência do utilizador negativa ou fazer com que a funcionalidade antecipada pelo utilizador não funcione como esperado (por exemplo, uma chamada telefónica tem de ser iniciada imediatamente e não pode ser diferida pelo sistema)
- Só funcionar durante o tempo necessário para concluir a tarefa

Os seguintes exemplos de utilização de serviços em primeiro plano estão isentos dos critérios acima:

- Serviços em primeiro plano dos tipos systemExempted ou shortService ;
- Serviço em primeiro plano do tipo dataSync apenas aquando da utilização das funcionalidades da Play Asset Delivery

A utilização do serviço em primeiro plano é explicada de modo mais pormenorizado aqui.

Tarefas de transferência de dados iniciadas pelo utilizador

As apps só podem usar a API User-Initiated Data Transfer Jobs se a utilização:

- For iniciada pelo utilizador
- Se destinar a tarefas de transferência de dados por rede
- Só funcionar durante o tempo necessário para concluir a transferência de dados

A utilização de APIs User-Initiated Data Transfer é explicada de modo mais pormenorizado aqui.

Requisitos Flag Secure

FLAG_SECURE é uma flag de ecrã declarada no código de uma app para indicar que a respetiva IU (interface do utilizador) contém dados confidenciais que se destinam a ser limitados a uma superfície segura durante a utilização da app. Esta flag foi concebida para evitar que os dados apareçam em capturas de ecrã ou sejam vistos em ecrãs não seguros. Os programadores declaram esta flag quando o conteúdo da app não deve ser transmitido, visto nem transmitido fora da app ou do dispositivo dos utilizadores.

Por questões de segurança e privacidade, todas as apps distribuídas no Google Play são obrigadas a respeitar a declaração FLAG_SECURE de outras apps. Ou seja, as apps não podem facilitar nem criar soluções para ignorar as definições FLAG_SECURE noutras apps.

As apps que se qualificam como uma ferramenta de acessibilidade estão isentas deste requisito, desde que não transmitam, guardem nem coloquem em cache conteúdos protegidos pela flag FLAG_SECURE para acesso fora do dispositivo do utilizador.

Apps que executam contentores Android no dispositivo

As apps num contentor Android no dispositivo fornecem ambientes que simulam a totalidade ou partes de um SO Android subjacente. A experiência nestes ambientes pode não refletir o conjunto completo de funcionalidades de segurança do Android e, por isso, os programadores podem optar por adicionar uma flag do manifesto do ambiente segura para comunicar aos contentores Android no dispositivo que não podem operar no respetivo ambiente do Android simulado.

Flag do manifesto do ambiente segura

REQUIRE_SECURE_ENV é uma flag que pode ser declarada no manifesto de uma app para indicar que esta app não pode ser executada em apps num contentor Android no dispositivo. Por questões de

segurança e privacidade, as apps que fornecem contentores Android no dispositivo têm de respeitar todas as apps que declaram esta flag e:

- Rever os manifestos das apps que querem carregar no respetivo contentor Android no dispositivo para esta flag.
- Não carregar as apps que declararam esta flag no respetivo contentor Android no dispositivo.
- Não funcionar como um proxy ao intercetar ou chamar APIs no dispositivo para parecerem estar instaladas no contentor.
- Não facilitar nem criar soluções para contornar a flag (como carregar uma versão mais antiga de uma app para contornar a flag REQUIRE_SECURE_ENV da app atual).

Saiba mais acerca desta política no nosso Centro de Ajuda.

Comportamento enganador

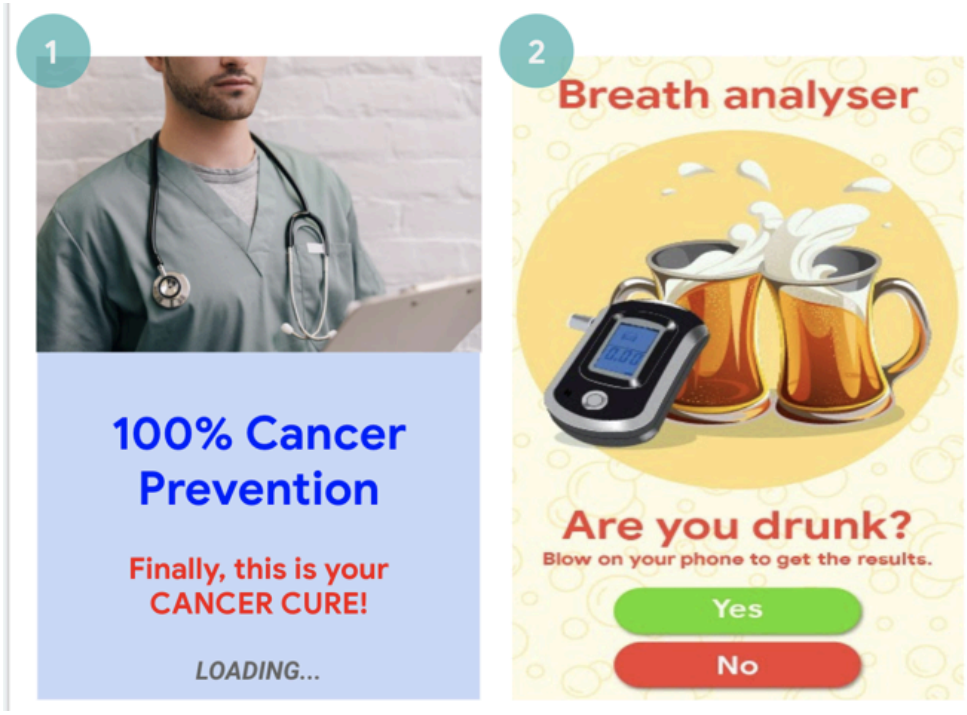
Não permitimos apps que tentem enganar os utilizadores ou permitam comportamentos desonestos, incluindo, entre outras, apps consideradas funcionalmente impossíveis. As apps devem fornecer uma divulgação, uma descrição e imagens/vídeos precisos da respetiva funcionalidade em todas as partes dos metadados.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

Declarações enganadoras

Não permitimos apps que incluam reivindicações ou informações falsas ou que induzam em erro, incluindo na descrição, no título, no ícone e nas capturas de ecrã.

Seguem-se alguns exemplos de violações comuns:

- Apps que deturpam ou não descrevem com precisão e claramente as respetivas funcionalidades:
  - Uma app que reivindica ser um jogo de corridas na descrição e nas capturas de ecrã, mas que, na realidade, é um puzzle em blocos com a imagem de um carro.
  - Uma app que reivindica ser uma app de antivírus, mas que contém apenas um guia de texto a explicar como remover vírus.
- Apps que reivindicam funcionalidades que não é possível implementar, como apps repelentes de insetos, mesmo que sejam representadas como uma partida, uma falsidade, uma anedota, etc.
- Apps categorizadas incorretamente, incluindo, entre outras, a classificação ou a categoria da app.
- Conteúdo comprovadamente enganador ou falso que pode interferir com os processos de voto ou sobre resultados de eleições.
- Apps que falsamente reivindicam uma afiliação a uma entidade governamental ou que oferecem ou facilitam serviços governamentais para os quais não estão devidamente autorizadas.
- Apps que reivindicam falsamente ser a app oficial de uma entidade estabelecida. Títulos como "Justin Bieber Oficial" não são permitidos sem as autorizações ou os direitos necessários.



(1) Esta app apresenta declarações médicas ou relacionadas com a saúde (Cure o cancro) que são enganadoras.
(2) Estas apps apresentam declarações sobre funcionalidades que não é possível implementar (usar o telemóvel como um alcoolímetro).

Alterações enganadoras de definições do dispositivo

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

Adicionalmente, não são permitidas:

- Apps que modifiquem as definições ou as funcionalidades do dispositivo com autorização do utilizador, mas que o façam de forma que não seja facilmente reversível.
- Apps ou anúncios que modifiquem as definições ou as funcionalidades do dispositivo como um serviço para terceiros ou fins publicitários.
- Apps que enganam os utilizadores para que removam ou desativem apps de terceiros, ou para que modifiquem as definições ou as funcionalidades do dispositivo.
- Apps que incentivam os utilizadores a remover ou desativar apps de terceiros, ou modifiquem definições ou funcionalidades, exceto se tal fizer parte de um serviço de segurança verificável.

Permissão de comportamentos desonestos

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

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

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

Seguem-se alguns exemplos de violações comuns:

- Apps que imitam outras apps ou Websites para enganar os utilizadores ao levá-los a divulgar informações pessoais ou de autenticação.
- Apps que contêm ou apresentam números de telefone, contactos, endereços ou informações de identificação pessoal reais ou não validados de pessoas ou entidades sem consentimento das mesmas.
- Apps com funcionalidades essenciais diferentes com base na geografia de um utilizador, em parâmetros do dispositivo ou noutros dados dependentes do utilizador nas quais essas diferenças não sejam anunciadas de forma proeminente ao utilizador na Ficha da loja.
- Apps que mudam significativamente entre versões sem alertar o utilizador (por exemplo, secção "novidades") nem atualizar a Ficha da loja.
- Apps que tentam modificar ou ocultar o comportamento durante a revisão.
- Apps com transferências facilitadas por uma rede de fornecimento de conteúdo (RFC), que não avisam o utilizador nem divulgam o tamanho da transferência antes da mesma.

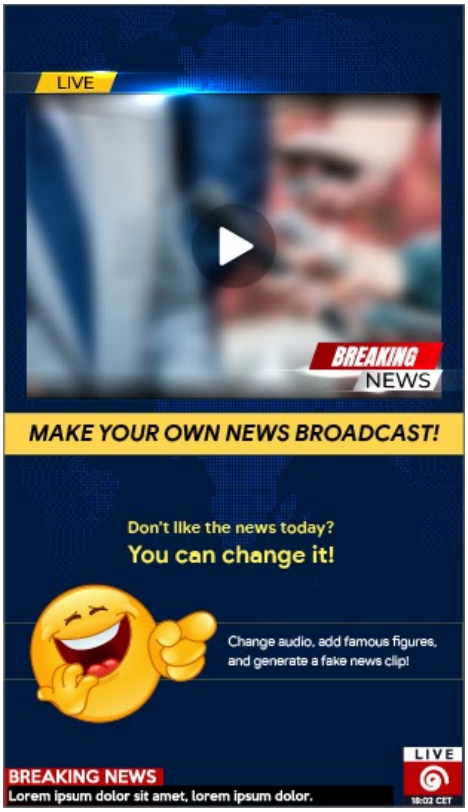
Conteúdos multimédia manipulados

Não permitimos apps que promovam ou ajudem a criar reivindicações ou informações falsas ou enganadoras através de imagens, áudio, vídeos e/ou texto. Não permitimos apps que pretendam promover ou perpetuar imagens, vídeos e/ou texto comprovadamente enganadores, que possam causar danos relacionados com um evento sensível, política, questão social ou outro assunto de interesse público.

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

Seguem-se alguns exemplos de violações comuns:

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



(1) Esta app disponibiliza funcionalidades para alterar clipes de conteúdos multimédia de forma a imitar uma transmissão de notícias e adicionar figuras públicas ou famosas ao clipe sem uma marca de água.

Transparência do comportamento

A funcionalidade da sua app tem de ser, tanto quanto possível, clara para os utilizadores. Não inclua eventuais funcionalidades ocultas, inativas ou não documentadas na app. As técnicas para evitar as críticas à app não são permitidas. As apps podem ter de facultar detalhes adicionais para garantir a segurança dos utilizadores, a integridade do sistema e a conformidade com as políticas.

Representação fraudulenta

Não são permitidas apps ou contas de programador que:

- Roubem a identidade de qualquer pessoa ou entidade, que representem de forma fraudulenta ou ocultem a respetiva propriedade ou objetivo principal.
- Participem em atividades coordenadas para enganar os utilizadores. Aqui incluem-se, entre outros, apps ou contas de programador que representem de forma fraudulenta ou ocultem o país de origem e que direcionem conteúdos para utilizadores noutro país.
- Coordenem com outros sites, apps, programadores ou contas para ocultar ou representar de forma fraudulenta a identidade do programador ou da app ou outros detalhes relevantes, quando o conteúdo da app estiver relacionado com política, questões sociais ou questões de interesse público.

Política do Nível da API de Destino do Google Play

Para proporcionar aos utilizadores uma experiência segura e protegida, o Google Play requer os seguintes níveis da API de destino para **todas as apps**:

As novas apps e atualizações de apps TÊM DE segmentar um nível da API do Android dentro do período de um ano após o lançamento da versão do Android principal mais recente. As novas apps e

atualizações de apps que não cumpram este requisito não vão poder ser enviadas na Play Console.

As apps do Google Play existentes que não estejam atualizadas e que não segmentem um nível da API no período de dois anos após o lançamento da versão do Android principal mais recente não vão estar disponíveis para novos utilizadores cujos dispositivos executem a versão mais recente do SO Android. Os utilizadores que tenham instalado anteriormente a app a partir do Google Play vão continuar a poder descobrir, reinstalar e utilizar a app em qualquer versão do SO Android que a app suporta.

Para aconselhamento técnico sobre como cumprir o requisito do nível da API de destino, consulte o guia de migração .

Para obter as linhas cronológicas exatas e as exceções, consulte este artigo do Centro de Ajuda .

SDK Requirements

Frequentemente, os programadores de apps dependem de código de terceiros (por exemplo, um SDK) para integrar as principais funcionalidades e serviços nas respetivas apps. Quando incluir um SDK na sua app, certifique-se de que consegue manter a segurança dos utilizadores e proteger a app de quaisquer vulnerabilidades. Nesta secção, demonstramos como alguns dos seus requisitos de segurança e privacidade existentes se aplicam no contexto de SDKs e são concebidos para ajudar os programadores a integrar os SDKs nas respetivas apps em segurança.

Se incluir um SDK na sua app, é responsável por garantir que o respetivo código e práticas de terceiros não fazem com que a sua app viole as Políticas do Programa para Programadores do Google Play. É importante estar ciente de como os SDKs na sua app processam os dados do utilizador e garantir que sabe que autorizações usam, que dados recolhem e porquê. Não se esqueça de que a recolha e o processamento dos dados do utilizador por parte de um SDK têm de estar em linha com a utilização dos referidos dados em conformidade com a política da app.

Para ajudar a garantir que a sua utilização de um SDK não viola os requisitos da política, leia e compreenda as seguintes políticas na íntegra e tenha em consideração alguns dos respetivos requisitos referentes aos SDKs abaixo:

Política de Dados do Utilizador

Tem de ser transparente no modo como processa os dados do utilizador (por exemplo, as informações recolhidas sobre ou de um utilizador, incluindo as informações do dispositivo). Isso significa divulgar o acesso, recolher, usar, processar e partilhar dados do utilizador a partir da sua app e limitar a utilização dos dados às finalidades divulgadas em conformidade com a política.

Se incluir código de terceiros (por exemplo, um SDK) na sua app, tem de assegurar que o código usado na app e as práticas de terceiros referentes aos dados do utilizador a partir da sua app estão em conformidade com as Políticas do Programa para Programadores do Google Play, as quais incluem requisitos de divulgação e utilização. Por exemplo, tem de assegurar que os fornecedores do SDK não vendem dados pessoais e confidenciais do utilizador a partir da sua app. Este requisito aplica-se independentemente de os dados do utilizadores serem transferidos depois de serem enviados para um servidor ou ao incorporar código de terceiros na sua app.

Dados do utilizador pessoais e confidenciais

- Limitar o acesso, a recolha, a utilização e a partilha de dados pessoais e confidenciais do utilizador adquiridos através da app para a funcionalidade da app e do serviço, bem como para as finalidades em conformidade com a política esperadas de forma razoável pelo utilizador:
  - As apps que expandem a utilização de dados pessoais e confidenciais do utilizador para publicação de anúncios têm de estar em conformidade com a Política de Anúncios do Google Play.
- Processar todos os dados pessoais e confidenciais do utilizador de forma segura, incluindo a transmissão através de criptografia moderna (por exemplo, por HTTPS).

- Usar um pedido de autorizações de tempo de execução sempre que estiver disponível, antes de aceder a dados bloqueados por autorizações do Android.

Venda de dados pessoais e confidenciais do utilizador

A venda de dados pessoais e confidenciais do utilizador não é permitida.

- "Venda" significa a troca ou a transferência de dados pessoais e confidenciais do utilizador para terceiros para consideração monetária.
  - Uma transferência de dados pessoais e confidenciais do utilizador iniciada pelo utilizador (por exemplo, quando o utilizador está a usar uma funcionalidade da app para transferir um ficheiro para terceiros ou quando o utilizador opta por usar uma app de estudo de investigação para uma finalidade dedicada) não é considerada venda.

