

[Continue](#)







What is the latest android version for nexus 7. Asus nexus 7 tablet android update. How to update nexus 7 to android 10. Update nexus 7 tablet to android 10.

Android Versão do sistema operativo Unix; Linux Tela inicial do Android 13 Produção Google LLCOpen Handset Alliance Linguagem Java (UI), C (núcleo), C++, Rust,[1] entre outras[2] Modelo Código aberto com aplicações com software de código fechado[3][4] Lançamento 23 de setembro de 2008 (13 anos) Versão estável 13.015 de agosto de 2022; há 19 dias Mercado-alvo Dispositivos móveis Idioma(s) Multilinguagem (63 idiomas) Método de atualização Over the Air Arquiteturas) ARM, MIPS[5], Power[6], x86[7], x64[8] Gestão de pacotes APK, Google Play Núcleo Monolítico (núcleo Linux modificado) Interface Gráfico Licença Apache 2.0, patches do kernel Linux estão sob a GPL v2[9] Página oficial www.android.com Estado de desenvolvimento Ativo Android é um sistema operacional (SO) baseado no núcleo Linux, desenvolvido por um consórcio de desenvolvedores conhecido como Open Handset Alliance, sendo o principal colaborador o Google.[10] Com uma interface de usuário baseada na manipulação direta, o Android é projetado principalmente para dispositivos móveis com tela sensível ao toque como smartphones e tablets; com interface específica para TV (Android TV), carros (Android Auto) e relógios inteligentes (Wear OS). O sistema operacional utiliza-se da tela sensível ao toque para que o usuário possa manipular objetos virtuais, assim como um teclado virtual. Apesar de ser principalmente utilizado em dispositivos com tela sensível ao toque, também é utilizado em consoles de videogames,[11] câmeras digitais,[12] computadores[13] e outros dispositivos eletrônicos. O Android é o sistema operacional móvel mais utilizado do mundo, e, em 2013, possuía a maior percentagem das vendas mundiais de SO móveis.[14] Dispositivos com o sistema Android vendem mais que eletrônicos com Windows, iOS e macOS combinados.[15][16][17][18] com vendas em 2012, 2013 e 2014[19] perto da base de computadores do mundo.[20] Em 2021, a loja de aplicativos Google Play Store possui mais de 2 milhões de aplicativos disponíveis.[21] Uma pesquisa com programadores entre abril e maio de 2013 revelou que 71% dos programadores para sistemas móveis desenvolviam para o Android.[22] Na conferência anual Google I/O de 2014, a companhia revelou que existem mais de 1 bilhão de usuários Android ativos. Em junho de 2013, este número era de 538 milhões.[23] O maior número de usuários no mundo também reflete no número de ataques de hackers no sistema, com cerca de 5 mil novos malwares sendo criados todos os dias para usuários Android.[24] O código do sistema operacional é disponibilizado pelo Google sob licença de código aberto, apesar de a maior parte dos dispositivos ser lançada com uma combinação de software livre e software privado.

