GUSTAVO CUSTODIO DE OLIVEIRA
JOÃO MARCOS LESSI

GUIA EDUCACIONAL DE PERMISSÕES ANDROID

UNIFEV – CENTRO UNIVERSITÁRIO DE VOTUPORANGA
DEZEMBRO/2019

GUSTAVO CUSTODIO DE OLIVEIRA
JOÃO MARCOS LESSI

GUIA EDUCACIONAL PARA GERENCIAMENTO DE PERMISSÕES ANDROID

Monografia apresentada à Unifev – Centro Universitário de Votuporanga – para obtenção do grau de Bacharel em Engenharia da Computação sob a orientação do professor Esp. Eric de Oliveira Freitas

UNIFEV – CENTRO UNIVERSITÁRIO DE VOTUPORANGA
Dezembro/2019

GUSTAVO CUSTODIO DE OLIVEIRA
JOÃO MARCOS LESSI

GUIA EDUCACIONAL PARA GERENCIAMENTO DE PERMISSÕES ANDROID

Monografia apresentada à Unifev – Centro Universitário de Votuporanga – para obtenção do grau de Bacharel em Engenharia da Computação.

Aprovado: ___/___/___

Primeiro examinador:	Segundo examinador:
Nome:	Nome:
Instituição	Instituição

Eric de Oliveira Freitas
Prof. Esp. Orientador
Unifev – Centro Universitário de Votuporanga
Dezembro/2019

“Aqueles que podem imaginar qualquer coisa, podem criar o impossível” (Alan Turing)

AGRADECIMENTOS

Aos professores que ajudaram a progredir no projeto, meus amigos que diante de momentos críticos para o desenvolvimento me ajudaram com seu apoio e habilidades, ao nosso orientador que que esteve presente em todos os momentos nos dando conselhos e direções para seguir.

RESUMO

Dispositivos móveis estão cada vez mais presentes no nosso cotidiano, milhares de aparelhos são ativos e funcionais e a cada dia que passa este número tende a aumentar, entretanto um fator muito importante e que poucas pessoas prestam atenção é a segurança destes aparelhos que, mesmo pequenos, possuem grande capacidade de armazenamento. Este trabalho tem como objetivo criar uma aplicação que sirva como um guia referencial capaz de trazer ao usuário informações a respeito de falhas na segurança de aplicativos mal-intencionados e mostrar na prática como funcionam as permissões dadas aos aplicativos e quais informações elas podem acessar. A segurança da informação é uma área de grande importância no meio da tecnologia, mas ao mesmo tempo é um assunto onde poucos dão a devida importância sempre possuindo o pensamento de que só o próximo está sujeito a cair em tais artimanhas.

Palavras-chave: Dispositivos moveis. Segurança. Informação. Vulnerabilidade. Permissão

ABSTRACT

Mobile devices are increasingly present in our daily lives, thousands of devices are active and functional and with each passing day this number tends to increase, however a very important factor and that few people pay attention is the safety of these devices that even small, have large storage capacity. This paper aims to create an application that serves as a reference guide that can provide users with information about malicious application security holes and show in practice how permissions given to applications work and what information they can access. Information security is an area of great importance in the midst of technology, but at the same time it is a subject where few give due importance always having the thought that only the next is subject to falling into such gimmicks.

Keywords: Mobile devices. Safety. Information. Vulnerability. Permission

LISTA DE FIGURAS

Sumário

1 INTRODUÇÃO

Dispositivos móveis, em particular smartphones e tablets, estão ganhando cada vez mais espaço dentro do mundo das TICs (Tecnologias da Informação e Comunicação) tanto em seu uso pessoal quanto em seu uso profissional.

Este fato é caracterizado pela quantidade de dispositivos ativos e disponíveis no mercado que possuem grande poder de processamento e conectividade, sem contar a variedade de serviços e aplicativos disponíveis em ambientes públicos e privados. Com o advento da tecnologia móvel, esses dispositivos ficam mais expostos e se tornam alvos de ataques cibernéticos de risco elevado.

Por conta deste fato, a segurança da informação que em outros casos já foi um tema bem estruturado e organizado, hoje se vê em desordem e descaso graças ao aumento drástico de usuários pouco informados e atentos às questões sobre a segurança da informação. Segundo Braga (2012), existem três aspectos inter-relacionados que abordam o tema de segurança móvel.

O primeiro aspecto é a constatação no segundo semestre de 2011 que os dispositivos móveis serão a próxima fronteira de proliferação de softwares maliciosos. Fato que foi comprovado logo no último quarto do ano de 2011 pela quantidade de dispositivos maliciosos que são voltados à plataforma Android, da Google.