Requisitos de divulgação destacada e consentimento

Em casos em que o acesso, a recolha, a utilização ou a partilha de dados pessoais e confidenciais do utilizador da app possam não estar dentro da expetativa razoável do utilizador do produto ou da funcionalidade em questão, tem de cumprir os requisitos de divulgação destacada e consentimento da Política de Dados do Utilizador.

Se a sua app integrar código de terceiros (por exemplo, um SDK) concebido para recolher dados pessoais e confidenciais do utilizador por predefinição, tem de, num prazo de duas semanas após a receção de um pedido do Google Play (ou, se o pedido do Google Play tiver um período mais longo, dentro desse período), fornecer provas suficientes que demonstrem que a sua app cumpre os requisitos de divulgação destacada e consentimento desta política, incluindo o acesso, a recolha, a utilização ou a partilha de dados através do código de terceiros.

Não se esqueça de garantir que a sua utilização do código de terceiros (por exemplo, um SDK) não faz com que a sua app viole a Política de Dados do Utilizador.

Consulte este artigo do Centro de Ajuda para obter mais informações sobre o requisito de divulgação destacada e consentimento.

Exemplos de violações causadas por SDKs

- Uma app com um SDK que recolha dados pessoais e confidenciais do utilizador, e não trate destes dados em conformidade com esta Política de Dados do Utilizador e os requisitos de divulgação destacada e consentimento, acesso e processamento de dados (incluindo venda não permitida).
- Uma app integra um SDK que recolhe dados pessoais e confidenciais do utilizador por predefinição em violação dos requisitos desta política relativamente à divulgação destacada e ao consentimento do utilizador.
- Uma app com um SDK que alega a recolha de dados pessoais e confidenciais do utilizador apenas para oferecer funcionalidades antifraude e antiabuso para a app, mas o SDK também partilha os dados que recolhe com terceiros para fins de publicidade ou estatísticas.
- Uma app inclui um SDK que transmite informações dos pacotes instalados pelos utilizadores que não cumprem as diretrizes da divulgação destacada e/ou as diretrizes da Política de Privacidade.
  - Consulte também a Política de Software Indesejável para Dispositivos Móveis.

Requisitos adicionais para o acesso a dados pessoais e confidenciais

A tabela abaixo descreve os requisitos para atividades específicas.

Atividade	Requisito
A sua app recolhe ou associa identificadores de dispositivos permanentes (por exemplo, IMEI, IMSI, número de série do SIM, etc.)	Os identificadores de dispositivos permanentes não podem estar associados a outros dados pessoais e confidenciais do utilizador nem a identificadores de dispositivos reajustáveis, exceto para finalidades de: • Telefonia associadas à identidade do SIM (por exemplo, chamadas Wi-Fi associadas à conta do operador); e • Apps de gestão de dispositivos empresariais que utilizem o modo de proprietário do dispositivo. Estas utilizações têm de ser divulgadas de forma proeminente aos utilizadores, conforme especificado na Política de Dados do Utilizador. Consulte este recurso para obter identificadores únicos alternativos.

	Leia a Política de Anúncios para obter diretrizes adicionais relativas ao ID de publicidade Android.
A sua app segmenta crianças	A sua app só pode incluir SDKs que tenham autocertificação para utilização em serviços dirigidos a crianças. Consulte o Programa de SDKs de anúncios autocertificados para famílias para obter os requisitos e a linguagem da política completa.

Exemplos de violações causadas por SDKs

- Uma app que use um SDK que associa a Localização e o ID Android
- Uma app com um SDK que associa o AAID (ID de publicidade Android) a identificadores de dispositivos persistentes para fins de publicidade ou estatísticas.
- Uma app que usa um SDK que associa o AAID e o endereço de email para fins de estatísticas.

Secção segurança dos dados

Todos os programadores têm de elaborar uma Secção segurança dos dados clara e precisa para cada app que detalhe a recolha, a utilização e a partilha dos dados do utilizador. Isto inclui dados recolhidos e processados através de quaisquer bibliotecas ou SDKs de terceiros usados nas respetivas apps. O programador é responsável pela exatidão da etiqueta e por manter estas informações atualizadas. Quando tal for relevante, a secção tem de ser consistente com as divulgações na política de privacidade da app.

Consulte este artigo do Centro de Ajuda para obter informações adicionais sobre como elaborar a Secção segurança dos dados.

Consulte a Política de Dados do Utilizador completa.

Política de Autorizações e APIs com Acesso a Informações Confidenciais

Os pedidos de autorização e APIs com acesso a informações confidenciais devem ser compreensíveis pelos utilizadores. Só pode pedir as autorizações e APIs com acesso a informações confidenciais necessárias para implementar as funcionalidades ou os serviços atuais na sua app que sejam promovidos na sua ficha do Google Play. Não pode usar autorizações ou APIs com acesso a informações confidenciais que dão acesso aos dados do utilizador ou dispositivo para funcionalidades ou finalidades não divulgadas, não implementadas ou não autorizadas. Os dados pessoais ou confidenciais acedidos através de autorizações ou APIs com acesso a informações confidenciais nunca podem ser vendidos nem partilhados numa venda facilitada.

Consulte a Política de Autorizações e APIs com Acesso a Informações Confidenciais completa.

Exemplos de violações causadas por SDKs

- A sua app inclui um SDK que pede a localização em segundo plano para fins não permitidos ou não divulgados.
- A sua app inclui um SDK que transmite o IMEI (International Mobile Equipment Identity) derivado da autorização do Android read_phone_state sem o consentimento do utilizador.

Política de Software Malicioso

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

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

Os requisitos desta política também se aplicam a código de terceiros (por exemplo, um SDK) que inclua na sua app.

Consulte a Política de Software Malicioso completa.

Exemplos de violações causadas por SDKs

- Uma app que inclui bibliotecas de SDKs de fornecedores que distribuem software malicioso.
- Uma app que viola o modelo de autorizações do Android ou rouba credenciais (tais como tokens OAuth) de outras apps.
- Apps que abusam das funcionalidades para impedir a respetiva desinstalação ou paragem.
- Uma app que desativa o SELinux.
- Uma app inclui um SDK que viola o modelo de autorizações do Android ao conseguir privilégios elevados através do acesso a dados do dispositivo para uma finalidade não divulgada.
- Uma app inclui um SDK com código que engana os utilizadores ao levá-los a subscrever ou comprar conteúdo através da respetiva fatura da operadora móvel.

Utilização de SDKs em apps

Se incluir um SDK na sua app, é responsável por garantir que o respetivo código e práticas de terceiros não fazem com que a sua app viole as Políticas do Programa para Programadores do Google Play. É importante estar ciente de como os SDKs na sua app tratam os dados do utilizador e garantir que sabe que autorizações usam, que dados recolhem e porquê.

SDK Requirements

Frequentemente, os programadores de apps dependem de código de terceiros (por exemplo, um SDK) para integrar as principais funcionalidades e serviços nas respetivas apps. Quando incluir um SDK na sua app, certifique-se de que consegue manter a segurança dos utilizadores e proteger a app de quaisquer vulnerabilidades. Nesta secção, demonstramos como alguns dos seus requisitos de segurança e privacidade existentes se aplicam no contexto de SDKs e são concebidos para ajudar os programadores a integrar os SDKs nas respetivas apps em segurança.

Se incluir um SDK na sua app, é responsável por garantir que o respetivo código e práticas de terceiros não fazem com que a sua app viole as Políticas do Programa para Programadores do Google Play. É importante estar ciente de como os SDKs na sua app processam os dados do utilizador e garantir que sabe que autorizações usam, que dados recolhem e porquê. Não se esqueça de que a recolha e o processamento dos dados do utilizador por parte de um SDK têm de estar em linha com a utilização dos referidos dados em conformidade com a política da app.

Para ajudar a garantir que a sua utilização de um SDK não viola os requisitos da política, leia e compreenda as seguintes políticas na íntegra e tenha em consideração alguns dos respetivos requisitos referentes aos SDKs abaixo:

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

Spyware

O spyware é uma aplicação, um código ou um comportamento malicioso que recolhe, exfiltra ou partilha dados do utilizador ou do dispositivo que não estão relacionados com a funcionalidade compatível com a política.

O código ou o comportamento malicioso que possa ser considerado espionagem sobre o utilizador ou exfiltre dados sem um aviso ou um consentimento adequado também é considerado spyware.

Veja a Política de Spyware completa.

Por exemplo, as violações de spyware causadas por um SDK incluem, entre outras:

- Uma app que usa um SDK que transmite dados de áudio ou gravações de chamadas quando não está relacionado com a funcionalidade da app em conformidade com a política.
- Uma app com código malicioso de terceiros (por exemplo, um SDK) que transmite dados para fora do dispositivo de uma forma inesperada para o utilizador e/ou sem um aviso nem um consentimento adequado.

Política de Software Indesejável para Dispositivos Móveis

Comportamento transparente e divulgações claras

Todo o código deve cumprir as promessas feitas ao utilizador. As apps devem fornecer todas as funcionalidades comunicadas. As apps não devem confundir os utilizadores.

Exemplos de violações:

- Fraude ao nível da publicidade
- Engenharia social

Proteja os dados do utilizador

Divulgue de forma clara e transparente o acesso, a utilização, a recolha e a partilha de dados pessoais e confidenciais do utilizador. A aplicação dos dados do utilizador tem de cumprir todas as Políticas de Dados do Utilizador relevantes, sempre que aplicável, e tomar todas as precauções para proteger os dados.

Exemplos de violações:

- Recolha de dados (cf. spyware)
- Abuso de autorizações restritas

Consulte a Política de Software Indesejável para Dispositivos Móveis completa

Política de Abuso na Rede e em Dispositivos

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

As apps ou o código de terceiros (por exemplo, SDKs) com idiomas interpretados (JavaScript, Python, Lua, etc.) carregadas no tempo de execução (por exemplo, não fornecidas com a app) não podem permitir potenciais violações das Políticas do Google Play.

Não é permitido código que introduza ou explore vulnerabilidades de segurança. Consulte o Programa de melhoria de segurança de apps para obter mais informações acerca dos problemas de segurança mais recentes denunciados aos programadores.

Consulte a Política de Abuso na Rede e em Dispositivos completa.

Exemplos de violações causadas por SDKs

- As apps que facilitam serviços de proxy a terceiros só podem fazê-lo em apps em que seja essa a finalidade principal, orientada para o utilizador, da app.
- A sua app inclui um SDK que transfere código executável, como ficheiros dex ou código nativo, de uma fonte que não é o Google Play.
- A sua app inclui um SDK com um WebView com interface de JavaScript adicionada que carrega conteúdo da Web não fidedigno (por exemplo, um URL http://) ou URLs não validados obtidos de fontes não fidedignas (por exemplo, URLs obtidos com intenções não fidedignas).
- A sua app inclui um SDK que contém código utilizado para atualizar o respetivo APK.

- A sua app inclui um SDK que expõe os utilizadores a uma vulnerabilidade de segurança ao transferir ficheiros através de uma ligação insegura.
- A sua app está a utilizar um SDK que contém código para transferir ou instalar aplicações de fontes desconhecidas fora do Google Play.
- A sua app inclui um SDK que utiliza serviços em primeiro plano sem um exemplo de utilização adequado.
- A sua app inclui um SDK que utiliza serviços em primeiro plano por um motivo em conformidade com a política, mas que não está declarado no manifesto da app.

Política de Comportamento Enganador

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

Consulte a Política de Comportamento Enganador completa.

Transparência do comportamento

A funcionalidade da sua app tem de ser, tanto quanto possível, clara para os utilizadores. Não inclua eventuais funcionalidades ocultas, inativas ou não documentadas na app. As técnicas para evitar as críticas à app não são permitidas. As apps podem ter de facultar detalhes adicionais para garantir a segurança dos utilizadores, a integridade do sistema e a conformidade com as políticas.

Exemplo de uma violação causada por um SDK

- A sua app inclui um SDK que utiliza técnicas para evitar críticas à app.

Que Políticas para Programadores do Google Play estão normalmente associadas a violações causadas por SDKs?

Para ajudar a garantir que qualquer código de terceiros usado pela sua app está em conformidade com as Políticas do Programa para Programadores do Google Play, consulte as seguintes políticas na íntegra.

- Política de Dados do Utilizador
- Autorizações e APIs com acesso a informações confidenciais
- Política de Abuso na Rede e em Dispositivos
- Software malicioso
- Software indesejável para dispositivos móveis
- Programa de SDKs de anúncios autocertificados para famílias
- Política de Anúncios
- Comportamento enganador
- Políticas do Programa para Programadores do Google Play

Embora estas políticas estejam em causa mais frequentemente, é importante ter em consideração que um mau código de SDK pode fazer com que a sua app viole uma política diferente da mencionada acima. Não se esqueça de rever e estar a par de todas as políticas na íntegra, uma vez que é da sua responsabilidade, enquanto programador de apps, garantir que os seus SDKs processam os dados de apps em conformidade com a política.

Para saber mais, visite o nosso Centro de Ajuda.

Software malicioso

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

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

Os requisitos desta política também se aplicam a código de terceiros (por exemplo, um SDK) que inclua na sua app.

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

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

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

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

Visite o Google Play Protect para obter mais informações.

Backdoors

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

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

Fraude por faturação

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

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

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

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

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

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

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

Stalkerware

Código que recolhe dados do utilizador pessoais ou confidenciais de um dispositivo e transmite os dados a terceiros (empresa ou outro indivíduo) para fins de monitorização.

As apps têm de fornecer uma divulgação destacada adequada e obter o consentimento, conforme exigido pela Política de Dados do Utilizador .

Diretrizes para aplicações de monitorização

As apps concebidas e comercializadas exclusivamente para monitorizar outro indivíduo, por exemplo, para a monitorização parental das crianças ou a gestão empresarial para monitorizar funcionários individuais são as únicas apps de monitorização aceitáveis, desde que cumpram totalmente os requisitos descritos abaixo. Estas apps não podem ser usadas para monitorizar outra pessoa (um cônjuge, por exemplo) mesmo com o respetivo conhecimento e autorização, independentemente de ser apresentada uma notificação persistente. Estas apps têm de usar a flag de metadados IsMonitoringTool no respetivo ficheiro de manifesto para se designarem apropriadamente como apps de monitorização.

As apps de monitorização têm de cumprir os seguintes requisitos:

- As apps não se podem apresentar como uma solução de espionagem ou vigilância secreta.
- As apps não podem ocultar nem utilizar o "cloaking" de comportamentos de monitorização nem tentar enganar os utilizadores quanto a esta funcionalidade.
- As apps têm sempre de apresentar aos utilizadores uma notificação persistente quando estão a ser executadas e um ícone exclusivo que as identifique claramente.

- As apps têm de divulgar a funcionalidade de monitorização ou acompanhamento na descrição da Google Play Store.
- As apps e as fichas das apps no Google Play não podem fornecer meios para ativar ou aceder a funcionalidades que violem estes termos, nomeadamente a ligação a um APK não conforme que esteja alojado fora do Google Play.
- As apps têm de estar em conformidade com todas as leis aplicáveis. O programador é o único responsável por determinar a legalidade da sua app no local segmentado.

Consulte o artigo Utilização da flag isMonitoringTool do Centro de Ajuda para obter mais informações.

Negação de serviço (DoS)

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

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

Gestores de transferências hostis

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

O código pode ser um gestor de transferências hostil se:

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

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

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

Ameaça que não afeta o Android

Código que contém ameaças que não afetam o Android.

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

Phishing

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

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

Abuso de privilégios elevados

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

Os exemplos incluem:

- Uma app que viola o modelo de autorizações do Android ou rouba credenciais (tais como símbolos OAuth) de outras apps.

- Apps que abusam das funcionalidades para impedir a respetiva desinstalação ou paragem.
- Uma app que desativa o SELinux.

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

Ransomware

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

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

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

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

Acesso máximo

Código com acesso máximo ao dispositivo.

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

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

Spam

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

Spyware

O spyware é uma aplicação, um código ou um comportamento malicioso que recolhe, exfiltra ou partilha dados do utilizador ou do dispositivo que não estão relacionados com a funcionalidade compatível com a política.

O código ou o comportamento malicioso que possa ser considerado espionagem sobre o utilizador ou exfiltre dados sem um aviso ou um consentimento adequado também é considerado spyware.

Os exemplos de violações de spyware incluem, entre outros:

- A gravação de áudio ou de chamadas feitas para o telemóvel
- O roubo de dados de apps
- Uma app com código malicioso de terceiros (por exemplo, um SDK) que transmite dados para fora do dispositivo de uma forma inesperada para o utilizador e/ou sem um aviso ou um consentimento adequado.

Todas as apps têm de estar em conformidade com todas as Políticas do Programa para Programadores do Google Play, incluindo políticas de dados do dispositivo e do utilizador, nomeadamente software indesejável para dispositivos móveis, dados do utilizador, autorizações e APIs com acesso a informações confidenciais e requisitos de SDKs.