[25] Inicialmente foi desenvolvido pela empresa Android, Inc., a qual o Google dava suporte financeiramente. Foi adquirida pelo Google em 2005[26] e revelado em 2007 junto com a fundação da Open Handset Alliance — consórcio entre empresas de hardware, software e telecomunicações com o intuito de desenvolver a indústria de dispositivos móveis.[27] O Android é muito popular entre empresas de tecnologia que buscam um software pronto, de baixo custo e personalizável para dispositivos de alta tecnologia.[28] A natureza do software de código aberto do sistema operacional tem encorajado uma grande comunidade de programadores e entusiastas a colocar uma fundação para o desenvolvimento de projetos feitos pela própria comunidade que adicionam recursos para usuários mais avançados,[29] ou trazem o Android para dispositivos que inicialmente não foram lançados com a plataforma. O sucesso do SO fez dele um alvo para disputas de patente na chamada "guerra de smartphones" entre empresas de tecnologia. A versão mais recente é o Android 13, lançado em 15 de agosto de 2022.[30][31][32] Uma das novas funções do Android 13 é a possibilidade de limitar o acesso de aplicativos à mídias como fotos, vídeos e áudios. Outra característica desse sistema é o Bluetooth Low Energy (LE), que, além de reduzir o delay nas reproduções via bluetooth[33], diminui o consumo da bateria em 10%.[34] História Android, Inc. foi fundada em Palo Alto, Califórnia em outubro de 2003 por Andy Rubin (cofundador da Danger),[35] Rich Miner (cofundador da Wildfire Communications, Inc.),[36] Nick Sears (ex-vice-presidente da T-Mobile),[37] e Chris White (encabeço o projeto de desenvolvimento de design e interface da WebTV)[26] para desenvolver, segundo o Rubin, “dispositivos móveis mais inteligentes que estejam mais cientes das preferências e da localização do seu dono”.[26] As primeiras intenções da empresa eram de desenvolver um sistema operacional avançado para câmeras digitais, quando se deram conta de que o mercado destes dispositivos não era grande o suficiente. Desviaram então seus esforços para produzir um sistema operacional móvel para ser rival aos Symbian e Windows Mobile.[38] Apesar daquelas últimas conquistas dos fundadores e primeiros empregados, Android Inc. entrou secretamente, revelando somente que estava trabalhando em um software para smartphones.[26] Naquele mesmo ano Andy Rubin ficou financeiramente escasso. Steve Pearlman, amigo íntimo de Rubin, entregou a ele dez mil dólares em um envelope e recousou sua parte na companhia.[39] O Google adquiriu Android Inc. em 17 de agosto de 2005; funcionários-chave da recém-comprada empresa, incluindo Rubin, Miner e White, continuaram na companhia após a aquisição.[26] Pouco se sabia sobre a Android Inc. naquele momento, mas muitos especularam que o Google estava planejando entrar no mercado de dispositivos móveis com essa jogada.[26] Dentro do Google, o grupo liderado por Rubin desenvolveu um sistema operacional móvel tendo com base o Kernel Linux. A empresa comercializou o Android persuadindo empresas fabricantes de celular e operadoras com a promessa de prover um sistema flexível e atualizável. O Google firmou parcerias com empresas fabricantes de hardware, software e operadores de telefonia móvel e reaffirmou que estaria aberta a mútuas cooperações.[40][41][42] A especulação sobre a intenção do Google de entrar no mercado de dispositivos móveis continuou até dezembro de 2006.[43] Um protótipo inicial de codinome “Sooner” tinha um aspecto parecido com um telefone BlackBerry, sem touchscreen e um teclado físico QWERTY, mas foi redesenhado para suportar visores touchscreen para competir com outros dispositivos recém-anunciados como o LG Prada (2006) e o iPhone da Apple (2007).[44][45] Em setembro de 2007, InformationWeek, revista digital americana, cobriu um estudo da EvaluateServe que revelou diversas patentes feitas pelo Google na área de tecnologia móvel.[46][47] Lançado em setembro de 2008, o HTC Dream foi o primeiro dispositivo comercial com o sistema Android. Em 5 de novembro de 2007 a Open Handset Alliance, consórcio de tecnologia entre empresas do ramo, incluindo Google, fabricantes de telefones como HTC, Sony e Samsung, operadoras de telefonia como Sprint Nextel e T-Mobile e fabricantes de chipsets como Qualcomm e a Texas Instruments se revelaram com o objetivo de criar uma plataforma de padrão aberto para dispositivos móveis.[27] Naquele dia o Android foi revelado como seu primeiro produto: uma plataforma móvel construída no Kernel Linux de versão 2.6.25.[27] O primeiro smarphone disponível comercialmente rodando o Android foi o HTC Dream, lançado em 22 de outubro de 2008.[48] Eric Schmidt, Andy Rubin, e Hugo Barra na coletiva de imprensa para o lançamento do tablet do Google Nexus 7. Em 2010 o Google apresentou sua série de dispositivos Nexus — uma linha de smartphones e tablets rodando o sistema Android e sendo fabricado por empresas parceiras. HTC colaborou com o Google para lançar o primeiro smartphone Nexus, (atualmente Pixel)[49] o Nexus One. Desde então o Google tem atualizado sua linha com novos dispositivos como, por exemplo, o Nexus 5, feito pela LG e o Nexus 7, feito pela Asus. O Google tem como objetivo através dos lançamentos Nexus mostrar as últimas atualizações de software e hardware do Android, sendo estes dispositivos tidos como carros-chefes do Android. No dia 13 de março de 2013, Larry Page, CEO e fundador do Google, anunciou em um post no seu blog que Andy Rubin foi realocado dentro do Google, sendo portanto da divisão do Android.[50] Ele foi substituído por Sundar Pichai, o qual também continua com seu papel como chefe da divisão Chrome do Google.[51] A qual desenvolve o Chrome OS. Desde 2008 o Android tem recebido inúmeras atualizações que incrementaram substancialmente o sistema, adicionando novas funcionalidades e consertando erros de versões anteriores. A cada grande atualização o codinome do sistema muda, em ordem alfabética, entre nomes de doces.[52][53] De 2010 até 2013 Hugo Barra, brasileiro funcionário do Google, foi o porta-voz oficial do grupo de programadores do Android, representando o Android nas conferências de imprensa e na Google I/O, evento do Google para programadores. O envolvimento de Hugo Barra no desenvolvimento do Android inclui e abrange todo o ecossistema do sistema operacional. Hugo Barra saiu do grupo de desenvolvimento do Android para trabalhar na fabricante de smartphones chinesa Xiaomi.[54][55][56] Características Interface As notificações são acessadas deslizando-se a barra do topo para baixo; notificações podem ser dispensadas individualmente simplesmente deslizando-as para o lado, e podem conter ainda funções adicionais, como retornar chamada e enviar mensagens. A interface padrão do usuário no Android é baseada na manipulação direta.[57] A resposta para a manipulação é desenhada para ser imediata e produzir uma sensação de fluidez, utilizando-se constantemente da resposta háptica para informar o usuário sobre a conclusão do comando. Hardwares internos como acelerômetros, giroscópios e sensores de proximidade[58] são utilizados por alguns aplicativos para responder à ações adicionais do usuário, como por exemplo a mudança da orientação da tela de retrato para paisagem, dependendo de como o dispositivo é separado ou o controle de jogos automotivos somente pela rotação do smartphone, como se fosse um volante de carro.[59] Dispositivos Androd são direcionados à tela inicial ou homescreen assim que são ligados. Lá se encontra a navegação primária e principal do sistema, a qual é similar ao conceito de desktop utilizado em computadores. São tipicamente compostas por ícones de aplicativos instalados e widgets. Os ícones, quando selecionados, direcionam o usuário ao aplicativo correspondente, enquanto o widget mostra na própria tela inicial as informações, atualizando constantemente seu conteúdo, como previsão do tempo, emails não lidos ou notícias.[60] A tela inicial pode ser composta de várias páginas, as quais o usuário por ir para frente ou para trás, sendo ela também altamente customizável, permitindo o usuário ajustar o design de acordo com preferências pessoais.[61] Aplicativos de terceiros disponíveis na loja Google Play ou em outras lojas virtuais podem remodelar extensivamente a tela inicial do Android, e até mesmo imitar a interface dos outros sistemas operacionais como Windows Phone e iOS.