O segundo aspecto é chamado consumerização, no qual as novas tecnologias começarão a surgir primeiro para os usuários finais e, só depois, são integradas ao ambiente corporativo, efeito contrário do que aconteceu com tecnologias de computadores de grande porte, como computadores e aparelhos de fax e impressoras. Deste modo, os indivíduos que trocam constantemente de aparelhos começam a utilizá-los de modo mais intenso não apenas em ambientes

pessoais e rotineiros, mas também em seus ambientes de trabalho, criando assim um fenômeno comportamental chamado BYOD (Bring Your Own Device). Deste modo os indivíduos forçam as organizações a se adaptar à novas tecnologias e ao tratamento de normas de segurança de uma forma descentralizada, pois a empresa perde o controle de ativos que entram no ambiente de rede e a noção de perímetro de segurança.

Já o terceiro aspecto, não é menos importante, pois é na verdade uma junção dos dois anteriores, onde em um ambiente de TIC, juntamente caracterizado pelos fenômenos de consumerização e BYOD, muitos dos controles de segurança tradicionalmente adotados e aplicados a desktops e outros ativos da infraestrutura se mostram ineficazes quando aplicados a dispositivos móveis.

1.1 OBJETIVOS GERAIS

Este trabalho tem como objetivo, estudar e analisar as permissões da plataforma android e poder trazer um guia educacional, voltado para aqueles que não estão familiarizados com o assunto, visando conscientizar e trazer informações de extrema importância.

1.2 PROBLEMÁTICA

Muitos aplicativos grandes e populares não permitem o acesso as permissões do mesmo, tornando difícil a implementação no guia sem antes consultar os mesmos para que queiram inserir o mesmo no projeto, limitando o uso do software em questão. Muitos especialistas ficam limitados ao mesmo, sendo necessário um tempo longo de espera para a comunicação com a empresa desenvolvedora.

1.3 OBJETIVO ESPECÍFICO

Considerando o desenvolvimento do trabalho e o objetivo geral apresentado, destacam-se os seguintes objetivos específicos:

- Criar uma aplicação simples e intuitiva que mostre ao usuário como funcionam as permissões de uma aplicação.
- Elaborar explicações que abordem o tema de maneira não complexa.
- Trazer experiencias práticas ao usuário de como suas informações podem ser acessadas ao conceder permissões especificas a aplicativos mal-intencionados.
- Conseguir demonstrar tudo o que foi dito.
- Ter a possibilidade de mostrar ao usuário de forma segura os riscos que este pode correr ao habilitar funções de modo desapercebido.

1.4 JUSTIFICATIVA

Com base em pesquisas já feitas e utilizadas por outros projetos direcionados à segurança de dispositivos móveis, entende-se que os usuários em sua maioria pouco se importam com questões de segurança e vulnerabilidades do sistema, dando atenção mínima à temas que podem ser relevantes, não lendo mensagens informativas que os próprios aplicativos disponibilizam simplesmente porque possuem pressa para usar o serviço ou a funcionalidade em questão e acabam por fim aceitando termos e permissões dos quais muitas vezes não se tem ideia.

1.5 METODOLOGIA

No processo de elaboração do projeto utilizou-se o Visual Studio Code, um *ambiente de desenvolvimento integrado com licença gratuita* e que possui suporte a diversas linguagens de programação como o Flutter e muitas ferramentas necessárias para a realização de atividades pertinentes ao projeto.

Também foram feitas pesquisas sobre o framework da plataforma Android e sua estrutura lógica de forma que seja possível realizar funções e atividades dentro da aplicação.

2 DISPOSITIVOS MÓVEIS

Mobilidade é uma característica do que é móvel ou que possui capacidade de se movimentar, quando falamos de dispositivos móveis a primeira coisa que vem a nossa cabeça são os telefones celulares, conhecidos popularmente como smartphones, que são dispositivos capazes de serem operados a distância ou sem fio e permitem comunicações com outras pessoas e a obtenção de informações de qualquer lugar, a qualquer hora.

Segundo (NOVO, 2011), o conceito de telefone celular foi desenvolvido em meados de 1960, tornando-se comercial a partir dos anos 80, sua primeira aparição foi em 1981, no Japão e na Escandinávia, já nas Américas os dispositivos foram introduzidos a partir de 1983. Essa tecnologia tomou grandes proporções em uma velocidade muito rápida, em menos de 30 anos alcançou cerca de 5 bilhões de telefones celulares ao redor do mundo.