Cavalo de Troia

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

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

Nota sobre apps invulgares

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

Nota sobre a categoria Backdoor

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

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

Maskware

Uma aplicação que usa uma variedade de técnicas de evasão para servir ao utilizador uma funcionalidade diferente, ou falsa, da aplicação. Estas apps fazem-se passar por aplicações ou jogos legítimos para parecerem inócuas às lojas de apps e usam técnicas como a ocultação, o carregamento dinâmico de código ou o cloaking para revelar conteúdo malicioso.

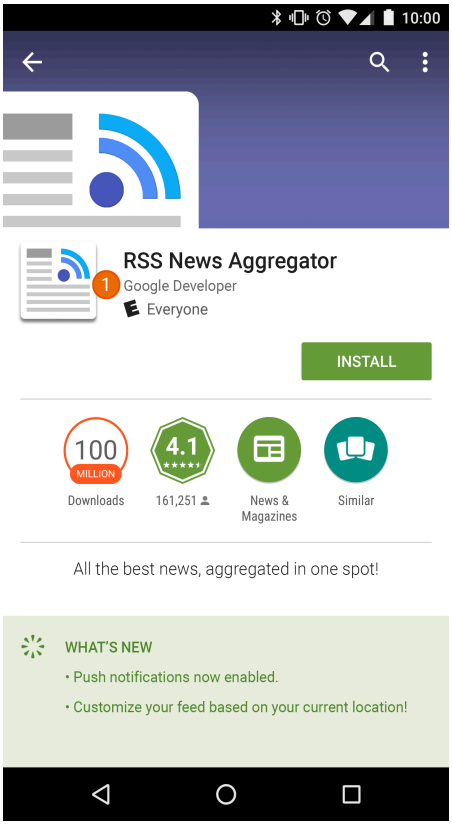
O maskware é semelhante a outras categorias de PHA, especificamente os cavalos de troia, sendo que as técnicas usadas para ocultar a atividade maliciosa são a principal diferença.

Roubo de identidade

Não são permitidas apps que enganem os utilizadores ao fazerem-se passar por outra pessoa (por exemplo, outro programador, empresa, entidade) ou outra app. Não insinue que a sua app está relacionada ou autorizada por alguém que não tem qualquer relação com a mesma ou não a autorizou. Tenha cuidado para não utilizar ícones de apps, descrições, títulos ou elementos na app que possam induzir os utilizadores em erro quanto à relação da sua app com outra pessoa ou app.

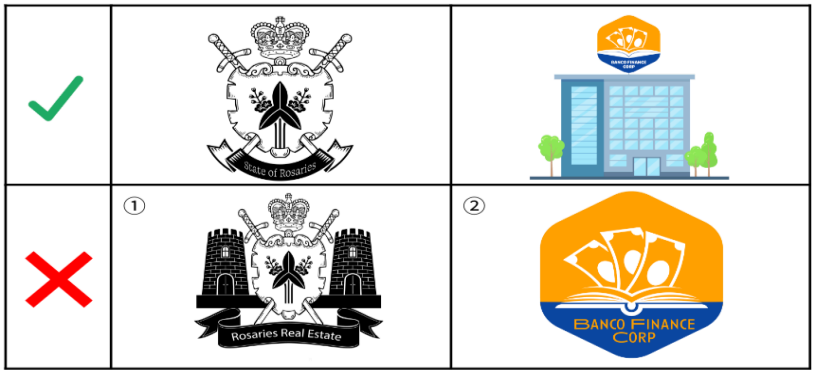
Seguem-se alguns exemplos de violações comuns:

- Programadores que insinuam falsamente uma relação com outra empresa/programador/entidade/organização.



① O nome de programador listado para esta app sugere uma relação oficial com a Google, embora tal relação não exista.

- Apps cujos ícones e títulos insinuam falsamente uma relação com outra empresa/programador/entidade/organização.



①A app está a usar um emblema nacional e a induzir os utilizadores a acreditar que está afiliada ao governo.
②A app está a copiar o logótipo de uma entidade empresarial para sugerir falsamente que é uma app oficial da empresa.

- Ícones e títulos de apps que sejam tão semelhantes aos de produtos ou serviços existentes que podem enganar os utilizadores.

①A app está a usar o logótipo de um Website popular de criptomoeda no respetivo ícone da app para sugerir que se trata do Website oficial.
②A app está a copiar a personagem e o título de um programa de TV famoso no respetivo ícone da app e a enganar os utilizadores tentando convencê-los de que está afiliada a um programa de TV.

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

Software indesejável para dispositivos móveis

Na Google, acreditamos que o fundamental é centrarmo-nos no utilizador, tudo o resto vem naturalmente. Nos nossos Princípios de software e na Política de Software Indesejável, fornecemos recomendações gerais para software que proporciona uma excelente experiência do utilizador. Esta política baseia-se na Política de Software Indesejável da Google ao definir princípios para o ecossistema Android e a Google Play Store. O software que viola estes princípios é potencialmente prejudicial para a experiência do utilizador, pelo que tomaremos as medidas adequadas para proteger os utilizadores contra o mesmo.

Tal como mencionado na Política de Software Indesejável, verificámos que a maioria do software indesejável apresenta uma ou mais das mesmas caraterísticas básicas:

- É enganador ao prometer uma proposta de valor que não é capaz de cumprir.
- Tenta levar os utilizadores a instalá-lo ou é instalado sub-repticiamente juntamente com outro programa.
- Não informa o utilizador sobre todas as funções principais e importantes.
- Afeta o sistema do utilizador de formas inesperadas.
- Recolhe ou transmite informações privadas sem conhecimento dos utilizadores.
- Recolhe ou transmite informações privadas sem um processamento seguro (por exemplo, transmissão através de HTTPS).
- Está integrado noutro software e a sua presença não é revelada.

Em dispositivos móveis, o software é um código sob a forma de uma app, um binário, uma modificação de framework, etc. Para evitar software prejudicial para o ecossistema de software ou perturbador da experiência do utilizador, vamos tomar medidas relativamente a código que viole estes princípios.

Abaixo, baseamo-nos na Política de Software Indesejável para alargar a respetiva aplicabilidade a software para dispositivos móveis. Tal como acontece com essa política, continuaremos a refinar esta Política de Software Indesejável para Dispositivos Móveis para abordar novos tipos de abuso.

Comportamento transparente e divulgações claras

Todo o código deve cumprir as promessas feitas ao utilizador. As apps devem fornecer todas as funcionalidades comunicadas. As apps não devem confundir os utilizadores.

- As apps devem ser claras acerca da funcionalidade e dos objetivos.
- Explique de forma explícita e clara ao utilizador as alterações ao sistema que a app irá efetuar. Permita que os utilizadores revejam e aprovem todas as opções e alterações significativas da instalação.
- O software não deve fazer uma representação fraudulenta do estado do dispositivo para o utilizador, por exemplo, ao alegar que o sistema está num estado de segurança crítico ou infetado com vírus.
- Não utilize atividades inválidas concebidas para aumentar o tráfego de anúncios e/ou as conversões.
- Não são permitidas apps que enganem os utilizadores ao fazerem-se passar por outra pessoa (por exemplo, outro programador, empresa, entidade) ou outra app. Não insinue que a sua app está relacionada ou autorizada por alguém que não tem qualquer relação com a mesma ou não a autorizou.

Exemplos de violações:

- Fraude ao nível da publicidade
- Engenharia social

Proteja a privacidade e os dados do utilizador

Divulgue de forma clara e transparente o acesso, a utilização, a recolha e a partilha de dados pessoais e confidenciais do utilizador. A aplicação dos dados do utilizador tem de cumprir todas as Políticas de Dados do Utilizador relevantes, sempre que aplicável, e tomar todas as precauções para proteger os dados.

Todas as apps têm de estar em conformidade com todas as Políticas do Programa para Programadores do Google Play, incluindo políticas de dados do dispositivo e do utilizador, nomeadamente a Política de Dados do Utilizador, a Política de Autorizações e APIs com Acesso a Informações Confidenciais, a Política de Spyware e a Política de Requisitos de SDKs.

- Não solicite aos utilizadores que desativem, nem os engane no sentido de desativarem, as proteções de segurança do dispositivo, como o Google Play Protect. Por exemplo, não pode oferecer recompensas nem funcionalidades de apps adicionais aos utilizadores em troca da desativação do Google Play Protect.

Não prejudique a experiência em dispositivos móveis

A experiência do utilizador deve ser intuitiva, fácil de compreender e baseada em escolhas claras feitas pelo utilizador. Deve apresentar uma proposta de valor clara ao utilizador e não interromper a experiência anunciada ou desejada do utilizador.

- Não mostre anúncios que sejam apresentados aos utilizadores de formas inesperadas, incluindo ao afetarem ou interferirem com a capacidade de utilização das funções do dispositivo ou ao serem apresentados fora do ambiente da app acionadora sem serem fáceis de ignorar e sem o devido consentimento e atribuição.
- As apps não devem interferir com outras apps nem com a capacidade de utilização do dispositivo.
- A desinstalação, quando aplicável, deve ser clara.

- O software para dispositivos móveis não deve simular pedidos do SO do dispositivo ou de outras apps. Não suprima alertas ao utilizador provenientes de outras apps ou do sistema operativo, nomeadamente aqueles que informam o utilizador acerca de alterações ao respetivo SO.

Exemplos de violações:

- Anúncios perturbadores
- Utilização não autorizada ou imitação da funcionalidade do sistema

---

Gestores de transferências hostis

Código que, por si só, não é um software indesejável, mas transfere outro software indesejável para dispositivos móveis (MUwS).

O código pode ser um gestor de transferências hostil se:

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

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

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

Fraude ao nível da publicidade

A fraude ao nível da publicidade é estritamente proibida. As interações com anúncios geradas com o objetivo de levar uma rede de publicidade a acreditar que o tráfego é proveniente de um interesse autêntico do utilizador é fraude ao nível da publicidade, que é uma forma de tráfego inválido. A fraude ao nível da publicidade pode ser um subproduto da implementação pelos programadores de anúncios de formas não permitidas, como mostrar anúncios ocultos, clicar automaticamente em anúncios, alterar ou modificar informações e tirar partido de ações não executadas por humanos (spiders, bots, etc.) ou atividade humana concebida para produzir tráfego de anúncios inválido. O tráfego inválido e a fraude ao nível da publicidade são prejudiciais para anunciantes, programadores e utilizadores, e conduzem a uma perda de confiança a longo prazo no ecossistema de anúncios para dispositivos móveis.

Seguem-se alguns exemplos de violações comuns:

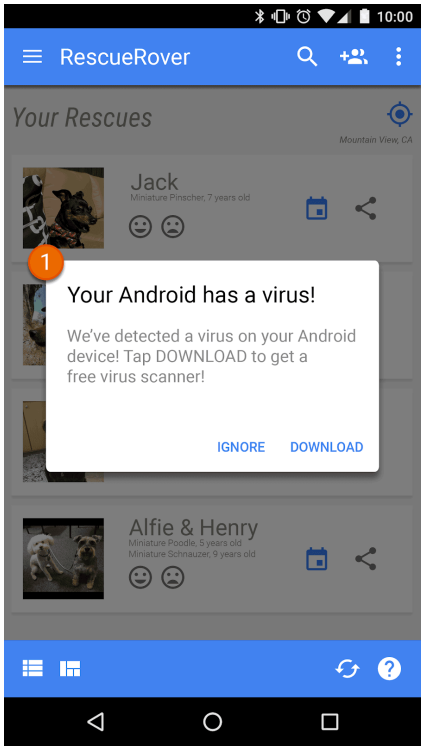
- Uma app que converte anúncios que não são visíveis para o utilizador.
- Uma app que gera automaticamente cliques em anúncios sem a intenção do utilizador ou que produz tráfego de rede equivalente para fornecer créditos de cliques de forma fraudulenta.
- Uma app que envia cliques falsos de atribuição de instalações para receber pagamentos por instalações que não tiveram origem na rede do remetente.
- Uma app que apresenta anúncios pop-up quando o utilizador não está na interface da app.
- Declarações falsas do inventário de anúncios feitas por uma app, por exemplo, uma app que comunique a redes de publicidade que está a ser executada num dispositivo iOS quando, de facto, está a ser executada num dispositivo Android; uma app que faça uma representação fraudulenta do nome do pacote que está a ser rentabilizado.

Utilização não autorizada ou imitação da funcionalidade do sistema

Não permitimos apps ou anúncios que imitem ou interfiram com a funcionalidade do sistema, como notificações ou avisos. Só é possível utilizar as notificações ao nível do sistema para funcionalidades integrais de uma app, como uma app de uma companhia aérea que notifica os utilizadores sobre ofertas especiais ou um jogo que notifica os utilizadores sobre promoções no jogo.

Seguem-se alguns exemplos de violações comuns:

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



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

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

Engenharia social

Não são permitidas apps que fingem ser outra app com a intenção de enganar os utilizadores para efetuarem ações que pretendiam efetuar na app fidedigna original.

Rentabilização e anúncios

O Google Play apoia várias estratégias de rentabilização para beneficiar os programadores e os utilizadores, incluindo distribuição paga, produtos na app, subscrições e modelos baseados em anúncios. Para garantir a melhor experiência do utilizador, tem de cumprir estas políticas.

Pagamentos

1. Os programadores que cobram por transferências de apps do Google Play têm de usar o sistema de faturação do Google Play como método de pagamento para essas transações.
2. As apps distribuídas no Google Play que exijam ou aceitem pagamentos para aceder a serviços ou funcionalidades na app, incluindo qualquer funcionalidade da app, conteúdo digital ou bens

(coletivamente, "compras na app"), têm de usar o sistema de faturação do Google Play para essas transações, a menos que se aplique a Secção 3, 8 ou 9.

Exemplos de funcionalidades ou serviços de apps que requerem a utilização do sistema de faturação do Google Play incluem, entre outros, compras na app de:

- Itens (como moedas virtuais, vidas extra, tempo de jogo adicional, itens suplementares, personagens e avatares);
- Serviços de subscrição (como serviços de fitness, jogos, encontros, educação, música, vídeo, atualizações de serviço e outros serviços de subscrição de conteúdo);
- Funcionalidades ou conteúdo de apps (como uma versão sem anúncios de uma app ou novas funcionalidades não disponíveis na versão gratuita);
- Software e serviços na nuvem (como serviços de armazenamento de dados, software de produtividade empresarial e software de gestão financeira).

3. O sistema de faturação do Google Play não pode ser usado nos casos em que:
   a. O pagamento se destinar principalmente:
      - À compra ou ao aluguer de bens físicos (como alimentos, vestuário, utensílios domésticos e produtos eletrónicos);
      - À aquisição de serviços físicos (como serviços de transporte, serviços de limpeza, bilhetes de avião, mensalidades de ginásio, entrega de comida e bilhetes para eventos em direto); ou
      - A uma remessa relativa a uma fatura de cartão de crédito ou uma fatura de serviços (como serviços de televisão por cabo e telecomunicações);
   b. A pagamentos que incluam pagamentos ponto a ponto, leilões online e donativos isentos de impostos;
   c. A pagamentos destinados a conteúdos ou serviços que facilitem jogos de azar online, conforme descrito na secção Apps de jogos de azar da Política de Jogos de Azar a Dinheiro Real, Jogos e Concursos;
   d. A pagamentos relativos a qualquer categoria de produtos considerada inaceitável ao abrigo das políticas de conteúdos do centro de pagamentos da Google.

   Nota: em alguns mercados, disponibilizamos o Google Pay para apps que vendem bens físicos e/ou serviços. Para mais informações, visite a nossa página do programador do Google Pay .

4. À parte das condições descritas na Secção 3, 8 e 9, as apps não podem direcionar os utilizadores para um método de pagamento diferente do sistema de faturação do Google Play. Esta proibição inclui, entre outros, direcionar os utilizadores para outros métodos de pagamento através:
   - Da ficha de uma app no Google Play;
   - De promoções na app relacionadas com conteúdo adquirível;
   - De WebViews, botões, links, mensagens, anúncios ou outros apelos à ação na app; e
   - De fluxos da interface do utilizador na app, incluindo fluxos de criação de contas ou inscrição, que direcionam os utilizadores de uma app para um método de pagamento diferente do sistema de faturação do Google Play como parte desses fluxos.
5. Só é possível usar moedas virtuais na app dentro da app ou do título do jogo para o qual foram compradas.
6. Os programadores têm de informar os utilizadores de forma clara e precisa acerca dos termos e preços das respetivas apps ou de quaisquer funcionalidades ou subscrições na app disponibilizadas para compra. Os preços na app têm de corresponder aos preços apresentados na interface da Faturação Play orientada para o utilizador. Se a descrição do produto no Google Play se referir a funcionalidades na app que possam requerer uma cobrança específica ou adicional, a sua ficha da app tem de notificar claramente os utilizadores de que é necessário um pagamento para aceder a essas funcionalidades.