[62] A maioria das fabricantes e algumas operadoras de telefonia customizam o visual do sistema para se destacar de seus concorrentes.[63] Presente no topo da tela está a status bar ou barra de status, a qual mostra informações sobre o dispositivo e sua conectividade. Esta barra pode ser puxada para baixo para mostrar a tela de notificações onde aplicativos mostram importantes informações ou atualizações, como um novo email ou um novo SMS, enquanto não atrapalha a atividade que o usuário esteja fazendo no momento.[64] As notificações são persistentes e não saem da tela de notificações a não ser que o usuário leia, clicando na notificação, ou a dispense, deslizando-a para o lado. A partir do Android 4.1, as notificações passaram a poder ser expandidas, mostrando mais informações ou podendo ter alguma interatividade, sendo por exemplo um player de música pode exibir suas funções de voltar, pausar e avançar na música, enquanto uma notificação de chamada perdida pode mostrar a opção de retornar a ligação.[65] O Android possui também a possibilidade de rodar aplicativos que mudam o iniciador padrão. Essas mudanças incluem colocar várias páginas no dock ou retrair o mesmo, e outras muitas mudanças que atingem diretamente a experiência do usuário com o sistema.[66] Aplicativos Aplicativos ou apps que estendem funcionalidades dos dispositivos são desenvolvidos principalmente na linguagem Java.[67] usando-se do sistema de desenvolvimento do software Android (SDK). O SDK inclui um compreensivo conjunto de ferramentas de desenvolvimento,[68] que incluem um depurador, uma biblioteca (computação), um emulador baseado em QEMU, documentação, códigos de exemplos e tutoriais. O ambiente de desenvolvimento integrado ou Ambiente de desenvolvimento integrado oficialmente suportado é o Eclipse utilizando o plugin do Android (ADT). Outras ferramentas de desenvolvimento estão disponíveis, como o Kit de Desenvolvimento Nativo para aplicativos ou extensões em C ou C++, o Google App Inventor, um ambiente de desenvolvimento para novos desenvolvedores, e múltiplas plataformas de desenvolvimento cross-plataform.[69] O Android tem crescido na quantidade de aplicativos de terceiros desenvolvidos para o sistema. Tais aplicativos podem ser adquiridos por usuários através do download e instalação do arquivo APK ou através do download utilizando-se de um programa de alguma loja de aplicativos virtual. Play Store é a loja primária dos usuários do Android. A Google Play Store permite ao usuário do Android navegar, comprar, baixar e atualizar aplicativos desenvolvidos ou pelo Google ou por terceiros. Em julho de 2013 a loja atingiu a marca de 1 milhão de aplicativos disponíveis.[70] Em maio de 2013, 48 bilhões de aplicativos haviam sido instalados a partir do Google Play[71] e em julho do mesmo ano esse número era de 50 bilhões.[72][73] Algumas operadoras de telefonia nos Estados Unidos oferecem uma conta conjunta da Google Play Store, onde os gastos na loja virtual vêm na conta de telefone mensal do usuário.[74] Devido à natureza aberta do Android, há também um alto número de aplicativos de lojas de terceiros, tanto para disponibilizar aplicativos para dispositivos não permitidos na Play Store, quanto para colocar à disposição aplicativos não permitidos na loja, ou aplicativos que burlam o sistema de pagamento do Google, fazendo que saiam de graça para o usuário.[75][76] [77] Os aparelhos Android possuem aplicativos pré-instalados, entre eles estão Google, Google Chrome, YouTube e Google Maps. Já aparelhos que precisam usar mais serviços do Google, tem instalados aplicativos como Gboard (teclado), Gerenciamento de Memória Já que dispositivos Android são normalmente movidos à bateria, o sistema foi desenvolvido para gerir a quantidade de memória (RAM) com o intuito de deixar a quantidade de memória gasta no mínimo, em contraste com desktops em que normalmente sistemas assumem estar conectados à fontes ilimitadas de eletricidade doméstica. Quando um aplicativo não está mais sendo usado, o sistema automaticamente o suspende da memória; enquanto a aplicação está tecnicamente “aberta”, aplicações suspensas não consomem nenhum recurso do sistema. Isso traz um benefício duplo, já que aumenta a responsividade do sistema, enquanto também não consome energia sem necessidade.[78][79] O Android gere aplicações na memória automaticamente: quando a memória está baixa, o sistema começa a “matar” aplicativos e processos que estão inativos há determinado tempo. Este processo é feito para ser invisível ao usuário, então ele não precisa administrar o sistema ou fechar processos por si mesmo.[80][81] Porém, a confusão sobre a regulação de memória no Android resultou que aplicativos de terceiros que gerem a memória ficaram famosos na Google Play Store; estes aplicativos são geralmente tidos como ineficazes, fazendo mais mal do que bem.[82] Quando o Android 5.0 foi lançado, um problema com o gerenciamento de memória fez com que muitos aparelhos sofressem com vazamento de memória, onde o sistema utilizava a memória, porém não conseguia liberá-la para outros aplicativos utilizarem, chegando a um ponto crítico onde o funcionamento do sistema estava comprometido, sendo necessário reiniciá-lo frequentemente.[83] O Google corrigiu o vazamento da versão 5.0, porém, outros vazamentos múltiplos foram detectados, como, por exemplo, na versão 5.0.1.[84] Hardware Samsung Galaxy, comercial com o sistema Android. A principal plataforma para o sistema Android é a Arquitetura ARM (ARMv7 ou posterior; Android 5.0 também dá suporte a ARMv6-A), com a arquitetura x86 e MIPS também oficialmente suportados. Tanto a variante 64-bit quanto a 32-bit das 3 arquiteturas possuem suporte desde o Android 5.0,[85] Desde 2012, os dispositivos Intel começaram a surgir no mercado em smartphones e tablets.[86] Para o Android 4.4, o Google recomenda no mínimo 512 MB de memória RAM.[87] enquanto para dispositivos que não consomem tanta memória, os chamados low-ram devices, o mínimo é 340 MB.[88] Também é necessário dar suporte à tecnologia OpenGL ES 2.0.[89] Possui também suporte à OpenGL ES 1.1, 2.0, 3.0 e 3.1, sendo que alguns aplicativos requerem explicitamente algumas dessas versões. Dispositivos Android incorporam muitos hardwares opcionais, que incluem câmeras, GPS, sensores de orientação, controles específicos para jogos, acelerômetros, giroscópios, harômetros, magnetômetros, sensores de proximidade, termômetros, e telas touchscreen. Alguns componentes não são obrigatórios, mas se tornaram padrão em certos dispositivos como smartphones. Alguns componentes eram obrigatórios no início, mas foram deixados de lado posteriormente. Por exemplo, enquanto o Android OS era desenvolvido primariamente para ser um sistema de telefones, hardwares como microfones eram obrigatórios, mas com o passar do tempo a função de telefone se tornou opcional, e o microfone também.[73] O Android também pode rodar nativamente em um computador, utilizando mouse e teclado.[90][91][92] em versões do Android, originalmente aquelas posteriores ao 4.4.[93] Empresas chinesas estão fabricando PCs com o sistema operacional móvel baseado em Android, para “competir diretamente com o Windows da Microsoft e o Android do Google”.[94] A Academia Chinesa de Engenharia revelou que “mais de uma dúzia” de companhias estavam customizando o Android, seguindo o banimento do Windows 8 dos PCs do governo chinês.[95][96][97] Desenvolvimento Arquitetura do Android. O SO móvel Android era desenvolvido em segredo pelo Google até a última das modificações, quando estaria pronto para ser lançado. Desde 2014, porém, o Google lança versões betas e disponibiliza o código com alguns meses de antecendência ao lançamento, para encontrar bugs antes da versão final. Então, o código é lançado publicamente e oficialmente.[98] O código só funcionará sem modificações em determinados aparelhos, como a da série Nexus e da linha Pixel. O código é então adaptado a cada fabricante para que rode nos hardwares específicos, com ou sem modificações.[99] O banco verde que representa o Android foi desenhado para o Google em 2007 pelo designer gráfico Irina Blok. Ao grupo de design responsável pela arte do símbolo foi dada a tarefa de criar um ícone universalmente identificável, com a especifica inclusão de um robô no design final. Após inúmeras tentativas de robô baseado em ficção-científica e filmes que se passam no espaço, a equipe eventualmente buscou inspiração no símbolo humano em portas de banheiros e modificou-o para a forma de um robô. Como o Androd é aberto (open-source), foi concordado que o símbolo e o robô também deveriam ser livres de licença, desde então o logo do robô verde tem sido reinterpretado em incontáveis variações do seu design original.[100] Seu nome é BugDroid,[101] Calendário de Atualizações O Google lança atualizações de grande porte a cada 6 a 12 meses, as quais a maioria dos dispositivos é capaz de receber através do ar (OTA).[102] A última grande atualização lançada é o Android 11. Comparado com o principal rival do Android, o iOS, as atualizações do Android são geralmente lentas para chegar à maioria dos dispositivos. Para dispositivos que não estão sob a marca Pixel, a atualização para a versão mais recente demora meses a partir da data de lançamento oficial.[103] Isso se deve parcialmente à extensa variação de hardware de dispositivos Android, aos quais a atualização deve ser especificamente modificada, de acordo com cada aparelho, já que o código puro somente roda em dispositivos Nexus.[103] Portar o Android para hardwares específicos consome tempo e dinheiro para diversas fabricantes, que acabam priorizando os dispositivos mais recentes em detrimento dos mais antigos. É comum que smartphones mais velhos não sejam atualizados, mesmo tendo hardware capaz de rodar a nova versão, já que a empresa pode decidir que não vale a pena. O problema se agrava quando as fabricantes customizam o sistema com seus apps e interface, que acabam tendo que ser reaplicados a cada dispositivo a cada atualização. A demora pode se agravar mais ainda se houver também interferência de operadoras nos dispositivos, que também customizam com seus aplicativos e interface própria.[103] A falta de suporte pós-venta de operadoras e fabricantes tem sido amplamente criticada por grupos de consumidores e pela mídia de tecnologia.[104][105] Alguns especialistas em tecnologia têm dito que a indústria de smartphones não consegue pagar o suficiente para atualizar seus dispositivos.[106] Já que isso traria um incentivo às pessoas a comprar novos produtos.[107] uma atitude descrita por alguns como “insultante”.[105] O The Guardian, jornal britânico, queixou-se de que o método de distribuição de atualizações é complicado e filmes que se passam no espaço, a equipe eventualmente buscou inspiração no símbolo humano em portas de banheiros e modificou-o para a forma de um robô. Como o Android é aberto (open-source), foi concordado que o símbolo e o robô também deveriam ser livres de licença, desde então o logo do robô verde tem sido reinterpretado em incontáveis variações do seu design original.[100] Seu nome é BugDroid,[101] Calendário de Atualizações O Google lança atualizações de grande porte a cada 6 a 12 meses, as quais a maioria dos dispositivos é capaz de receber através do ar (OTA).[102] A última grande atualização lançada é o Android 11. Comparado com o principal rival do Android, o iOS, as atualizações do Android são geralmente lentas para chegar à maioria dos dispositivos. Para dispositivos que não estão sob a marca Pixel, a atualização para a versão mais recente demora meses a partir da data de lançamento oficial.[103] Isso se deve parcialmente à extensa variação de hardware de dispositivos Android, aos quais a atualização deve ser especificamente modificada, de acordo com cada aparelho, já que o código puro somente roda em dispositivos Nexus.[103] Portar o Android para hardwares específicos consome tempo e dinheiro para diversas fabricantes, que acabam priorizando os dispositivos mais recentes em detrimento dos mais antigos. É comum que smartphones mais velhos não sejam atualizados, mesmo tendo hardware capaz de rodar a nova versão, já que a empresa pode decidir que não vale a pena. O problema se agrava quando as fabricantes customizam o sistema com seus apps e interface, que acabam tendo que ser reaplicados a cada dispositivo a cada atualização. A demora pode se agravar mais ainda se houver também interferência de operadoras nos dispositivos, que também customizam com seus aplicativos e interface própria.[103] A falta de suporte pós-venta de operadoras e fabricantes tem sido amplamente criticada por grupos de consumidores e pela mídia de tecnologia.[104][105] Alguns especialistas em tecnologia têm dito que a indústria de smartphones não consegue pagar o suficiente para atualizar seus dispositivos.[106] Já que isso traria um incentivo às pessoas a comprar novos produtos.[107] uma atitude descrita por alguns como “insultante”.[105] O Wi-Fi no Android (Logo) Smartphones Android têm a habilidade de reportar localizações de pontos de acesso Wi-Fi, que são somente porque fabricantes e operadores o designaram assim.[105] Em 2011, o Google criou parcerias com fabricantes e indústrias para anunciar uma “Aliança de Atualização do Android”, designada a oferecer updates para até 18 meses após o lançamento dos dispositivos.[108] Porém, desde então não houve mais nenhuma comunicação oficial sobre esta aliança.[103][109] Em 2012 o Google começou a dissociar determinados componentes do sistema operacional, assim eles poderiam ser atualizados pela Play Store, independente do Android em si. Um destes componentes, o Google Play Services, é um aplicativo de código fechado, que funciona no nível do sistema, provendo APIs para o Google, e que foi instalado automaticamente em praticamente todos os dispositivos com Android 2.2 ou superior. Com estas mudanças, o Google consegue adicionar novas funções no sistema através do Play Services, sem necessariamente ter que distribuir uma nova versão do Android em si. Como resultado, o Android 4.2 e 4.3 possuem relativamente poucas mudanças perceptíveis pelo usuário, focando mais em melhorias na plataforma e conserto de pequenos bugs.[110] Kernel Linux Tux, a mascote do Linux. O sistema Android consiste em um Kernel baseado no Kernel Linux, especificamente do ramo (LTS), suporte a longo tempo. Em janeiro de 2014 a maior parte das versões do Android eram moldadas em cima da versão do Kernel Linux 3.4 ou superior.[111][112] mas a versão específica do kernel depende do dispositivo Android e do processador utilizado por ele.[113][114][115] O Android utiliza vários Kernels desde o primeiro, o 2.6.25.[116] O Kernel Linux do Android possui alterações profundas na arquitetura que foram implementadas pelo Google, fora do típico círculo de desenvolvimento Kernel do Linux, como a inclusão de componentes como binder, ashmem, pmem, loggger, wakelocks e uma diferente saída de memória—out-of-memory (OOM).[117] O Android é uma distribuição Linux de acordo com a Linux Foundation.[118] com a chefe do projeto open-source do Google, Chris DiBona,[119] e outros diversos jornalistas.[120][121] Outros, porém, como o engenheiro do Google Patrick Brady, afirmam que o Android não é Linux no tradicional estilo Unix, já que o Android não inclui a biblioteca GNU C e outros componentes tipicamente encontrados nas distribuições Linux.[122] Comunidades Open-Source O Android possui comunidades de desenvolvedores e entusiastas que usam o Android Open Source Project (AOSP) para desenvolver e distribuir suas próprias versões modificadas do sistema operacional.[123] Esses sistemas desenvolvidos pela comunidade possuem geralmente novas características e funcionalidades e atualizações mais rápidas do que os disponibilizados oficialmente pelas fabricantes ou operadoras, embora sem a opção de controle de qualidade muito rígido.[124] Também contribuem para prover suporte, contínuo para dispositivos mais antigos que já não possuem mais atualizações oficiais ou trazer o Android para dispositivos que não foram lançados com Android originalmente, como o HP TouchPad. Tais comunidades lançam ROMs que geralmente são pre-rooted, e possuem modificações que não são recomendáveis para usuários sem conhecimento técnico do sistema, como opções para fazer overclock ou overvolt.[125] CyanogenMod foi o firmware mais utilizado[126] entre as comunidades do Android, até o dia que foi descontinuada.[127] Foi substituído por LineageOS.[127] Enquanto isso existia, servia como base para diversas outras ROMs. Historicamente, fabricantes de smartphones e operadoras de telefonia móvel, tipicamente são contra o desenvolvimento de firmware por terceiros. Tais fabricantes expressam preocupação com a má funcionalidade dos dispositivos rodando software desenvolvido por usuários, e o custo do suporte que isso traria.