7. As apps e os jogos que ofereçam mecanismos para receber itens virtuais aleatórios de uma compra, incluindo, entre outros, "caixas de saque", têm de divulgar de forma clara as probabilidades de receção desses itens imediatamente antes dessa compra.
8. A menos que se apliquem as condições descritas na Secção 3, os programadores de apps distribuídas no Google Play que exijam ou aceitem pagamentos de utilizadores nestes países/regiões para aceder a compras na app podem oferecer aos utilizadores um sistema de faturação alternativo na app além do sistema de faturação do Google Play para essas transações, caso preencham o formulário de declaração de faturação com êxito para cada programa respetivo e aceitem os termos adicionais e os requisitos do programa aí incluídos.
9. Os programadores de apps distribuídas no Google Play podem levar os utilizadores do Espaço Económico Europeu (EEE) para fora da app, inclusive para promover ofertas de funcionalidades e serviços digitais na app. Os programadores que levem os utilizadores do EEE para fora da app têm de preencher um formulário de declaração com êxito para o programa e aceitar os termos adicionais e os requisitos do programa aí incluídos.

Nota: para ver as linhas cronológicas e as Perguntas frequentes relativas a esta política, visite o nosso Centro de Ajuda.

Anúncios

Para manter uma experiência de qualidade, temos em conta o conteúdo, o público-alvo, a experiência do utilizador e o comportamento, bem como a segurança e a privacidade do seu anúncio. Consideramos os anúncios e as ofertas associadas como parte da sua app e, por isso, têm de cumprir todas as outras Políticas do Google Play. Também temos requisitos adicionais para anúncios se estiver a rentabilizar uma app que segmenta crianças no Google Play.

Também pode ler mais sobre as nossas Políticas de Promoção de Apps e da Ficha da Loja aqui, incluindo a forma como abordamos as práticas de promoção enganosas.

Conteúdo do anúncio

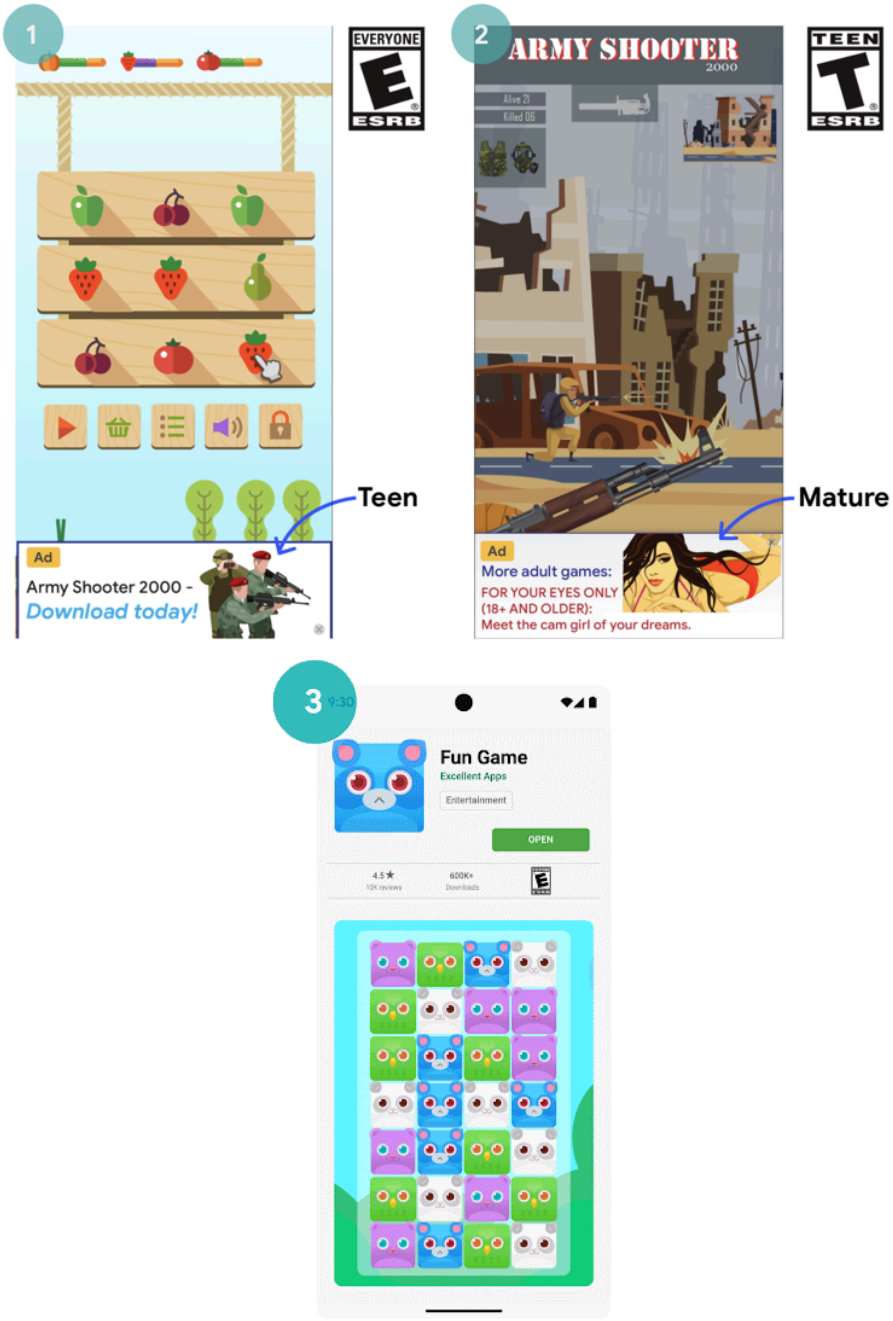
Os anúncios e as ofertas associadas fazem parte da sua app e têm de cumprir as nossas Políticas de Conteúdo Restrito. Aplicam-se requisitos adicionais se a sua app for uma app de jogos de azar.

Anúncios impróprios

Os anúncios e as respetivas ofertas associadas (por exemplo, o anúncio está a promover a transferência de outra app) apresentados na sua app têm de ser apropriados para a classificação de conteúdo da sua app, mesmo que o conteúdo por si só esteja em conformidade com as nossas políticas.

Seguem-se alguns exemplos de violações comuns:

- Anúncios que são inadequados para a classificação de conteúdo da app



① Este anúncio é impróprio (Adolescentes) para a classificação de conteúdo da app (Todos)
② Este anúncio é impróprio (Adultos) para a classificação de conteúdo da app (Adolescentes)
③ A oferta do anúncio (que promove a transferência de uma app para adultos) é imprópria para a classificação de conteúdo da app de jogos na qual o anúncio foi apresentado (Todos)

Requisitos de anúncios para famílias

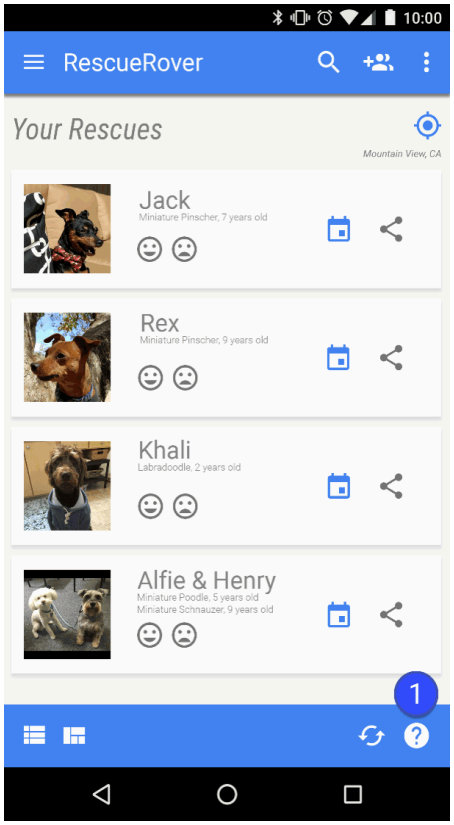
Se estiver a rentabilizar uma app que segmenta crianças no Google Play, é importante que a sua app cumpra os requisitos da Política de Rentabilização e Anúncios para Famílias.

Anúncios enganadores

Os anúncios não podem simular nem imitar a interface do utilizador de qualquer funcionalidade da app, como as notificações ou os elementos de aviso de um sistema operativo. Deve ser claro para o utilizador que app está a publicar cada anúncio.

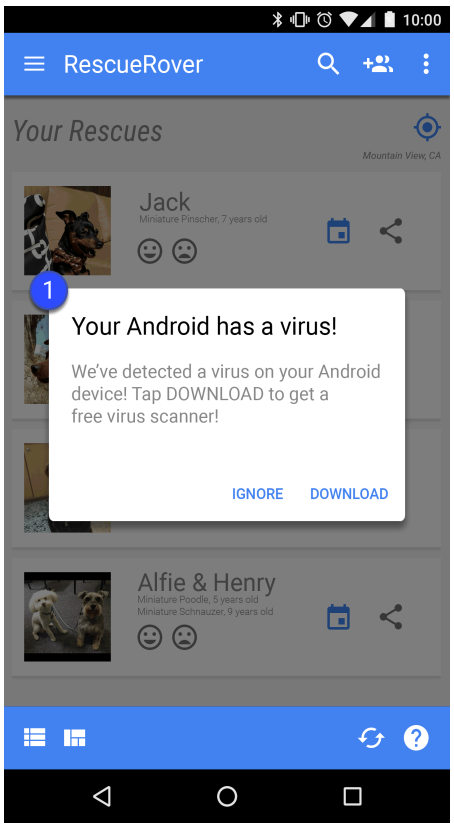
Seguem-se alguns exemplos de violações comuns:

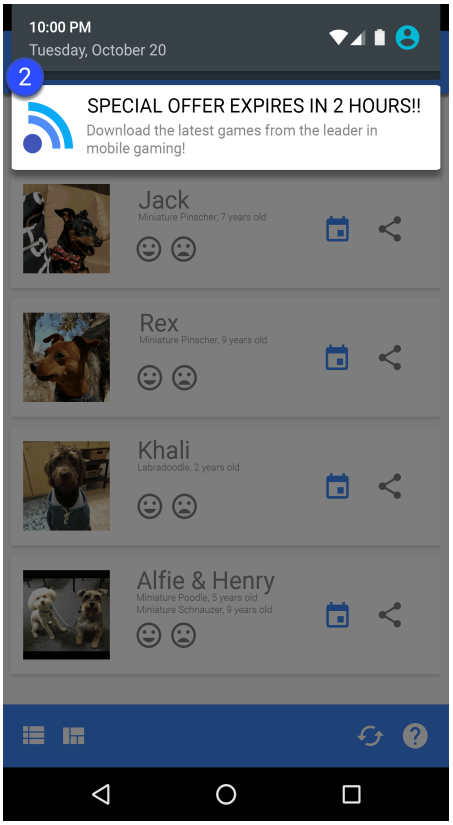
- Anúncios que imitam a IU de uma app:



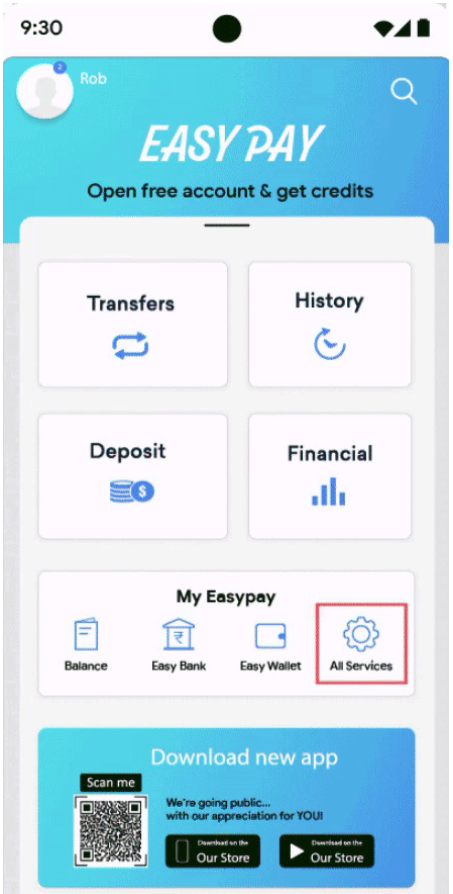
① O ícone do ponto de interrogação nesta app é um anúncio que direciona o utilizador para uma página de destino externa.

- Anúncios que imitam uma notificação de sistema:





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



① O exemplo acima ilustra uma secção de funcionalidades que imita outras funcionalidades, mas apenas direciona o utilizador para um ou vários anúncios.

Anúncios perturbadores

Anúncios perturbadores são anúncios apresentados aos utilizadores de formas inesperadas, que podem resultar em cliques inadvertidos, prejudicar ou interferir com a capacidade de utilização das funções do dispositivo.

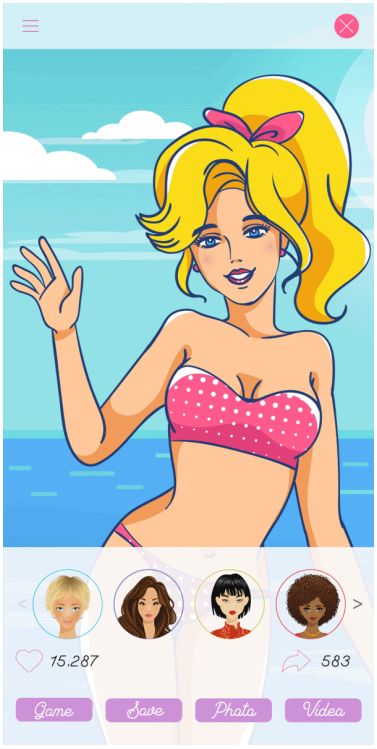
A sua app não pode forçar um utilizador a clicar num anúncio ou a enviar informações pessoais para fins publicitários antes de poder usar totalmente uma app. Os anúncios só podem ser apresentados na app que os publica e não podem interferir com outras apps, anúncios ou com o funcionamento do dispositivo, incluindo botões e portas do sistema ou dispositivo. Isto inclui sobreposições, funcionalidade associada e blocos de anúncios com widgets. Se a sua app apresentar anúncios que interfiram com a utilização normal, estes devem ser fáceis de ignorar sem penalizações.

Seguem-se alguns exemplos de violações comuns:

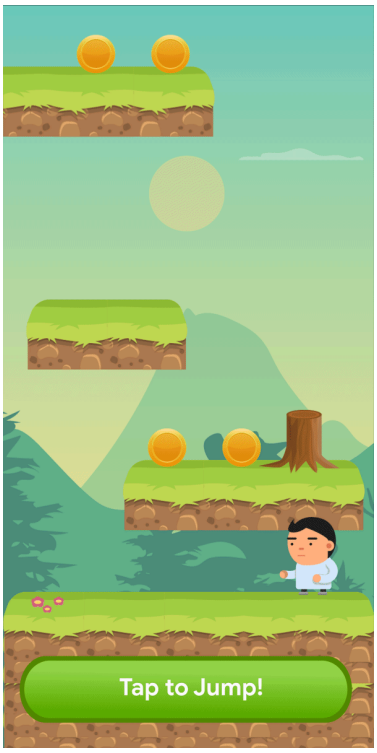
- Anúncios que ocupam todo o ecrã ou interferem com a utilização normal e não fornecem um meio claro para os ignorar:

① Este anúncio não tem um botão de ignorar.

- Anúncios que forçam o utilizador a clicar através de um botão de ignorar falso ou ao fazer com que sejam apresentados anúncios de forma repentina em áreas da app em que o utilizador toca normalmente para outra função:

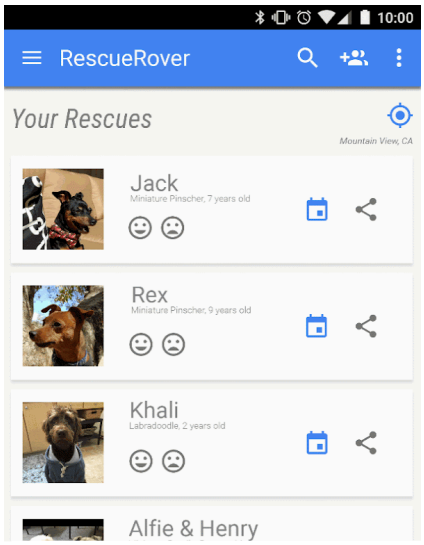


① Este anúncio usa um botão de ignorar falso.