[128] Além disso, esses softwares modificados frequentemente possuem novas ferramentas, como o tethering, o qual as operadoras normalmente cobrariam uma taxa adicional. Como resultado destas modificações, obstáculos técnicos ao desenvolvimento e acesso aos softwares são criados por fabricantes e operadoras, como bootloader bloqueado, e acesso restrito às permissões de root. Porém, com o crescimento da comunidade Open-Source e a declaração do Congresso dos Estados Unidos permitindo o jailbreak de dispositivos móveis, as fabricantes e operadoras começaram a relaxar ações contrárias a esse tipo de desenvolvimento, chegando ao ponto de até mesmo fabricantes como HTC,[129] Motorola,[130] Samsung,[131][132] e Sony[133] dar suporte e encorajar o desenvolvimento destes softwares. Como resultado destas declarações, necessidade de circular bootloaders bloqueados para instalar softwares não-oficiais tem caído, já que o número de celulares enviados sem estas restrições sofreu um aumento considerável, apesar do usuário ainda perder a garantia se o fizer.[129] Apesar do relaxamento das fabricantes, algumas operadoras móveis dos Estados Unidos ainda proíbem a utilização de softwares de terceiros, frustrando muitos consumidores.[134] Segurança e privacidade Permissões são utilizadas para controlar determinados acessos dos aplicativos ao sistema. Os aplicativos do Android funcionam numa sandbox, local isolado do resto do sistema e que não possui nenhum acesso ao resto dele, a não ser que a permissão seja explicitamente dada no momento da instalação do programa. Antes de instalar um aplicativo, a Play Store mostra todas as permissões da qual o aplicativo precisa: um jogo pode precisar de acesso à vibração ou de acessar conteúdo no cartão de memória, por exemplo, mas não precisará de acesso às mensagens de texto ou à lista de contatos. Após revisar estas permissões, o usuário pode aceitá-las ou recusá-las, sendo o aplicativo instalado somente se o usuário as aceitar.[135] Este sistema de sandbox diminui o impacto sobre vulnerabilidades do sistema, mas a confusão entre desenvolvedores fez com que o sistema se tornasse ineficaz, já que os aplicativos pediam acesso à determinadas informações desnecessárias ao funcionamento do aplicativo.[136] Recentemente o Google lançou um update aos seus dispositivos para inserir um app que roda em segundo plano detectando aplicativos maliciosos.[137] O aplicativo “App Ops”, que foi designado para testes e desenvolvimento interno do Google para o Android na área de segurança e privacidade, foi introduzido a partir do Android 4.3 nos dispositivos Nexus. Inicialmente escondido dentro do sistema, o programa foi descoberto por programadores, ele permite que se instalsse o aplicativo de gerenciamento de permissões individuais dos aplicativos, selecionando o que o usuário gostaria que o aplicativo tivesse acesso, e ao o que o aplicativo não tivesse acesso.[138] O acesso ao programa foi removido a partir do Android 4.4.2, com a explicação de que ele fora colocado para o usuário final de maneira acidental. Por esta decisão, a empresa recebeu duras críticas da Electronic Frontier Foundation.[139][140][141] Seleção individual das permissões de aplicativos foi adicionada oficialmente junto ao Android Marshmallow.[142] É possível obter essa função em versões anteriores a essa com acesso root.[143][144] De acordo com pesquisas conduzidas pela empresa de segurança Trend Micro, a forma mais comum de malware no sistema Android é o abuso em relação a serviços premium, onde celulares infectados são colocados em serviços pagos sem o consentimento do usuário.[145] Outros malware introduzem propaganda não permitida e intrusiva no celular, ou enviam dados pessoais a terceiros, também sem a autorização do usuário.[145] Ameaças à segurança do Android têm crescido exponencialmente; por outro lado, engenheiros do Google têm argumentado que ameaças de malware ou vírus estão sendo exageradas por empresas de segurança por motivos estritamente comerciais.[146][147] e têm acusado a indústria de segurança de colocar medo nos usuários para vender aplicativos de segurança.[146] O Google ainda afirma que malwares perigosos são extremamente raros.[147] e que uma pesquisa conduzida pela F-Secure mostrou que apenas 0,5% dos malwares denunciados têm origem na Play Store.[148] O Google atualmente utiliza do sistema de escaneamento de malware Google Bouncer para detectar ameaças na Play Store.[149] Sua função é alertar usuários de aplicativos potencialmente perigosos antes que sejam baixados.[150] A versão Jelly Bean 4.2 do Android trouxe ferramentas de segurança aprimoradas, incluindo um detector de malware embutido no sistema, que trabalha em conjunto com o Google Play, mas também pode escanear aplicativos de terceiros que estejam instalados no sistema.[151] Várias companhias de segurança virtual lançaram aplicativos de segurança para o Android, como a Lookout Mobile Security.[152] AVG,[153] McAfee,[154] Avast,[155] BitDefender,[155] Kaspersky[155] e Trend Micro.[155] Esse tipo de aplicativo é geralmente tido como ineficaz, já que o sistema sandbox também é aplicado a eles, limitando a habilidade de escanear e proteger o sistema.[156][157] O Wi-Fi no Android (Logo) Smartphones Android têm a habilidade de reportar localizações de pontos de acesso Wi-Fi, que são somente porque fabricantes e operadores o designaram assim.[105] Em 2011, o Google criou parcerias com fabricantes e indústrias para anunciar uma “Aliança de Atualização do Android”, designada a oferecer updates para até 18 meses após o lançamento dos dispositivos.[108] Porém, desde então não houve mais nenhuma comunicação oficial sobre esta aliança.[103][109] Em 2012 o Google começou a dissociar determinados componentes do sistema operacional, assim eles poderiam ser atualizados pela Play Store, independente do Android em si. Um destes componentes, o Google Play Services, é um aplicativo de código fechado, que funciona no nível do sistema, provendo APIs para o Google, e que foi instalado automaticamente em praticamente todos os dispositivos com Android 2.2 ou superior. Com estas mudanças, o Google consegue adicionar novas funções no sistema através do Play Services, sem necessariamente ter que distribuir uma nova versão do Android em si. Como resultado, o Android 4.2 e 4.3 possuem relativamente poucas mudanças perceptíveis pelo usuário, focando mais em melhorias na plataforma e conserto de pequenos bugs.[110] Kernel Linux Tux, a mascote do Linux. O sistema Android consiste em um Kernel baseado no Kernel Linux, especificamente do ramo (LTS), suporte a longo tempo. Em janeiro de 2014 a maior parte das versões do Android eram moldadas em cima da versão do Kernel Linux 3.4 ou superior.[111][112] mas a versão específica do kernel depende do dispositivo Android e do processador utilizado por ele.[113][114][115] O Android utiliza vários Kernels desde o primeiro, o 2.6.25.[116] O Kernel Linux do Android possui alterações profundas na arquitetura que foram implementadas pelo Google, fora do típico círculo de desenvolvimento Kernel do Linux, como a inclusão de componentes como binder, ashmem, pmem, loggger, wakelocks e uma diferente saída de memória—out-of-memory (OOM).[117] O Android é uma distribuição Linux de acordo com a Linux Foundation.[118] com a chefe do projeto open-source do Google, Chris DiBona,[119] e outros diversos jornalistas.[120][121] Outros, porém, como o engenheiro do Google Patrick Brady, afirmam que o Android não é Linux no tradicional estilo Unix, já que o Android não inclui a biblioteca GNU C e outros componentes tipicamente encontrados nas distribuições Linux.[122] Comunidades Open-Source O Android possui comunidades de desenvolvedores e entusiastas que usam o Android Open Source Project (AOSP) para desenvolver e distribuir suas próprias versões modificadas do sistema operacional.[123] Esses sistemas desenvolvidos pela comunidade possuem geralmente novas características e funcionalidades e atualizações mais rápidas do que os disponibilizados oficialmente pelas fabricantes ou operadoras, embora sem a opção de controle de qualidade muito rígido.[124] Também contribuem para prover suporte, contínuo para dispositivos mais antigos que já não possuem mais atualizações oficiais ou trazer o Android para dispositivos que não foram lançados com Android originalmente, como o HP TouchPad. Tais comunidades lançam ROMs que geralmente são pre-rooted, e possuem modificações que não são recomendáveis para usuários sem conhecimento técnico do sistema, como opções para fazer overclock ou overvolt.