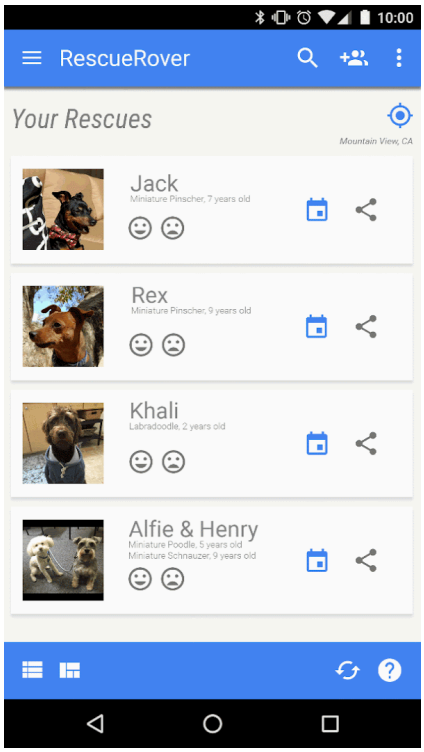
② Este anúncio aparece de forma repentina numa área onde o utilizador está habituado a tocar para funções na app.

- Anúncios apresentados fora da app que os publica:



① O utilizador navega para o ecrã principal a partir desta app e, de repente, surge um anúncio no ecrã principal.

- Anúncios que são acionados pelo botão página inicial ou por outras funcionalidades expressamente concebidas para sair da app:



① O utilizador tenta sair da app e navegar até ao ecrã principal, mas, em vez disso, o fluxo esperado é interrompido por um anúncio.

Better Ads Experiences

Os programadores são obrigados a cumprir as seguintes diretrizes de anúncios para garantir experiências de alta qualidade para os utilizadores quando estes utilizam as apps do Google Play. Os seus anúncios podem não ser apresentados aos utilizadores das seguintes formas inesperadas:

- Não são permitidos anúncios intercalares de ecrã inteiro de todos os formatos (vídeo, em GIF, estático, etc.), que aparecem inesperadamente, normalmente quando o utilizador optou por fazer outra coisa.
  - Não são permitidos anúncios que aparecem durante o jogo no início de um nível ou durante o início de um segmento de conteúdo.
  - Não são permitidos anúncios intercalares de vídeo em ecrã inteiro que aparecem antes do ecrã de carregamento de uma app (ecrã inicial).
- Não são permitidos anúncios intercalares de ecrã inteiro de todos os formatos que não podem ser fechados após 15 segundos. Os anúncios intercalares de ecrã inteiro de inclusão ou os anúncios intercalares de ecrã inteiro que não interrompem as ações dos utilizadores (por exemplo, após o ecrã de pontuação numa app de jogos) podem persistir mais de 15 segundos.

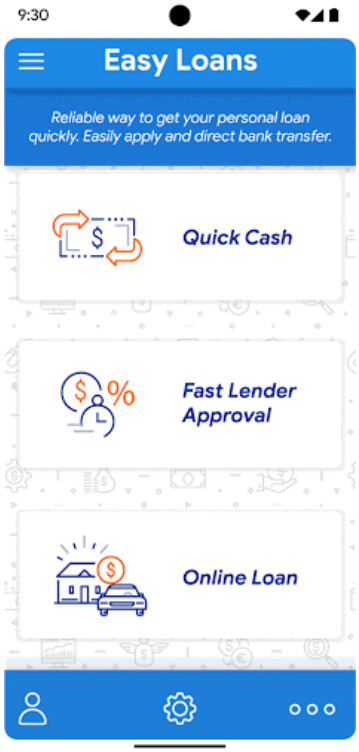
Esta política não se aplica a anúncios premiados que são explicitamente ativados pelos utilizadores (por exemplo, um anúncio que os programadores oferecem explicitamente a um utilizador para ver em troca do desbloqueio de uma funcionalidade específica do jogo ou de uma parte de conteúdo). Esta política também não se aplica à rentabilização nem à publicidade que não interfere com a utilização normal de apps ou jogos (por exemplo, conteúdo de vídeo com anúncios integrados, anúncios de faixa de ecrã não inteiro).

Estas diretrizes baseiam-se nas diretrizes Better Ads Standards . Para mais informações sobre as Better Ads Standards, consulte a Coalition for Better Ads .

Seguem-se alguns exemplos de violações comuns:

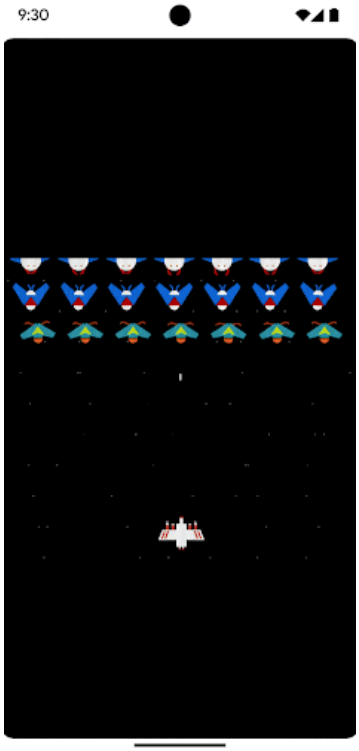
- Anúncios inesperados que aparecem durante o jogo ou durante o início de um segmento de conteúdo (por exemplo, após um utilizador clicar num botão e antes da ação pretendida pelo clique no botão ter entrado em vigor). Estes anúncios são inesperados para os utilizadores, uma vez que estes esperam o início de um jogo ou a interação com o conteúdo em vez disso.

① Um anúncio estático inesperado aparece durante o jogo no início de um nível.



② Um anúncio de vídeo inesperado aparece durante o início de um segmento de conteúdo.

- Um anúncio de ecrã inteiro que aparece durante o jogo e que não pode ser fechado após 15 segundos.



① Um anúncio intercalar aparece durante o jogo e não oferece aos utilizadores uma opção para ignorar dentro de 15 segundos.

Concebidas para anúncios

Não são permitidas apps que apresentem anúncios intercalares repetidamente para distrair os utilizadores de interagirem com uma app e realizarem tarefas na app.

Seguem-se alguns exemplos de violações comuns:

- Apps nas quais é posicionado um anúncio intercalar após uma ação do utilizador (incluindo, entre outras, cliques, deslizes, etc.) de uma forma consecutiva.

① A primeira página na app tem vários botões com os quais é possível interagir. Quando o utilizador clica em **Iniciar app** para usar a app, surge um anúncio intercalar. Após o anúncio ser fechado, o utilizador regressa à app e clica em **Serviço** para começar a usar o serviço, mas aparece outro anúncio intercalar.

② Na primeira página, o utilizador é induzido a clicar em **Jogar**, uma vez que é o único botão disponível para usar a app. Quando o utilizador clica no mesmo, aparece um anúncio intercalar. Após o anúncio ser fechado, o utilizador clica em **Iniciar**, uma vez que é o único botão com o qual pode interagir e aparece outro anúncio intercalar.

Rentabilização do ecrã de bloqueio

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

Fraude ao nível da publicidade

A fraude ao nível da publicidade é estritamente proibida. Para mais informações, consulte a nossa Política de Fraude de Anúncios.

Utilização de dados de localização para anúncios

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

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

atuais na app e não podem solicitar autorizações de acesso à localização do dispositivo exclusivamente para a utilização de anúncios.

Utilização do ID de publicidade Android

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

- **Utilização**. O identificador de publicidade Android (AAID) apenas deve ser utilizado para análises de utilizadores e de publicidade. O estado da definição "Excluir publicidade baseada em interesses" ou "Desativar a personalização de anúncios" deve ser validado em cada acesso do ID.
- **Associação a informações de identificação pessoal ou outros identificadores**.
  - Utilização para fins de publicidade: o identificador de publicidade não pode estar ligado a identificadores de dispositivos persistentes (por exemplo: SSAID, endereço MAC, IMEI, etc.) para qualquer finalidade de publicidade. O identificador de publicidade só pode estar ligado a informações de identificação pessoal com o consentimento explícito do utilizador.
  - Utilização para fins estatísticos: o identificador de publicidade não pode estar ligado a informações de identificação pessoal nem associado a qualquer identificador de dispositivo persistente (por exemplo: SSAID [ID Android], endereço MAC [Media Access Control], IMEI [International Mobile Equipment Identity], etc.) para qualquer finalidade estatística. Leia a Política de Dados do Utilizador para obter diretrizes adicionais sobre identificadores de dispositivos persistentes.
- **Respeito das seleções dos utilizadores**.
  - Em caso de reposição, um novo identificador de publicidade não pode estar associado a um identificador de publicidade anterior ou a dados derivados de um identificador de publicidade anterior sem o consentimento expresso do utilizador.
  - Tem de respeitar a definição "Excluir publicidade baseada em interesses" ou "Desativar a personalização de anúncios" do utilizador. Se um utilizador tiver ativado esta definição, não pode utilizar o identificador de publicidade para criar perfis de utilizador para fins de publicidade ou segmentar utilizadores com publicidade personalizada. As atividades permitidas incluem a publicidade por contexto, o limite de frequência, o acompanhamento de conversões, os relatórios, a segurança e a deteção de fraude.
  - Em dispositivos mais recentes, quando um utilizador elimina o identificador de publicidade Android, este é removido. Todas as tentativas de aceder ao identificador irão receber uma string de zeros. Um dispositivo sem um identificador de publicidade não pode estar associado a dados ligados ou derivados de um identificador de publicidade anterior.
- **Transparência para os utilizadores**. A recolha e a utilização do identificador de publicidade e o compromisso para com os presentes termos devem ser divulgados aos utilizadores através de uma notificação de privacidade juridicamente adequada. Para saber mais acerca das nossas normas de privacidade, reveja a nossa Política de Dados do Utilizador .
- **Cumprimento dos Termos de Utilização**. Só é possível usar o identificador de publicidade de acordo com a Política do Programa para programadores do Google Play, incluindo por qualquer parte com a qual o possa partilhar no decorrer da sua atividade. Todas as apps carregadas ou publicadas no Google Play têm de utilizar o ID de publicidade (quando estiver disponível num dispositivo) em detrimento de quaisquer outros identificadores de dispositivos para quaisquer fins publicitários.

Para mais informações, consulte a nossa Política de Dados do Utilizador.

Subscrições

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

em todos os ecrãs iniciais ou promoções na app. Não são permitidas apps que sujeitem os utilizadores a experiências de compra enganosas ou manipuladoras (incluindo subscrições ou compras na app).

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

As subscrições têm de fornecer um valor sustentado ou recorrente aos utilizadores durante todo o período da subscrição e não podem ser utilizadas para oferecer benefícios que são, na realidade, de utilização única aos utilizadores (por exemplo, SKUs que fornecem moedas/créditos na app de um montante fixo ou impulsos de jogos de utilização única). A sua subscrição pode oferecer bónus promocionais ou de incentivo, mas estes têm de ser complementares ao valor sustentado ou recorrente durante todo o período da subscrição**.** Os produtos que não oferecerem um valor sustentado ou recorrente têm de utilizar um produto na app em vez de um produto de subscrição.

Não pode disfarçar nem descaraterizar vantagens de utilização única como subscrições junto dos utilizadores. Isto inclui a modificação de uma subscrição para se tornar uma oferta de utilização única (por exemplo, cancelamento, descontinuação ou minimização do valor recorrente) depois de o utilizador ter comprado a subscrição.

Seguem-se alguns exemplos de violações comuns:

- Subscrições mensais que não informam os utilizadores de que serão automaticamente renovadas e que pagarão um valor todos os meses.
- Subscrições anuais que apresentam os preços mais proeminentemente em termos de custo mensal.
- Termos e preços da subscrição que estão localizados de forma incompleta.
- Promoções na app que não demonstram claramente que o utilizador pode aceder ao conteúdo sem uma subscrição (se disponível).
- Nomes de SKUs que não transmitem com exatidão a natureza da subscrição, como "Avaliação gratuita" ou "Experimente a subscrição Premium durante 3 dias grátis" para uma subscrição com uma cobrança recorrente automática.
- Vários ecrãs no fluxo de compra que induzem os utilizadores a clicar acidentalmente no botão de subscrição.
- Subscrições que não oferecem um valor sustentado ou recorrente — por exemplo, oferta de 1000 pedras preciosas no primeiro mês e, depois, redução da vantagem para 1 pedra preciosa nos meses subsequentes da subscrição.
- Exigir a um utilizador que se inscreva numa subscrição de renovação automática para oferecer uma vantagem de utilização única e cancelar a subscrição do utilizador sem o respetivo pedido após a compra.

Exemplo 1:

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

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

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

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

Exemplo 2:

① Cliques recorrentes na mesma área do botão fazem com que o utilizador clique inadvertidamente no botão "continuar" final para subscrever.

② O valor cobrado aos utilizadores no final da avaliação é de difícil leitura, o que pode levar os utilizadores a pensarem que o plano é gratuito

Avaliações gratuitas e ofertas iniciais

Antes de um utilizador estar inscrito na sua subscrição: tem de descrever de forma clara e precisa os termos da sua oferta, incluindo a duração, o preço e a descrição dos conteúdos ou serviços acessíveis. Certifique-se de que informa os seus utilizadores sobre quando e como uma avaliação gratuita será convertida numa subscrição paga, quanto a mesma irá custar e que podem cancelar se não quiserem converter numa subscrição paga.

Seguem-se alguns exemplos de violações comuns:

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

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

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

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

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

Gestão, cancelamento e reembolsos de subscrições

Se vender subscrições nas suas apps, tem de garantir que as mesmas divulgam claramente a forma como um utilizador pode gerir ou cancelar a respetiva subscrição. Também tem de incluir na sua app o acesso a um método online e fácil de usar para cancelar a subscrição. Nas definições da conta da sua app (ou página equivalente), pode satisfazer este requisito ao incluir:

- Um link para o centro de subscrições do Google Play (para apps que usam o sistema de faturação do Google Play); e/ou
- acesso direto ao seu processo de cancelamento.

Se um utilizador cancelar uma subscrição comprada através do sistema de faturação do Google Play, a nossa política geral prevê que o utilizador não irá receber um reembolso pelo período de faturação

atual, mas vai continuar a receber os conteúdos da respetiva subscrição durante o período de faturação restante, independentemente da data de cancelamento. O cancelamento do utilizador entra em vigor após a conclusão do período de faturação atual.

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

Programa de SDKs de anúncios autocertificados para famílias

Se publicar anúncios na sua app e o respetivo público-alvo incluir apenas crianças, tal como descrito na Política para Famílias , só pode usar versões de SDKs de anúncios com conformidade autocertificada com as Políticas do Google Play, incluindo os requisitos de SDKs de anúncios autocertificados para famílias abaixo.

Se o público-alvo da sua app incluir tanto crianças como utilizadores mais velhos, tem de assegurar que os anúncios apresentados a crianças são provenientes exclusivamente de uma destas versões de SDKs de anúncios autocertificados (por exemplo, através do uso de medidas de filtragem de idade neutras).

Tenha em conta que é da sua responsabilidade garantir que todas as versões do SDK que implementa na sua app, incluindo versões de SDKs de anúncios autocertificados, estão em conformidade com todas as políticas, leis locais e regulamentos aplicáveis. A Google não faz representações ou garantias quanto à exatidão das informações facultadas pelos SKDs de anúncios durante o processo de autocertificação.

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

- Publicidade interna, através da qual usa SDKs para gerir a promoção cruzada das suas apps ou de outro merchandising e conteúdo multimédia dos quais é proprietário.
- Estabelecer acordos diretos com anunciantes através dos quais usa SDKs para gestão de inventário.

Requisitos de SDKs de anúncios autocertificados para famílias

- Defina o que são comportamentos e conteúdos de anúncios censuráveis e proíba-os nos termos ou nas políticas do SDK de anúncios. As definições devem estar em conformidade com as Políticas do Programa para programadores do Google Play.
- Crie um método de classificação dos seus criativos de anúncios de acordo com grupos adequados para a idade. Estes grupos devem incluir, no mínimo, grupos para Todos e Adultos. A metodologia de classificação tem de estar em linha com a metodologia que a Google fornece aos SDKs assim que tiverem preenchido o formulário de interesse abaixo.
- Permita que os publicadores, por pedido ou app, solicitem o tratamento dirigido a crianças para a publicação de anúncios. Este tratamento tem de estar em conformidade com as leis e os regulamentos aplicáveis, como a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA e o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE . O Google Play requer que os SDKs de anúncios desativem anúncios personalizados, publicidade baseada em interesses e remarketing como parte do tratamento dirigido a crianças.
- Permita que os publicadores selecionem formatos de anúncios que estejam em conformidade com a Política de Rentabilização e Anúncios para Famílias do Google Play e cumpram o requisito do programa Aprovado por professores .
- Certifique-se de que, quando forem utilizados lances em tempo real para publicar anúncios para crianças, os criativos foram revistos e os indicadores de privacidade são propagados para os

licitadores.

- Forneça à Google informações suficientes, como o envio de uma app de teste e as informações indicadas no formulário de interesse abaixo, para validar a conformidade da política do SDK de anúncios com todos os requisitos de autocertificação, responda atempadamente a quaisquer pedidos de informação subsequentes, como o envio de lançamentos de novas versões para validar a conformidade da versão do SDK de anúncios com todos os requisitos de autocertificação e o fornecimento de uma app de teste.
- Certifique-se de que todos os lançamentos de novas versões estão em conformidade com as Políticas do Programa para programadores do Google Play mais recentes, incluindo os Requisitos da Política para Famílias.

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

Pode encontrar mais informações sobre marcas de água em criativos de anúncios e o fornecimento de uma app de teste aqui .

Seguem-se os requisitos de mediação para plataformas de publicação ao publicar anúncios para crianças:

- Use apenas SDKs de anúncios autocertificados para famílias ou implemente as salvaguardas necessárias para assegurar que todos os anúncios publicados a partir da mediação estão em conformidade com estes requisitos; e
- Transmita as informações necessárias às plataformas de mediação para indicar a classificação do conteúdo do anúncio e qualquer tratamento dirigido a crianças aplicável.

Os programadores podem encontrar uma lista de SDKs de anúncios autocertificados para famílias e verificar que versões específicas desses SDKs de anúncios são autocertificados para utilização em apps do programa Concebido para Famílias aqui .

Os programadores podem ainda partilhar este formulário de interesse com os SDKs de anúncios que querem autocertificar.

Ficha da loja e promoção

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

Promoção de apps

Não são permitidas apps que participem ou beneficiem, direta ou indiretamente, de práticas de promoção (como anúncios) enganadoras ou que sejam prejudiciais para os utilizadores ou para o ecossistema de programadores. As práticas de promoção são consideradas enganadoras ou prejudiciais se o respetivo comportamento ou conteúdo violar as nossas Políticas do Programa para programadores.

Seguem-se alguns exemplos de violações comuns:

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

- Texto ou imagem no nome do programador, ícone ou título da app que indique a classificação ou o desempenho na loja, o preço ou informações promocionais, ou que sugira relações com programas do Google Play existentes.

É da sua responsabilidade assegurar que quaisquer redes de publicidade, afiliados ou anúncios associados à sua app agem em conformidade com estas políticas.

Metadados

Os utilizadores dependem das descrições da sua app para os ajudar a compreender a respetiva funcionalidade e objetivo. Não permitimos apps com metadados enganadores, incorretamente formatados, não descritivos, irrelevantes, excessivos ou impróprios, incluindo, entre outros, a descrição da app, o nome do programador, o título, o ícone, as capturas de ecrã e as imagens promocionais. Os programadores têm de fornecer uma descrição clara e bem escrita da respetiva app. Da mesma forma, não permitimos testemunhos de utilizadores não atribuídos ou anónimos na descrição da app.

O título, o ícone e o nome do programador da sua app são particularmente úteis para os utilizadores encontrarem e saberem mais sobre a mesma. Não utilize emojis, ícones expressivos nem carateres especiais repetidos nestes elementos de metadados. Evite texto em MAIÚSCULAS, exceto se fizer parte do nome da sua marca. Não são permitidos símbolos enganosos nos ícones da app, tais como: um ponto indicador de nova mensagem quando não existem mensagens novas e símbolos de transferência/instalação quando a app não está relacionada com a transferência de conteúdo. O título da app tem de ter, no máximo, 30 carateres. Não use texto nem imagens no nome do programador, ícone ou título da app que indiquem a classificação ou o desempenho da app, o preço ou informações promocionais, ou que sugira relações com programas do Google Play existentes.

Para além dos requisitos mencionados aqui, algumas Políticas para Programadores do Google Play específicas podem exigir que forneça informações de metadados adicionais.

Seguem-se alguns exemplos de violações comuns:

① Testemunhos de utilizadores não atribuídos ou anónimos
② Comparação de dados de apps ou marcas
③ Blocos de palavras e listas de palavras verticais/horizontais

① Texto em MAIÚSCULAS que não pertença ao nome da marca
② Sequências de carateres especiais que sejam irrelevantes para a app
③ Utilização de emojis, ícones expressivos (incluindo kaomojis) e carateres especiais
④ Símbolos enganosos
⑤ Texto enganoso

- Imagens ou texto que indiquem o desempenho ou a classificação na loja, tais como ícones de prémios "App do ano", "N.º 1", "Melhor do Google Play em 20XX", "Popular", etc.

- Imagens ou texto que indiquem o preço e as informações promocionais, tais como "10% de desconto", "50 € de reembolso", "grátis apenas por tempo limitado", etc.

- Imagens ou texto que indiquem programas do Google Play, como "Escolha dos Editores", "Novo", etc.

Seguem-se alguns exemplos de texto, imagens ou vídeos impróprios na sua ficha:

- Imagens ou vídeos que incluem conteúdo com conotações sexuais. Evite imagens sugestivas com seios, nádegas, órgãos genitais ou outra parte anatómica, ou outro conteúdo alvo de fetiches, independentemente de serem ilustrados ou reais.
- Utilizar linguagem obscena, vulgar ou outra linguagem imprópria para um público-alvo geral na Ficha da loja da sua app.
- Violência gráfica representada proeminentemente em ícones de apps, vídeos ou imagens promocionais.
- Representações do uso ilícito de drogas. O conteúdo EDSA (educativo, documental, científico ou artístico) também tem de ser adequado a todos os públicos-alvo da Ficha da loja.

Eis algumas práticas recomendadas:

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

Classificações dos utilizadores, opiniões e instalações

Os programadores não podem tentar manipular o posicionamento das apps no Google Play. Isto inclui, entre outras ações, inflacionar as classificações, as críticas ou o número de instalações do produto por meios ilegítimos, como críticas e classificações fraudulentas ou incentivadas, ou incentivar os utilizadores a instalarem outras apps como a funcionalidade principal da app.

Seguem-se alguns exemplos de violações comuns:

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

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

- Enviar repetidamente classificações fazendo-se passar por utilizadores diferentes para influenciar o posicionamento de uma app no Google Play.

- Enviar ou incentivar os utilizadores a enviarem críticas com conteúdo impróprio, incluindo afiliados, cupões, códigos de jogos, endereços de email ou links para Websites ou outras apps:

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

As classificações e as críticas são elementos que informam sobre a qualidade da app. Os utilizadores dependem da sua autenticidade e relevância. Seguem-se algumas práticas recomendadas a utilizar nas respostas a críticas de utilizadores:

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

Classificações de conteúdo

As classificações de conteúdo no Google Play são fornecidas pela International Age Rating Coalition (IARC) e são concebidas para ajudar os programadores a divulgar as classificações de conteúdo pertinentes do ponto de vista geográfico junto dos utilizadores. As autoridades regionais da IARC mantêm diretrizes que são utilizadas para determinar o nível de maturidade do conteúdo de uma app. Não são permitidas apps sem classificação de conteúdo no Google Play.

Como são utilizadas as classificações de conteúdo

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

Como são atribuídas as classificações de conteúdo

Para receber uma classificação de conteúdo, tem de preencher um questionário de classificação na Play Console que indique a natureza do conteúdo das suas apps. É atribuída à app uma classificação de conteúdo de várias autoridades de classificação com base nas respostas do

questionário. A representação fraudulenta do conteúdo da sua app pode resultar na respetiva remoção ou suspensão, pelo que é importante fornecer respostas corretas ao questionário de classificação de conteúdo.

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

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

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

Recursos de classificação

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

Notícias

Uma app de notícias é uma app que:

- Se declara como app de "Notícias" na Google Play Console, ou
- Está incluída na categoria "Notícias e revistas" na Google Play Store e se descreve como de "notícias" no respetivo título, ícone, nome do programador ou descrição.

Exemplos de apps na categoria "Notícias e revistas" que se qualificam como apps de notícias:

- Apps que se descrevem como de "notícias" nas respetivas descrições, incluindo, entre outras:
  - Notícias mais recentes
  - Jornal
  - Notícias de última hora
  - Notícias locais
  - Notícias diárias
- Apps com a palavra "Notícias" nos respetivos títulos, ícones ou nome do programador.

No entanto, as apps que incluem principalmente conteúdo gerado pelo utilizador (por exemplo, apps de redes sociais) não se devem declarar como apps de notícias e não são consideradas como tal.

As apps de notícias que requerem que um utilizador compre uma subscrição têm de disponibilizar uma pré-visualização do conteúdo na app aos utilizadores antes da compra.

As apps de notícias têm de:

- Fornecer informações de propriedade sobre a app e a fonte dos artigos noticiosos incluindo, entre outras, a editora ou o autor original de cada artigo. Nos casos em que não é habitual listar os autores individuais dos artigos, a app de notícias tem de ser a editora original dos artigos. Tenha em atenção que os links para contas de redes sociais não são formas suficientes de informações do autor ou editora.
- Ter um Website dedicado ou uma página na app que identifique claramente que contém informações de contacto, seja fácil de encontrar (por exemplo, com um link na parte inferior da página inicial ou na barra de navegação do site) e forneça informações de contacto válidas para a editora de notícias, incluindo um número de telefone ou um endereço de email de contacto. Tenha em atenção que os links para contas de redes sociais não são formas suficientes de informações de contacto da editora.

As apps de notícias não podem:

- Conter erros ortográficos e/ou gramaticais significativos,
- Conter apenas conteúdo estático (por exemplo, conteúdo com mais de três meses) ou
- Ter o marketing afiliado ou a receita de anúncios como objetivo principal.

Tenha em atenção que as apps de notícias *podem* utilizar anúncios e outras formas de marketing para rentabilizar, desde que o propósito principal da app não seja vender produtos e serviços ou gerar receita publicitária.

As apps de notícias que agregam conteúdos de diferentes fontes de publicação têm de ser transparentes quanto à fonte de publicação do conteúdo na app e cada uma das fontes tem de cumprir os requisitos da Política de Notícias.

Consulte este artigo para saber qual é a melhor forma de fornecer as informações necessárias.

Spam, funcionalidade e experiência do utilizador

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

Spam

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

Spam em mensagens

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

Segue-se um exemplo de uma violação comum:

- Quando o utilizador prime o botão "Partilhar", a app envia mensagens em nome do utilizador sem possibilitar a hipótese de confirmar o conteúdo e os destinatários pretendidos:

Spam de afiliados e em visualizações na Web

Não são permitidas apps cujo objetivo principal seja direcionar tráfego afiliado para um Website ou fornecer uma visualização na Web de um Website sem autorização do administrador ou do proprietário do Website.

Seguem-se alguns exemplos de violações comuns:

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

① Esta app chama-se "Ted's Shopping Deal" e fornece simplesmente um WebView do Google Shopping.

Conteúdo repetitivo

Não são permitidas apps que se limitem a proporcionar a mesma experiência que outras apps já proporcionam no Google Play. As apps devem proporcionar valor aos utilizadores através da criação de conteúdos ou de serviços exclusivos.

Seguem-se alguns exemplos de violações comuns:

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

Funcionalidade, conteúdo e experiência do utilizador

As apps devem oferecer uma experiência do utilizador estável, dinâmica e envolvente. As apps que falham, não têm o nível básico de utilidade adequada como apps para dispositivos móveis, têm falta de conteúdos envolventes ou apresentam outro comportamento que não é consistente com uma experiência do utilizador funcional e envolvente não são permitidas no Google Play.

Funcionalidade e conteúdo limitados

Não são permitidas apps que apenas tenham uma funcionalidade e um conteúdo limitados.

Segue-se um exemplo de uma violação comum:

- Apps estáticas sem funcionalidades específicas de apps, por exemplo, apps apenas de texto ou de ficheiros PDF
- Apps com muito pouco conteúdo e que não oferecem uma experiência do utilizador envolvente, por exemplo, apps com uma única imagem de fundo

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

Funcionalidade danificada

Não permitimos apps que falhem, forcem o encerramento, bloqueiem ou, de qualquer outro modo, funcionem incorretamente.

Seguem-se alguns exemplos de violações comuns:

- Apps que **não instalam**.
-

Apps que instalam, mas **não carregam**.

- Apps que carregam, mas **não respondem**.

Outros programas

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

Apps instantâneas para Android

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

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

Identidade

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

Suporte de links

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

Especificações técnicas

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

Oferta da instalação de apps

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

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

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

Alterar o estado do dispositivo

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

Visibilidade das apps

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

Identificadores do dispositivo

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

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

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

Tráfego de rede

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

Política de Emojis do Android

A nossa Política de Emojis foi concebida para promover uma experiência do utilizador inclusiva e consistente. Para tal, todas as apps têm de suportar a versão mais recente dos emojis Unicode ao utilizar o Android 12 ou superior.

As apps que utilizam os emojis Android predefinidos sem qualquer implementação personalizada já utilizam a versão mais recente dos emojis Unicode ao utilizar o Android 12 ou superior.

As apps com implementações personalizadas de emojis, incluindo as fornecidas por bibliotecas de terceiros, têm de suportar totalmente a versão mais recente do Unicode ao utilizar o Android 12 ou superior no prazo de 4 meses após o lançamento dos novos emojis Unicode.

Consulte este guia para saber como suportar emojis modernos.

Famílias

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

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

Políticas para Famílias do Google Play

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

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

Todas as apps que estejam em conformidade com as Políticas para Famílias do Google Play podem optar por receber uma classificação no âmbito do programa Aprovado por professores, mas não podemos garantir que a sua app seja incluída neste programa.

Requisitos da Play Console

Público-alvo e conteúdo

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

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

Atualizações à secção Público-alvo e conteúdo

Pode atualizar as informações da app na secção Público-alvo e conteúdo na Google Play Console sempre que pretender. É necessária uma atualização da app antes de estas informações serem refletidas na Google Play Store. No entanto, quaisquer alterações efetuadas nesta secção da Google

Play Console podem ser revistas quanto à conformidade com as políticas mesmo antes de ser enviada uma atualização da app.

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

Representação fraudulenta na Play Console

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

Requisitos da Política para Famílias

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

1. **Conteúdo da app:** o conteúdo da app acessível a crianças tem de ser adequado para as mesmas. Se a sua app incluir conteúdos que não sejam globalmente apropriados, mas que sejam considerados apropriados para utilizadores menores de idade numa determinada região, a app pode estar disponível nessa região (regiões limitadas), mas permanecerá indisponível noutras regiões.
2. **Funcionalidade da app:** a sua app não deve apenas fornecer um WebView de um Website ou ter como objetivo principal direcionar tráfego afiliado para um Website sem autorização do administrador ou proprietário do Website.
3. **Respostas à Play Console:** tem de responder com precisão às perguntas na Play Console sobre a app e atualizar essas respostas para que reflitam de forma precisa quaisquer alterações a esta. Isto inclui, entre outros, dar respostas exatas sobre a sua app na secção Público-alvo e conteúdo, na Secção segurança dos dados e no Questionário de classificação de conteúdo da IARC (International Age Rating Coalition).
4. **Práticas de dados:** tem de divulgar a recolha de quaisquer informações pessoais e confidenciais sobre crianças na sua app, inclusive através de APIs e SDKs chamados ou usados nesta. As informações confidenciais de crianças incluem, entre outras, informações de autenticação, dados do microfone e do sensor da câmara, dados do dispositivo, ID Android e dados de utilização de anúncios. Além disso, tem de assegurar que a app cumpre as práticas de dados abaixo:
   - As apps destinadas unicamente a crianças não podem transmitir o identificador de publicidade Android (AAID), a série do SIM (Módulo de Identidade do Subscritor), o Número de série da compilação, o BSSID (Identificador do Conjunto de Serviços Básicos), o MAC (Media Access Control), o SSID (Identificador do Conjunto de Serviços), o IMEI (International Mobile Equipment Identity) nem o IMSI (International Mobile Subscriber Identity).
     - As apps apenas destinadas a crianças não devem pedir a autorização AD_ID ao segmentar o nível da API 33 ou superior do Android.
   - As apps destinadas tanto a crianças como a públicos-alvos mais velhos não podem transmitir o AAID, a série do SIM, o Número de série da compilação, o BSSID, o MAC, o SSID, o IMEI nem o IMSI de crianças ou utilizadores de idade desconhecida.
   - O número de telefone do dispositivo não pode ser pedido a partir do TelephonyManager da API Android.
   - As apps destinadas unicamente a crianças não podem pedir autorização de acesso à localização nem recolher, usar e transmitir a localização exata.
   - As apps têm de usar o Gestor de dispositivos associados (CDM) quando pedirem o Bluetooth, exceto se a app se destinar apenas a versões do sistema operativo (SO) do dispositivo não compatíveis com o CDM.
5. **APIs e SDKs:** tem de assegurar que a app implementa corretamente quaisquer APIs e SDKs.