[125] CyanogenMod foi o firmware mais utilizado[126] entre as comunidades do Android, até o dia que foi descontinuada.[127] Foi substituído por LineageOS.[127] Enquanto isso existia, servia como base para diversas outras ROMs. Historicamente, fabricantes de smartphones e operadoras de telefonia móvel, tipicamente são contra o desenvolvimento de firmware por terceiros. Tais fabricantes expressam preocupação com a má funcionalidade dos dispositivos rodando software desenvolvido por usuários, e o custo do suporte que isso traria.[128] Além disso, esses softwares modificados frequentemente possuem novas ferramentas, como o tethering, o qual as operadoras normalmente cobrariam uma taxa adicional. Como resultado destas modificações, obstáculos técnicos ao desenvolvimento e acesso aos softwares são criados por fabricantes e operadoras, como bootloader bloqueado, e acesso restrito às permissões de root. Porém, com o crescimento da comunidade Open-Source e a declaração do Congresso dos Estados Unidos permitindo o jailbreak de dispositivos móveis, as fabricantes e operadoras começaram a relaxar ações contrárias a esse tipo de desenvolvimento, chegando ao ponto de até mesmo fabricantes como HTC,[129] Motorola,[130] Samsung,[131][132] e Sony[133] dar suporte e encorajar o desenvolvimento destes softwares. Como resultado destas declarações, necessidade de circular bootloaders bloqueados para instalar softwares não-oficiais tem caído, já que o número de celulares enviados sem estas restrições sofreu um aumento considerável, apesar do usuário ainda perder a garantia se o fizer.[129] Apesar do relaxamento das fabricantes, algumas operadoras móveis dos Estados Unidos ainda proíbem a utilização de softwares de terceiros, frustrando muitos consumidores.[134] Segurança e privacidade Permissões são utilizadas para controlar determinados acessos dos aplicativos ao sistema. Os aplicativos do Android funcionam numa sandbox, local isolado do resto do sistema e que não possui nenhum acesso ao resto dele, a não ser que a permissão seja explicitamente dada no momento da instalação do programa. Antes de instalar um aplicativo, a Play Store mostra todas as permissões da qual o aplicativo precisa: um jogo pode precisar de acesso à vibração ou de acessar conteúdo no cartão de memória, por exemplo, mas não precisará de acesso às mensagens de texto ou à lista de contatos. Após revisar estas permissões, o usuário pode aceitá-las ou recusá-las, sendo o aplicativo instalado somente se o usuário as aceitar.[135] Este sistema de sandbox diminui o impacto sobre vulnerabilidades do sistema, mas a confusão entre desenvolvedores fez com que o sistema se tornasse ineficaz, já que os aplicativos pediam acesso à determinadas informações desnecessárias ao funcionamento do aplicativo.[136] Recentemente o Google lançou um update aos seus dispositivos para inserir um app que roda em segundo plano detectando aplicativos maliciosos.[137] O aplicativo “App Ops”, que foi designado para testes e desenvolvimento interno do Google para o Android na área de segurança e privacidade, foi introduzido a partir do Android 4.3 nos dispositivos Nexus. Inicialmente escondido dentro do sistema, o programa foi descoberto por programadores, ele permite que se instalsse o aplicativo de gerenciamento de permissões individuais dos aplicativos, selecionando o que o usuário gostaria que o aplicativo tivesse acesso, e ao o que o aplicativo não tivesse acesso.[138] O acesso ao programa foi removido a partir do Android 4.4.2, com a explicação de que ele fora colocado para o usuário final de maneira acidental. Por esta decisão, a empresa recebeu duras críticas da Electronic Frontier Foundation.[139][140][141] Seleção individual das permissões de aplicativos foi adicionada oficialmente junto ao Android Marshmallow.[142] É possível obter essa função em versões anteriores a essa com acesso root.[143][144] De acordo com pesquisas conduzidas pela empresa de segurança Trend Micro, a forma mais comum de malware no sistema Android é o abuso em relação a serviços premium, onde celulares infectados são colocados em serviços pagos sem o consentimento do usuário.[145] Outros malware introduzem propaganda não permitida e intrusiva no celular, ou enviam dados pessoais a terceiros, também sem a autorização do usuário.[145] Ameaças à segurança do Android têm crescido exponencialmente; por outro lado, engenheiros do Google têm argumentado que ameaças de malware ou vírus estão sendo exageradas por empresas de segurança por motivos estritamente comerciais.[146][147] e têm acusado a indústria de segurança de colocar medo nos usuários para vender aplicativos de segurança.[146] O Google ainda afirma que malwares perigosos são extremamente raros.[147] e que uma pesquisa conduzida pela F-Secure mostrou que apenas 0,5% dos malwares denunciados têm origem na Play Store.[148] O Google atualmente utiliza do sistema de escaneamento de malware Google Bouncer para detectar ameaças na Play Store.[149] Sua função é alertar usuários de aplicativos potencialmente perigosos antes que sejam baixados.[150] A versão Jelly Bean 4.2 do Android trouxe ferramentas de segurança aprimoradas, incluindo um detector de malware embutido no sistema, que trabalha em conjunto com o Google Play, mas também pode escanear aplicativos de terceiros que estejam instalados no sistema.[151] Várias companhias de segurança virtual lançaram aplicativos de segurança para o Android, como a Lookout Mobile Security.[152] AVG,[153] McAfee,[154] Avast,[155] BitDefender,[155] Kaspersky[155] e Trend Micro.[155] Esse tipo de aplicativo é geralmente tido como ineficaz, já que o sistema sandbox também é aplicado a eles, limitando a habilidade de escanear e proteger o sistema.[156][157] O Wi-Fi no Android (Logo) Smartphones Android têm a habilidade de reportar localizações de pontos de acesso Wi-Fi, que são somente porque fabricantes e operadores o designaram assim.[105] Em 2011, o Google criou parcerias com fabricantes e indústrias para anunciar uma “Aliança de Atualização do Android”, designada a oferecer updates para até 18 meses após o lançamento dos dispositivos.[108] Porém, desde então não houve mais nenhuma comunicação oficial sobre esta aliança.[103][109] Em 2012 o Google começou a dissociar determinados componentes do sistema operacional, assim eles poderiam ser atualizados pela Play Store, independente do Android em si. Um destes componentes, o Google Play Services, é um aplicativo de código fechado, que funciona no nível do sistema, provendo APIs para o Google, e que foi instalado automaticamente em praticamente todos os dispositivos com Android 2.2 ou superior. Com estas mudanças, o Google consegue adicionar novas funções no sistema através do Play Services, sem necessariamente ter que distribuir uma nova versão do Android em si. Como resultado, o Android 4.2 e 4.3 possuem relativamente poucas mudanças perceptíveis pelo usuário, focando mais em melhorias na plataforma e conserto de pequenos bugs.[110] Kernel Linux Tux, a mascote do Linux. O sistema Android consiste em um Kernel baseado no Kernel Linux, especificamente do ramo (LTS), suporte a longo tempo. Em janeiro de 2014 a maior parte das versões do Android eram moldadas em cima da versão do Kernel Linux 3.4 ou superior.[111][112] mas a versão específica do kernel depende do dispositivo Android e do processador utilizado por ele.[113][114][115] O Android utiliza vários Kernels desde o primeiro, o 2.6.25.[116] O Kernel Linux do Android possui alterações profundas na arquitetura que foram implementadas pelo Google, fora do típico círculo de desenvolvimento Kernel do Linux, como a inclusão de componentes como binder, ashmem, pmem, loggger, wakelocks e uma diferente saída de memória—out-of-memory (OOM).[117] O Android é uma distribuição Linux de acordo com a Linux Foundation.[118] com a chefe do projeto open-source do Google, Chris DiBona,[119] e outros diversos jornalistas.[120][121] Outros, porém, como o engenheiro do Google Patrick Brady, afirmam que o Android não é Linux no tradicional estilo Unix, já que o Android não inclui a biblioteca GNU C e outros componentes tipicamente encontrados nas distribuições Linux.[122] Comunidades Open-Source O Android possui comunidades de desenvolvedores e entusiastas que usam o Android Open Source Project (AOSP) para desenvolver e distribuir suas próprias versões modificadas do sistema operacional.[123] Esses sistemas desenvolvidos pela comunidade possuem geralmente novas características e funcionalidades e atualizações mais rápidas do que os disponibilizados oficialmente pelas fabricantes ou operadoras, embora sem a opção de controle de qualidade muito rígido.[124] Também contribuem para prover suporte, contínuo para dispositivos mais antigos que já não possuem mais atualizações oficiais ou trazer o Android para dispositivos que não foram lançados com Android originalmente, como o HP TouchPad. Tais comunidades lançam ROMs que geralmente são pre-rooted, e possuem modificações que não são recomendáveis para usuários sem conhecimento técnico do sistema, como opções para fazer overclock ou overvolt.[125] CyanogenMod foi o firmware mais utilizado[126] entre as comunidades do Android, até o dia que foi descontinuada.[127] Foi substituído por LineageOS.[127] Enquanto isso existia, servia como base para diversas outras ROMs. Historicamente, fabricantes de smartphones e operadoras de telefonia móvel, tipicamente são contra o desenvolvimento de firmware por terceiros. Tais fabricantes expressam preocupação com a má funcionalidade dos dispositivos rodando software desenvolvido por usuários, e o custo do suporte que isso traria.[128] Além disso, esses softwares modificados frequentemente possuem novas ferramentas, como o tethering, o qual as operadoras normalmente cobrariam uma taxa adicional. Como resultado destas modificações, obstáculos técnicos ao desenvolvimento e acesso aos softwares são criados por fabricantes e operadoras, como bootloader bloqueado, e acesso restrito às permissões de root. Porém, com o crescimento da comunidade Open-Source e a declaração do Congresso dos Estados Unidos permitindo o jailbreak de dispositivos móveis, as fabricantes e operadoras começaram a relaxar ações contrárias a esse tipo de desenvolvimento, chegando ao ponto de até mesmo fabricantes como HTC,[129] Motorola,[130] Samsung,[131][132] e Sony[133] dar suporte e encorajar o desenvolvimento destes softwares. Como resultado destas declarações, necessidade de circular bootloaders bloqueados para instalar softwares não-oficiais tem caído, já que o número de celulares enviados sem estas restrições sofreu um aumento considerável, apesar do usuário ainda perder a garantia se o fizer.[129] Apesar do relaxamento das fabricantes, algumas operadoras móveis dos Estados Unidos ainda proíbem a utilização de softwares de terceiros, frustrando muitos consumidores.[134] Segurança e privacidade Permissões são utilizadas para controlar determinados acessos dos aplicativos ao sistema. Os aplicativos do Android funcionam numa sandbox, local isolado do resto do sistema e que não possui nenhum acesso ao resto dele, a não ser que a permissão seja explicitamente dada no momento da instalação do programa. Antes de instalar um aplicativo, a Play Store mostra todas as permissões da qual o aplicativo precisa: um jogo pode precisar de acesso à vibração ou de acessar conteúdo no cartão de memória, por exemplo, mas não precisará de acesso às mensagens de texto ou à lista de contatos. Após revisar estas permissões, o usuário pode aceitá-las ou recusá-las, sendo o aplicativo instalado somente se o usuário as aceitar.[135] Este sistema de sandbox diminui o impacto sobre vulnerabilidades do sistema, mas a confusão entre desenvolvedores fez com que o sistema se tornasse ineficaz, já que os aplicativos pediam acesso à determinadas informações desnecessárias ao funcionamento do aplicativo.[136] Recentemente o Google lançou um update aos seus dispositivos para inserir um app que roda em segundo plano detectando aplicativos maliciosos.[137] O aplicativo “App Ops”, que foi designado para testes e desenvolvimento interno do Google para o Android na área de segurança e privacidade, foi introduzido a partir do Android 4.3 nos dispositivos Nexus. Inicialmente escondido dentro do sistema, o programa foi descoberto por programadores, ele permite que se instalsse o aplicativo de gerenciamento de permissões individuais dos aplicativos, selecionando o que o usuário gostaria que o aplicativo tivesse acesso, e ao o que o aplicativo não tivesse acesso.[138] O acesso ao programa foi removido a partir do Android 4.4.2, com a explicação de que ele fora colocado para o usuário final de maneira acidental. Por esta decisão, a empresa recebeu duras críticas da Electronic Frontier Foundation.[139][140][141] Seleção individual das permissões de aplicativos foi adicionada oficialmente junto ao Android Marshmallow.[142] É possível obter essa função em versões anteriores a essa com acesso root.[143][144] De acordo com pesquisas conduzidas pela empresa de segurança Trend Micro, a forma mais comum de malware no sistema Android é o abuso em relação a serviços premium, onde celulares infectados são colocados em serviços pagos sem o consentimento do usuário.[145] Outros malware introduzem propaganda não permitida e intrusiva no celular, ou enviam dados pessoais a terceiros, também sem a autorização do usuário.[145] Ameaças à segurança do Android têm crescido exponencialmente; por outro lado, engenheiros do Google têm argumentado que ameaças de malware ou vírus estão sendo exageradas por empresas de segurança por motivos estritamente comerciais.[146][147] e têm acusado a indústria de segurança de colocar medo nos usuários para vender aplicativos de segurança.[146] O Google ainda afirma que malwares perigosos são extremamente raros.[147] e que uma pesquisa conduzida pela F-Secure mostrou que apenas 0,5% dos malwares denunciados têm origem na Play Store.[148] O Google atualmente utiliza do sistema de escaneamento de malware Google Bouncer para detectar ameaças na Play Store.[149] Sua função é alertar usuários de aplicativos potencialmente perigosos antes que sejam baixados.[150] A versão Jelly Bean 4.2 do Android trouxe ferramentas de segurança aprimoradas, incluindo um detector de malware embutido no sistema, que trabalha em conjunto com o Google Play, mas também pode escanear aplicativos de terceiros que estejam instalados no sistema.[151] Várias companhias de segurança virtual lançaram aplicativos de segurança para o Android, como a Lookout Mobile Security.[152] AVG,[153] McAfee,[154] Avast,[155] BitDefender,[155] Kaspersky[155] e Trend Micro.[155] Esse tipo de aplicativo é geralmente tido como ineficaz, já que o sistema sandbox também é aplicado a eles, limitando a habilidade de escanear e proteger o sistema.[156][157] O Wi-Fi no Android (Logo) Smartphones Android têm a habilidade de reportar localizações de pontos de acesso Wi-Fi, que são somente porque fabricantes e operadores o designaram assim.[105] Em 2011, o Google criou parcerias com fabricantes e indústrias para anunciar uma “Aliança de Atualização do Android”, designada a oferecer updates para até 18 meses após o lançamento dos dispositivos.[108] Porém, desde então não houve mais nenhuma comunicação oficial sobre esta aliança.[103][109] Em 2012 o Google começou a dissociar determinados componentes do sistema operacional, assim eles poderiam ser atualizados pela Play Store, independente do Android em si. Um destes componentes, o Google Play Services, é um aplicativo de código fechado, que funciona no nível do sistema, provendo APIs para o Google, e que foi instalado automaticamente em praticamente todos os dispositivos com Android 2.2 ou superior. Com estas mudanças, o Google consegue adicionar novas funções no sistema através do Play Services, sem necessariamente ter que distribuir uma nova versão do Android em si. Como resultado, o Android 4.2 e 4.3 possuem relativamente poucas mudanças perceptíveis pelo usuário, focando mais em melhorias na plataforma e conserto de pequenos bugs.[110] Kernel Linux Tux, a mascote do Linux. O sistema Android consiste em um Kernel baseado no Kernel Linux, especificamente do ramo (LTS), suporte a longo tempo. Em janeiro de 2014 a maior parte das versões do Android eram moldadas em cima da versão do Kernel Linux 3.4 ou superior.[111][112] mas a versão específica do kernel depende do dispositivo Android e do processador utilizado por ele.[113][114][115] O Android utiliza vários Kernels desde o primeiro, o 2.6.25.[116] O Kernel Linux do Android possui alterações profundas na arquitetura que foram implementadas pelo Google, fora do típico círculo de desenvolvimento Kernel do Linux, como a inclusão de componentes como binder, ashmem, pmem, loggger, wakelocks e uma diferente saída de memória—out-of-memory (OOM).[117] O Android é uma distribuição Linux de acordo com a Linux Foundation.[118]