- As apps destinadas unicamente a crianças não podem conter APIs ou SDKs não aprovados para utilização em serviços dirigidos principalmente a crianças.
  - Por exemplo, um serviço de API que use a tecnologia OAuth para autenticação e autorização e cujos termos de utilização indiquem que não está aprovado para utilização em serviços dirigidos a crianças.
- As apps destinadas a crianças e públicos-alvo mais velhos não podem implementar APIs ou SDKs não aprovados para utilização em serviços dirigidos a crianças, exceto se forem usados atrás de um ecrã de idade neutro ou implementados de uma forma que não resulte na recolha de dados de crianças. As apps destinadas tanto a crianças como públicos-alvo mais velhos não podem exigir que os utilizadores acedam ao conteúdo da app através de uma API ou de um SDK não aprovado para utilização em serviços dirigidos a crianças.

6. **Realidade aumentada:** se a app usar a realidade aumentada, tem de incluir um aviso de segurança imediatamente após o lançamento da secção de realidade aumentada. O aviso deve conter o seguinte:
   - Uma mensagem adequada acerca da importância da supervisão parental.
   - Um lembrete para ter cuidado com os perigos físicos no mundo real (por exemplo, ter cuidado com a área envolvente).
   - A app não pode exigir a utilização de um dispositivo não aconselhado para crianças (por exemplo, Daydream ou Oculus).

7. **Apps sociais e funcionalidades:** se as suas apps permitirem que os utilizadores partilhem ou troquem informações, tem de divulgar com precisão estas funcionalidades no questionário de classificação de conteúdo na Play Console.
   - Apps sociais: uma app social é uma app cujo foco principal é permitir que os utilizadores partilhem conteúdos de forma livre ou comuniquem com grandes grupos de pessoas. Todas as apps sociais que incluam crianças no respetivo público-alvo têm de fornecer um lembrete na app para que estas estejam seguras online e conscientes do risco real das interações online antes de as crianças terem autorização para trocarem conteúdos multimédia ou informações de forma livre. Também tem de exigir uma ação de um adulto antes de permitir que as crianças troquem informações pessoais.
   - Funcionalidades sociais: uma funcionalidade social é qualquer funcionalidade adicional da app que permite que os utilizadores partilhem conteúdos de forma livre ou comuniquem com grandes grupos de pessoas. Qualquer app que inclua crianças no respetivo público-alvo e que tenha funcionalidades sociais tem de fornecer um lembrete na app. Este destina-se a garantir que as crianças estão seguras online e que o adulto tem consciência do risco real das interações online antes de autorizar as crianças a trocarem conteúdos multimédia ou informações de forma livre. Também tem de fornecer um método para os adultos gerirem as funcionalidades sociais das crianças, incluindo, entre outros, a ativação/desativação da funcionalidade social ou a seleção de diferentes níveis de funcionalidade. Por último, tem de exigir uma ação de um adulto antes da ativação das funcionalidades que permitem que as crianças troquem informações pessoais.
   - Uma ação de um adulto refere-se a um mecanismo para validar que o utilizador não é uma criança e que não incentiva as crianças a falsificarem a respetiva idade para terem acesso a áreas da sua app concebidas para adultos (ou seja, um PIN, uma palavra-passe, uma data de nascimento, uma validação de email, um ID com foto, um cartão de crédito ou um NISS [número de identificação da segurança social] de um adulto).
   - As apps sociais não devem segmentar crianças se o foco principal das apps for conversar com pessoas que estas não conhecem. Exemplos: apps estilo roleta de chat, apps de encontros, salas de chat abertas e orientadas para crianças, etc.

8. **Conformidade com a lei:** tem de assegurar que a sua app, incluindo quaisquer APIs ou SDKs chamados ou usados por esta, está em conformidade com a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA , o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE e quaisquer outros regulamentos ou leis aplicáveis.

Seguem-se alguns exemplos de violações comuns:

- Apps que promovam jogos para crianças na Ficha da loja, mas cujo conteúdo apenas é adequado para adultos.
- Apps que implementem APIs com termos de utilização que proíbam a respetiva utilização em apps dirigidas a crianças.
- Apps que destaquem o consumo de álcool, tabaco ou substâncias controladas.
- Apps que incluam jogos de azar reais ou simulados.
- Apps que incluam violência, sanguinolência ou conteúdo chocante não adequado para crianças.
- Apps que forneçam serviços de encontros ou ofereçam conselhos sexuais ou matrimoniais.
- Apps que contenham links para Websites que apresentem conteúdo que viola as Políticas do Programa para Programadores do Google Play.
- Apps que mostrem anúncios para adultos (por exemplo, conteúdos violentos, conteúdos de natureza sexual ou conteúdos de jogos de azar) a crianças.

Anúncios e rentabilização

Se estiver a rentabilizar uma app que segmenta crianças no Play, é importante que a sua app cumpra os seguintes requisitos da Política de Rentabilização e Anúncios para Famílias.

As políticas abaixo aplicam-se a todos os tipos de rentabilização e publicidade na app, incluindo anúncios, promoções cruzadas (para as suas apps e apps de terceiros), ofertas de compras na app ou qualquer outro conteúdo comercial (como posicionamentos de produtos pagos). Todos os tipos de rentabilização e publicidade nestas apps têm de estar em conformidade com todas as leis e regulamentos aplicáveis (incluindo quaisquer diretrizes da indústria ou de autorregulação relevantes).

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

Requisitos de anúncios

Se a app apresentar anúncios a crianças ou utilizadores de idade desconhecida, tem de:

- Usar apenas SDKs de anúncios autocertificados para famílias do Google Play para apresentar anúncios a esses utilizadores;
- Assegurar que os anúncios apresentados a esses utilizadores não envolvem publicidade baseada em interesses (publicidade destinada a utilizadores individuais com determinadas caraterísticas com base no respetivo comportamento de navegação online) ou remarketing (publicidade destinada a utilizadores individuais com base na interação anterior com uma app ou um Website);
- Assegurar que os anúncios apresentados a esses utilizadores mostram conteúdo adequado para crianças;
- Assegurar que os anúncios apresentados a esses utilizadores seguem os requisitos de formato de anúncio para famílias; e
- Assegurar a conformidade com todos os regulamentos legais e as normas da indústria aplicáveis relativos à publicidade para crianças.

Requisitos do formato de anúncios

A rentabilização e a publicidade na sua app não podem ter conteúdo fraudulento ou concebido de forma a provocar cliques inadvertidos de utilizadores menores de idade.

Se as crianças forem o único público-alvo da app, é proibido o seguinte. Se as crianças e os públicos-alvo mais velhos forem os públicos-alvo da sua app, é proibido o seguinte ao publicar anúncios para crianças ou utilizadores de idade desconhecida:

- A rentabilização e a publicidade perturbadoras, incluindo a rentabilização e a publicidade que ocupam todo o ecrã ou interferem com a utilização normal e não fornecem um meio claro para ignorar o anúncio (por exemplo, murais de anúncios).

- A rentabilização e a publicidade que interfiram com a utilização normal de apps ou jogos, incluindo anúncios premiados ou de aceitação, que não se podem fechar após 5 segundos.
- A rentabilização e a publicidade que não interfiram com a utilização normal da app ou de jogos podem persistir durante mais de 5 segundos (por exemplo, conteúdo de vídeo com anúncios integrados).
- A rentabilização e a publicidade de anúncios intercalares apresentados imediatamente após o início da app.
- Vários posicionamentos de anúncios numa página (por exemplo, não são permitidos anúncios de faixa que mostrem várias ofertas num posicionamento ou a apresentação de mais do que um anúncio de faixa ou vídeo).
- A rentabilização e a publicidade que não sejam facilmente distinguíveis do conteúdo da app, como as Offerwalls e outras experiências de anúncios envolventes.
- A utilização de táticas chocantes ou emocionalmente manipulativas para incentivar a visualização de anúncios ou as compras na app.
- Anúncios enganadores que forcem o utilizador a clicar através de um botão de ignorar para acionar outro anúncio ou fazendo com que sejam apresentados anúncios de forma repentina em áreas da app em que o utilizador toca normalmente para outra função.
- Não fazer uma distinção entre a utilização de moedas de jogo virtuais e dinheiro real para fazer compras na app.

Seguem-se alguns exemplos de violações comuns:

- A rentabilização e a publicidade que se afastam do dedo do utilizador à medida que este as tenta fechar
- A rentabilização e a publicidade que não fornecem ao utilizador uma forma de sair da oferta após cinco (5) segundos, conforme mostrado no exemplo abaixo:

- A rentabilização e a publicidade que ocupam a maior parte do ecrã do dispositivo sem fornecer ao utilizador uma forma clara de as ignorar, conforme mostrado no exemplo abaixo:

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

- A rentabilização e a publicidade que o utilizador pode confundir com o conteúdo da app, conforme mostrado no exemplo abaixo:

- Botões, anúncios ou outro tipo de rentabilização que promovem as suas outras Fichas da loja do Google Play, mas que não se distinguem do conteúdo da app, conforme mostrado no exemplo

abaixo:

Seguem-se alguns exemplos de conteúdo do anúncio impróprio que não deve apresentar a crianças.

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

SDKs de anúncios

Se publicar anúncios na sua app e o seu público-alvo incluir apenas crianças, tem de usar apenas versões de SDKs de anúncios autocertificados para famílias . Se o público-alvo da sua app incluir tanto crianças como utilizadores mais velhos, tem de implementar medidas de filtragem de idade, como um ecrã de idade neutro , e assegurar que os anúncios apresentados a crianças são provenientes exclusivamente de versões de SDKs de anúncios autocertificados do Google Play.

Consulte a página da Política do Programa de SDKs de Anúncios Autocertificados para Famílias para obter mais detalhes acerca destes requisitos e veja a lista atual de versões de SDKs de anúncios autocertificados para famílias aqui .

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

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

Política de SDKs de Anúncios Autocertificados para Famílias

O Google Play está empenhado na criação de uma experiência segura para as crianças e as famílias. Uma parte fundamental deste processo é ajudar a garantir que as crianças só veem anúncios

adequados para a respetiva idade e que os respetivos dados são processados de forma apropriada. Para alcançar este objetivo, exigimos que as plataformas de mediação e os SDKs de anúncios tenham a autocertificação em como são adequados para crianças e estão em conformidade com as Políticas do Programa para Programadores do Google Play e as Políticas para Famílias do Google Play, incluindo os Requisitos do Programa de SDKs de anúncios autocertificados para famílias.

O Programa de SDKs de anúncios autocertificados para famílias do Google Play é uma forma importante para os programadores identificarem que plataformas de mediação ou SDKs de anúncios têm a autocertificação em como são adequadas para utilização em apps concebidas especificamente para crianças.

A representação fraudulenta de quaisquer informações sobre o seu SDK, incluindo no formulário de interesse da sua candidatura, pode resultar na remoção ou suspensão do seu SDK do Programa de SDKs de anúncios autocertificados para famílias, por isso, é importante fornecer informações exatas.

Requisitos da política

Se o seu SDK ou plataforma de mediação publicar apps que fazem parte do programa Famílias do Google Play, tem de agir em conformidade com todas as Políticas para Programadores do Google Play, incluindo os seguintes requisitos. O incumprimento de quaisquer requisitos da política pode resultar na remoção ou suspensão do Programa de SDKs de anúncios autocertificados para famílias.

É da sua responsabilidade assegurar que o seu SDK ou plataforma de mediação está em conformidade, por isso reveja as Políticas do Programa para Programadores do Google Play, as Políticas para Famílias do Google Play e os requisitos do Programa de SDKs de anúncios autocertificados para famílias.

1. **Conteúdo do anúncio:** o conteúdo do anúncio acessível a crianças tem de ser adequado para as mesmas.
   - Tem de (i) definir o que são comportamentos e conteúdos de anúncios censuráveis e (ii) proibi-los nos termos ou nas políticas. As definições devem estar em conformidade com as Políticas do Programa para Programadores do Google Play.
   - Também tem de criar um método de classificação dos seus criativos de anúncios de acordo com grupos adequados para a idade. Estes grupos devem incluir, no mínimo, grupos para Todos e Adultos. A metodologia de classificação tem de estar em linha com a metodologia que a Google disponibiliza aos SDKs assim que tiverem preenchido o formulário de interesse.
   - Tem de garantir que, quando forem usados lances em tempo real para publicar anúncios para crianças, os criativos foram revistos e estão em conformidade com os requisitos acima.
   - Além disso, tem de ter um mecanismo para identificar visualmente os criativos provenientes do respetivo inventário (por exemplo, adicionar marcas de água ao criativo do anúncio com um logótipo visual da sua empresa ou uma funcionalidade semelhante).
2. **Formato de anúncio:** tem de garantir que todos os anúncios apresentados aos utilizadores menores de idade seguem os Requisitos do formato de anúncio para Famílias e tem de permitir que os programadores selecionem formatos de anúncios que estejam em conformidade com a Política para Famílias do Google Play.
   - A publicidade não pode ter conteúdo fraudulento ou concebido de forma a provocar cliques inadvertidos de utilizadores menores de idade. Não são permitidos anúncios enganadores que forcem o utilizador a clicar através de um botão de ignorar para acionar outro anúncio ou fazendo com que sejam apresentados anúncios de forma repentina em áreas da app em que o utilizador toca normalmente para outra função.
   - Não é permitida publicidade perturbadora, incluindo publicidade que ocupa todo o ecrã ou interfere com a utilização normal e não oferece um meio claro para ignorar o anúncio (por exemplo, murais de anúncios).
   - Tem de ser possível fechar a publicidade que interfira com a utilização normal de apps ou jogos, incluindo anúncios premiados ou de aceitação, após 5 segundos.

- Não são permitidos vários posicionamentos para anúncios numa página. Por exemplo, não são permitidos anúncios de faixa que mostrem várias ofertas num posicionamento nem a apresentação de mais do que um anúncio de faixa ou vídeo.
- A publicidade tem de ser facilmente distinguível do conteúdo da app. Não são permitidas Offerwalls nem experiências de anúncios envolventes que não sejam claramente identificáveis como publicidade pelos utilizadores menores de idade.
- A publicidade não pode usar táticas chocantes nem emocionalmente manipulativas para incentivar a visualização de anúncios.

3. **PBI/remarketing:** tem de garantir que os anúncios apresentados aos utilizadores menores de idade não envolvem publicidade baseada em interesses (publicidade destinada a utilizadores individuais com determinadas caraterísticas com base no respetivo comportamento de navegação online) nem remarketing (publicidade destinada a utilizadores individuais com base na interação anterior com uma app ou um Website).
4. **Práticas de dados:** enquanto fornecedor do SDK, tem de ser transparente no modo como processa os dados do utilizador (por exemplo, as informações recolhidas sobre ou de um utilizador, incluindo as informações do dispositivo). Isso significa divulgar o acesso, a recolha, a utilização e a partilha dos dados do seu SDK e limitar a utilização dos dados às finalidades divulgadas. Estes requisitos do Google Play são adicionais a quaisquer requisitos estabelecidos por leis de privacidade e proteção de dados aplicáveis. Tem de divulgar a recolha de quaisquer informações pessoais e confidenciais de crianças, incluindo, entre outras, informações de autenticação, dados do microfone e do sensor da câmara, dados do dispositivo, ID Android e dados de utilização de anúncios.
   - Tem de permitir que os programadores, por pedido ou app, peçam o tratamento dirigido a crianças para a publicação de anúncios. Este tratamento tem de estar em conformidade com as leis e os regulamentos aplicáveis, como a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA e o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE .
     - O Google Play requer que os SDKs de anúncios desativem anúncios personalizados, publicidade baseada em interesses e remarketing, como parte do tratamento dirigido a crianças.
   - Certifique-se de que, quando forem usados lances em tempo real para publicar anúncios para crianças, os indicadores de privacidade são propagados para os licitadores.
   - Não pode transmitir o AAID, o número de série do SIM, o Número de série da compilação, o BSSID, o MAC, o SSID, o IMEI e/ou o IMSI de crianças ou utilizadores de idade desconhecida.
5. **Plataformas de mediação**: ao publicar anúncios para crianças:
   - Use apenas SDKs de anúncios autocertificados para famílias ou implemente as salvaguardas necessárias para assegurar que todos os anúncios publicados a partir da mediação estão em conformidade com estes requisitos; e
   - Transmita as informações necessárias às plataformas de mediação para indicar a classificação do conteúdo do anúncio e qualquer tratamento dirigido a crianças aplicável.
6. **Autocertificação e conformidade:** tem de facultar à Google informações suficientes, como as informações indicadas no formulário de interesse , para validar a conformidade da política do SDK de anúncios com todos os requisitos de autocertificação, incluindo, entre outros:
   - Facultar uma versão em inglês dos termos de utilização, da política de privacidade e do guia de integração dos publicadores do seu SDK ou plataforma de mediação
   - Enviar uma app de teste de amostra que use a versão em conformidade mais recente do SDK de anúncios. A app de teste de amostra deve ser um APK Android totalmente concluído e executável que usa todas as funcionalidades do SDK. Requisitos da app de teste:
     - Tem de ser enviada como um APK Android totalmente concluído e executável destinado a ser executado num formato de telemóvel.
     - Tem de usar a versão lançada mais recentemente do SDK de anúncios ou uma versão prestes a ser lançada que cumpra as Políticas do Google Play.