bits. Outro exemplo são as GPUs (Unidade de Processamento Gráfico), mais conhecidas como Placas de vídeo; as placas mais atuais variam entre 64 a 512 bits, onde é clara a diferença de desempenho. Uma placa de vídeo de 600 MHz e 64 bits, por exemplo, apresentará um desempenho significativamente inferior à outra de 600 MHz de 256 bits caso tenham a mesma construção interna. Apesar de ambas apresentarem a mesma velocidade de processamento, uma vez que a de 256 bits irá processar mais informações por vez, pode-se até dizer que uma é 4 vezes melhor do que a outra, em termos de qualidade de processamento.
Compatibilidade
Para manter a compatibilidade com programas 32-bits, que são os mais usados atualmente, foi criada a extensão "x86-64" fazendo que processadores de 64 bits normalmente simulam o processamento de 32 bits a menos que estejam rodando programas especificamente construídos para funcionar em 64 bits. Barramento
Quando se classifica um processador como sendo de 4, 8, 16, 32 ou 64 bits, referimos-nos à dimensão dos seus registradores internos. Tradicionalmente, o número de bits dos registradores do processador é o mesmo que o número de linhas do barramento de dados. Assim, o 8088 e o 80188 são ambos processadores de 16 bits, porque apesar de terem um barramento de dados de 8 bits, têm os registradores internos com 16 bits, tal como os seus equivalentes 8086 e 80186 respectivamente. O número de linhas do barramento de endereços de um processador é que define a sua capacidade de endereçamento e não tem relação com o número de bits que processa.
Arquiteturas
A AMD foi a primeira empresa a anunciar, em 2003, um processador de 64 bits compatível com Windows.[3][4] enquanto a Apple foi a primeira empresa a empregar a arquitetura 64-bit em um Smartphone.
Referências
↑ Sérgio, Luiz. «apostila de AOC» (PDF) ↑ Ltd, Arm. «News - Arm®». Arm | The Architecture for the Digital World (em inglês). Consultado em 18 de novembro de 2021 
↑ AMD. «AMD Ushers in Era of Cinematic Computing with the AMD Athlon™ 64 FX Processor» (em inglês). Consultado em 5 de junho de 2007 
A referência emprega parâmetros obsoletos |língua2= (ajuda)
↑ «Primeiro processador para PC de 64 bits compatível com Windows». Consultado em 5 de junho 2007 
Portal das tecnologias de informação
Obtida de "

1980

1981

1982

1983

1984

1985

1986

1987

1988

1989

1990

1991

1992

1993

1994

1995

1996

1997

1998

1999

2000

2001

2002

2003

2004

2005

2006

2007

2008

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

2019

2020

2021

2022

2023

2024

2025

2026

2027

2028

2029

2030

2031

2032

2033

2034

2035

2036

2037

2038

2039

2040

2041

2042

2043

2044

2045

2046

2047

2048

2049

2050

2051

2052

2053

2054

2055

2056

2057

2058

2059

2060

2061

2062

2063

2064

2065

2066

2067

2068

2069

2070

2071

2072

2073

2074

2075

2076

2077

2078

2079

2080

2081

2082

2083

2084

2085

2086

2087

2088

2089

2090

2091

2092

2093

2094

2095

2096

2097

2098

2099

2100

2101

2102

2103

2104

2105

2106

2107

2108

2109

2110

2111

2112

2113

2114

2115

2116

2117

2118

2119

2120

2121

2122

2123

2124

2125

2126

2127

2128

2129

2130

2131

2132

2133

2134

2135

2136

2137

2138

2139

2140