- Tem de usar todas as funcionalidades do SDK de anúncios, incluindo chamar o SDK de anúncios para obter e apresentar anúncios.
- Tem de ter acesso total a todos os inventários de anúncios publicados na rede através dos criativos pedidos pela app de teste.
- Não pode ter restrições de geolocalização.
- Se o seu inventário se destinar a um público-alvo misto, a sua app de teste tem de ser capaz de distinguir entre pedidos de criativos de anúncios do inventário completo e do inventário adequado para crianças ou todas as faixas etárias.
- Não pode estar restrita a anúncios específicos no inventário, a menos que seja controlada pelo ecrã de idade neutro.

7. Tem de responder atempadamente a quaisquer pedidos de informação subsequentes e autocertificar-se de que todos os lançamentos de novas versões estão em conformidade com as Políticas do Programa para Programadores do Google Play mais recentes, incluindo os Requisitos da Política para Famílias.
8. **Conformidade com a lei:** os SDKs de anúncios autocertificados para famílias têm de suportar a publicação de anúncios em conformidade com todos os estatutos e regulamentos relevantes no que se refere a crianças que possam ser aplicáveis aos respetivos publicadores.
   - Tem de assegurar que o seu SDK ou plataforma de mediação está em conformidade com a Lei de Proteção à Privacidade da Criança na Internet (COPPA) dos EUA, o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE e quaisquer outros regulamentos ou leis aplicáveis.

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

Consulte a página do Programa de SDKs de anúncios autocertificados para famílias para ver mais detalhes sobre os requisitos do Programa.

Aplicação

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

Abrangência das políticas

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

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

Os termos definidos utilizados nestas políticas têm o mesmo significado que no Contrato de Distribuição para Programadores (DDA). Além de estar em conformidade com estas políticas e o DDA,

o conteúdo da sua app tem de ser classificado de acordo com as nossas Diretrizes de classificação de conteúdo.

Não permitimos apps ou conteúdos de apps que prejudiquem a confiança dos utilizadores no ecossistema do Google Play. Na avaliação da inclusão ou remoção de apps do Google Play, consideramos vários fatores, incluindo, entre outros, um padrão de comportamento prejudicial ou elevado risco de abuso. Identificamos o risco de abuso, incluindo, entre outros, itens como reclamações relativas a apps e programadores específicos, noticiários, histórico de violações anteriores, feedback dos utilizadores e utilização de marcas, personagens e outros recursos populares.

Como funciona o Google Play Protect

O Google Play Protect verifica as apps quando as instala. Além disso, analisa periodicamente o dispositivo. Se encontrar uma app potencialmente prejudicial, poderá:

- Enviar-lhe uma notificação. Para remover a app, toque na notificação e, em seguida, em Desinstalar.
- Desativar a app até a desinstalar.
- Remover a app automaticamente. Na maioria dos casos, se for detetada uma app prejudicial, recebe uma notificação a indicar que esta foi removida.

Como funciona a proteção contra software malicioso

Para assegurar a sua proteção contra software de terceiros e URLs maliciosos, assim como outros problemas de segurança, a Google pode receber informações sobre:

- As ligações de rede do seu dispositivo.
- URLs potencialmente prejudiciais.
- O sistema operativo e as apps instaladas no seu dispositivo através do Google Play ou de outras fontes.

Pode receber um aviso da Google sobre uma app ou um URL que podem não ser seguros. A Google pode remover a app ou o URL ou bloquear a instalação dos mesmos se forem conhecidos por serem prejudiciais para os dispositivos, os dados ou os utilizadores.

Pode optar por desativar algumas destas proteções nas definições do dispositivo. No entanto, a Google pode continuar a receber informações sobre as apps instaladas através do Google Play. Além disso, as apps instaladas no dispositivo a partir de outras origens podem continuar a ser verificadas para detetar problemas de segurança sem enviar informações à Google.

Como funcionam os alertas de privacidade

Se uma app for removida da Google Play Store porque pode aceder às suas informações pessoais, o Google Play Protect envia-lhe um alerta e dá-lhe a opção de a desinstalar.

Processo de aplicação

Quando revemos conteúdos ou contas para determinar se são ilegais ou violam as nossas políticas, temos em consideração várias informações para tomar uma decisão, incluindo os metadados da app (por exemplo, o título e a descrição da app), a experiência na app, as informações da conta (por exemplo, histórico de violações de políticas anteriores), código de terceiros nas apps e outras informações facultadas através de mecanismos de denúncia (quando aplicável) e de revisões internas realizadas por iniciativa própria. Tenha em atenção que é responsável por garantir que qualquer código de terceiros (por exemplo, um SDK) usado na sua app e as práticas desses terceiros relativamente à sua app estão em conformidade com todas as Políticas do Programa para Programadores do Google Play.

Se a sua app ou conta de programador violar alguma das nossas políticas, iremos tomar as medidas adequadas, conforme descrito abaixo. Além disso, iremos fornecer-lhe informações relevantes por email acerca da ação que tomámos, bem como instruções sobre como recorrer se considerar que tomámos medidas por engano.

Tenha em atenção que os avisos de remoção ou administrativos podem não indicar absolutamente todas as violações de políticas existentes na sua conta, app ou catálogo de apps mais abrangente. Os programadores são responsáveis por solucionar qualquer problema relativo às políticas e por aplicar as devidas diligências adicionais para garantir que o restante da app ou conta está totalmente em conformidade com as políticas. Se as violações de políticas não forem solucionadas na sua conta e em todas as suas apps, podem ser tomadas ações de aplicação adicionais.

Violações repetidas ou graves (como software malicioso, fraude e apps que possam provocar danos no dispositivo ou prejuízos para o utilizador) destas políticas ou do Contrato de Distribuição para Programadores (DDA) resultam no encerramento de contas de programador do Google Play individuais ou relacionadas.

Medidas de aplicação

Existem diversas medidas de aplicação que podem afetar as apps de várias formas. Usamos uma combinação de avaliação humana e automática para rever as apps e o conteúdo destas, de modo a detetar e avaliar conteúdo que viole as nossas políticas e seja prejudicial para os utilizadores e o ecossistema do Google Play em geral. A utilização de modelos automáticos ajuda-nos a detetar mais violações e avaliar potenciais problemas mais rapidamente, o que ajuda a manter o Google Play seguro para todas as pessoas. O conteúdo que viole as políticas é removido pelos nossos modelos automáticos ou, se for necessária uma determinação mais diferenciada, sinalizado para uma revisão mais aprofundada por operadores e analistas com formação para realizarem avaliações de conteúdo. Esta revisão mais detalhada pode ser necessária, por exemplo, para a compreensão do contexto do conteúdo em questão. Os resultados destas revisões manuais são depois usados para ajudar a compilar dados de preparação, de modo a melhorar ainda mais os nossos modelos de aprendizagem automática.

A secção seguinte descreve as várias medidas que o Google Play pode tomar e o impacto na sua app e/ou conta de programador do Google Play.

Salvo indicação em contrário numa comunicação de aplicação, estas ações afetam todas as regiões. Por exemplo, se a sua app for suspensa, fica indisponível em todas as regiões. Além disso, salvo indicação em contrário, estas ações permanecem em vigor, a não ser que recorra da ação e o recurso seja deferido.

Rejeição

- Uma nova app ou atualização da app enviada para revisão não será disponibilizada no Google Play.
- Se for rejeitada uma atualização de uma app existente, a versão da app publicada antes da atualização permanece disponível no Google Play.
- As rejeições não afetam o seu acesso a instalações, estatísticas e classificações de utilizadores existentes de uma app rejeitada.
- As rejeições não têm impacto na conformidade da sua conta de programador do Google Play.

Nota: não tente reenviar uma app rejeitada até ter corrigido todas as violações de políticas.

Remoção

- A app e quaisquer versões anteriores desta são removidas do Google Play e deixam de estar disponíveis para transferência pelos utilizadores.
- Uma vez que a app é removida, os utilizadores não vão poder ver a respetiva Ficha da loja. Estas informações serão restauradas assim que enviar uma atualização em conformidade com a política

para a app removida.
- Os utilizadores podem não conseguir fazer compras na app ou usar funcionalidades de faturação na app até que uma versão em conformidade com a política seja aprovada pelo Google Play.
- As remoções não têm impacto imediato na conformidade da sua conta de programador do Google Play, mas várias remoções podem resultar numa suspensão.

Nota: não tente publicar novamente uma app removida até ter corrigido todas as violações de políticas.

Suspensão

- A app e quaisquer versões anteriores desta são removidas do Google Play e deixam de estar disponíveis para transferência pelos utilizadores.
- A suspensão pode ocorrer como resultado de várias violações de políticas ou violações extremamente graves, bem como rejeições ou remoções de apps repetidas.
- Uma vez que a app é suspensa, os utilizadores não vão poder ver a Ficha da loja desta.
- Deixa de poder utilizar o APK ou o app bundle de uma app suspensa.
- Os utilizadores não vão poder fazer compras na app nem utilizar funcionalidades de faturação na app.
- As suspensões contam como advertências relativamente à conformidade da sua conta de programador do Google Play. Várias advertências podem resultar no encerramento de contas de programador do Google Play individuais e relacionadas.

Visibilidade limitada

- A deteção da sua app no Google Play é restrita. A sua app permanece disponível no Google Play e os utilizadores podem aceder-lhe com um link direto para a Ficha da loja da app.
- Colocar a app num estado de Visibilidade limitada não afeta a conformidade da sua conta de programador do Google Play.
- Colocar a app num estado de Visibilidade limitada não afeta a capacidade de os utilizadores verem a Ficha da loja existente da app.

Regiões limitadas

- A sua app só pode ser transferida por utilizadores através do Google Play em determinadas regiões.
- Os utilizadores de outras regiões não conseguirão encontrar a app na Play Store.
- Os utilizadores que instalaram anteriormente a app podem continuar a utilizá-la no respetivo dispositivo, mas deixarão de receber atualizações.
- A limitação regional não têm impacto na conformidade da sua conta de programador do Google Play.

Estado restrito da conta

- Quando a sua conta de programador está num estado restrito, todas as apps no seu catálogo são removidas do Google Play e deixa de poder publicar novas apps ou de voltar a publicar apps existentes. Continua a poder aceder à Play Console.
- Uma vez que todas as apps são removidas, os utilizadores não vão poder ver a Ficha da loja da sua app nem o seu Perfil do programador.
- Os seus utilizadores atuais não vão poder fazer compras na app nem usar nenhuma das funcionalidades da Faturação em apps das suas apps.
- Ainda pode usar a Play Console para facultar mais informações ao Google Play e alterar as informações da sua conta.
- Vai poder publicar as suas apps novamente quando tiver corrigido todas as violações de políticas.

Encerramento da conta

- Quando a sua conta de programador é encerrada, todas as apps no seu catálogo são removidas do Google Play e deixa de poder publicar novas apps. Isto também significa que quaisquer contas de programador do Google Play relacionadas são igualmente suspensas de forma permanente.
- Várias suspensões ou suspensões devido a violações graves de políticas podem resultar no encerramento da sua conta da Play Console.
- Uma vez que as apps na conta encerrada são removidas, os utilizadores não vão poder ver as respetivas Fichas da loja nem o seu Perfil do programador.
- Os seus utilizadores atuais não vão poder fazer compras na app nem usar nenhuma das funcionalidades da Faturação em apps das suas apps.

Nota: qualquer nova conta que tente abrir também será encerrada (sem reembolso da taxa de registo de programador) e, por isso, não deve tentar registar uma nova conta da Play Console enquanto uma das suas outras contas estiver encerrada.

Contas inativas

As contas inativas são contas de programador que estão inativas ou abandonadas. As contas inativas não estão em conformidade com o Contrato de Distribuição para Programadores .

As contas de programador do Google Play destinam-se a programadores ativos que publicam e mantêm apps de forma ativa. Para prevenir abusos, encerramos contas que estão inativas, que não são usadas ou com as quais não há interação regular (por exemplo, para publicar e atualizar apps, aceder a estatísticas ou gerir Fichas da loja).

O encerramento de uma conta inativa elimina a sua conta e todos os dados associados a esta. A sua taxa de registo não é reembolsável e será perdida. Antes de encerrarmos a sua conta inativa, enviar-lhe-emos uma notificação através das informações de contacto que forneceu para essa conta.

O encerramento de uma conta inativa não limita a sua capacidade de criar uma nova conta no futuro, se decidir publicar no Google Play. Não vai poder reativar a sua conta e dados ou apps anteriores não vão estar disponíveis numa nova conta.

Gestão e denúncia de violações de políticas

Recorrer de uma medida de aplicação

Procedemos à reposição de apps se tiver sido cometido um erro e considerarmos que a sua aplicação não viola as Políticas do Programa e o Contrato de Distribuição para Programadores do Google Play. Se reviu cuidadosamente as políticas e considera que a nossa decisão pode estar errada, siga as instruções incluídas na notificação por email relativa à aplicação ou clique aqui para recorrer da decisão.

Recursos adicionais

Para obter mais informações relativamente a uma medida de aplicação ou um comentário/uma classificação de um utilizador, pode consultar alguns dos recursos abaixo ou contactar-nos através do Centro de Ajuda do Google Play. No entanto, não lhe podemos disponibilizar aconselhamento legal. Se necessitar de aconselhamento legal, deve contactar o seu consultor jurídico.

- Verificação de apps
- Denuncie a violação de uma política
- Contacte o Google Play acerca do encerramento de uma conta ou da remoção de uma app
- Avisos cordiais
- Denuncie apps e comentários impróprios

- A minha app foi removida do Google Play
- Compreender o encerramento de contas de programador do Google Play

---

Requisitos da Play Console

Para garantir a segurança do nosso ecossistema de apps dinâmico, o Google Play exige que todos os programadores cumpram os requisitos da Play Console, incluindo quaisquer perfis associados à sua conta de programador da Play Console. As informações validadas vão ser apresentadas no Google Play para ajudar os utilizadores a criar confiança junto dos programadores. Saiba mais sobre as informações apresentadas no Google Play.

O Google Play oferece dois tipos de contas de programador: pessoal e de organização. Selecionar o tipo de conta de programador correto e concluir as validações necessárias é fundamental para uma experiência de integração sem problemas. Saiba como escolher um tipo de conta de programador.

Quando criar a sua conta da Play Console, os programadores que fornecem os seguintes serviços têm de se registar como uma organização:

- Produtos e serviços financeiros, incluindo, entre outros, serviços bancários, empréstimos, negociação de ações, fundos de investimento, software de carteira para criptomoedas e câmbios de criptomoedas. Saiba mais sobre a Política de Serviços Financeiros.
- Apps de saúde, como apps médicas e apps de investigação em seres humanos. Saiba mais sobre as categorias de apps de saúde.
- Apps com aprovação para usar a classe VpnService . Saiba mais sobre a Política do Serviço VPN.
- Apps governamentais, incluindo apps desenvolvidas por ou em nome de um organismo governamental.

Depois de selecionar um tipo de conta, é necessário:

- Fornecer de forma precisa as informações da sua conta de programador, incluindo os seguintes detalhes:
  - Nome legal e morada
  - Número DUNS , caso se registe como organização
  - Endereço de email e número de telefone de contacto
  - Endereço de email e número de telefone do programador apresentados no Google Play, quando aplicável
  - Métodos de pagamento, quando aplicável
  - Perfil de pagamentos Google associado à sua conta de programador
- Se se registar como organização, certifique-se de que as informações da sua conta de programador estão atualizadas e são coerentes com os detalhes armazenados no seu perfil da Dun & Bradstreet

Antes de enviar a sua app, tem de:

- Fornecer de forma precisa todas as informações e os metadados da app
- Carregar a Política de Privacidade da app e preencher os requisitos da Secção segurança dos dados
- Fornecer uma conta de demonstração ativa, as informações de início de sessão e todos os outros recursos necessários para o Google Play rever a sua app (especificamente, credenciais de início de sessão, código QR, etc.)

Como sempre, deve certificar-se de que a sua app oferece uma experiência do utilizador estável, apelativa e adaptável; confirmar se todos os elementos da app, incluindo as redes de publicidade, os serviços de estatísticas e os SDKs de terceiros, estão em conformidade com as Políticas do Programa para Programadores do Google Play; e, se o público-alvo da app incluir crianças, certificar-se de que está em conformidade com a nossa Política para Famílias.

É importante não esquecer que lhe cabe a responsabilidade de analisar o Contrato de Distribuição para Programadores e todas as Políticas do Programa para Programadores para garantir que a sua app está em plena conformidade.

Developer Distribution Agreement

Precisa de mais ajuda?

Experimente estes passos seguintes:

Postar na Comunidade de Ajuda

Receber respostas dos membros da comunidade

Contacte-nos

Forneça-nos mais informações e iremos ajudá-lo a encontrar o que procura.