2.1 SMARTPHONES

> Smartphone significa telefone inteligente, numa tradução livre do inglês, é um telefone celular com funcionalidades avançadas e sistema operacional. Os smartphones são a combinação de duas classes de dispositivos: os celulares e os assistentes pessoais (Palms e PDAs). A principal vantagem dos smartphones, comparados aos antecessores, é que podem se conectar à web através de conexões 3G ou WI-FI, o que permite que eles ofereçam uma enorme variedade de recursos. (NOVO, T., 2011, p.5)

Um smartphone é essencial para os dias atuais, pois além de concentrar um grande volume de funções em um aparelho de pequeno peso, é

possível carregá-lo em um bolso e ter acesso contínuo à internet. Hoje em dia até mesmo um modelo relativamente simples e barato pode navegar na web, acessar e-mails e chats, fazer chamadas VOIP, usar uma câmera fotográfica, tocar música, exibir e gravas vídeos e utilizar recursos como o navegador de GPS.

Sua principal característica que o define e difere de outros aparelhos pessoais é a capacidade de instalar aplicações adicionais, o que permite que os smartphones executem diversas funções no dia a dia. Esse conjunto de fatores torna os smartphones indispensáveis para qualquer pessoa.

2.2 SEGURANÇA DA INFORMAÇÃO

De acordo com D'Andrea (2017) e SIGNIFICADOS (2017) e FIA (2018), a segurança da informação tem um conjunto de informações e medidas que são cada vez mais necessárias para os usuários, pois com o avanço tecnológico continuo, principalmente dos dispositivos móveis, tendo muitas falhas de segurança que são exploradas diariamente por usuários mal-intencionados, com o objetivo de roubar dados, informações que possam favorecer os mesmos.

O surgimento da segurança da informação veio para justamente como é dito no nome, para trazer segurança e medidas que possam ser tomadas para preservar a confidencialidade e integridade dos dados, das informações, buscando trazer segurança e tranquilidade ao usuário, para que o mesmo saiba que nada de errado pode estar acontecendo com suas informações e dados, sempre haverá riscos, mas o intuito da segurança da informação é diminuir os riscos que as pessoas correm todos os dias navegando pela rede seja em um computador ou em um dispositivo móvel. Com o crescimento constante da tecnologia é possível acessar muitas informações e de qualquer lugar, a qualquer momento a partir de inúmeros dispositivos, ao mesmo tempo é possível ter sempre vantagens em relação a segurança, mas existem usuários mal-intencionados que estão se aproveitando desse crescimento contínuo para prejudicar as pessoas.

Alguns pilares regem a segurança da informação, sendo eles: confidencialidade, disponibilidade, integridade, autenticidade e irretratabilidade, a junção desses cinco pilares são responsáveis pela segurança das informações que são trafegadas o tempo todo, resumindo de maneira simples, a segurança da

informação sempre estará trabalhando para manter dados e informações confidencias, ou seja, conteúdo protegido que será somente para pessoas que forem autorizadas, mas ao mesmo tempo, garantir que sejam confiáveis, que não tenham sido alterados e assegurar a origem do mesmo.

Com a popularização dos dispositivos moveis nesse mundo dos TICs(Tecnologias da informação e comunicação) muitos incidentes relacionados à segurança são cada vez mais frequentes, pois as TICs(Tecnologia da informação e comunicação) tem como intuito facilitar a comunicação entre as pessoas, empresas com o uso do avanço tecnológico que é disponibilizado para as pessoas, estando sempre em alta por revolucionar os processos de negócios, empresas e pesquisas cientificas com o uso da comunicação de fácil acesso, a informação e comunicação, mas ao mesmo tempo, é necessário atrelar a segurança da informação aos TICs para reduzir os riscos e as falhas que muitas vezes podem ser exploradas, comprometendo toda essa comunicação e interação que é feita

2.3 SEGURANÇA DE DISPOSITIVOS MÓVEIS

A segurança da informação digital constitui uma questão de grande atualidade e inegável relevância. Seja em bibliotecas ou arquivos digitais, na banca electrónica, no e-learning ou em qualquer outra área, a segurança da informação digital é uma questão chave para a sobrevivência de muitas organizações (PEREIRA, 2005).

Tendo em vista que muitos estudos comprovam que os sistemas antivírus não são altamente eficazes nos próprios computadores que são os principais usuários dos sistemas antivírus, acaba se tornando ineficaz nos sistemas de dispositivos móveis, apesar de a ideia principal das empresas serem trazer um dispositivo móvel que se assemelha ao seu computador tenha em mente “Não são a mesma coisa”.

A ideia de ter algo mais simples e de eficácia média a alta vem de todos esses incidentes que temos todos os dias com relação aos dispositivos móveis e vamos separar em dois pontos.

O primeiro ponto é a sincronização do meio de uso pessoal para o meio corporativo/profissional e a sincronização total que temos atualmente, os

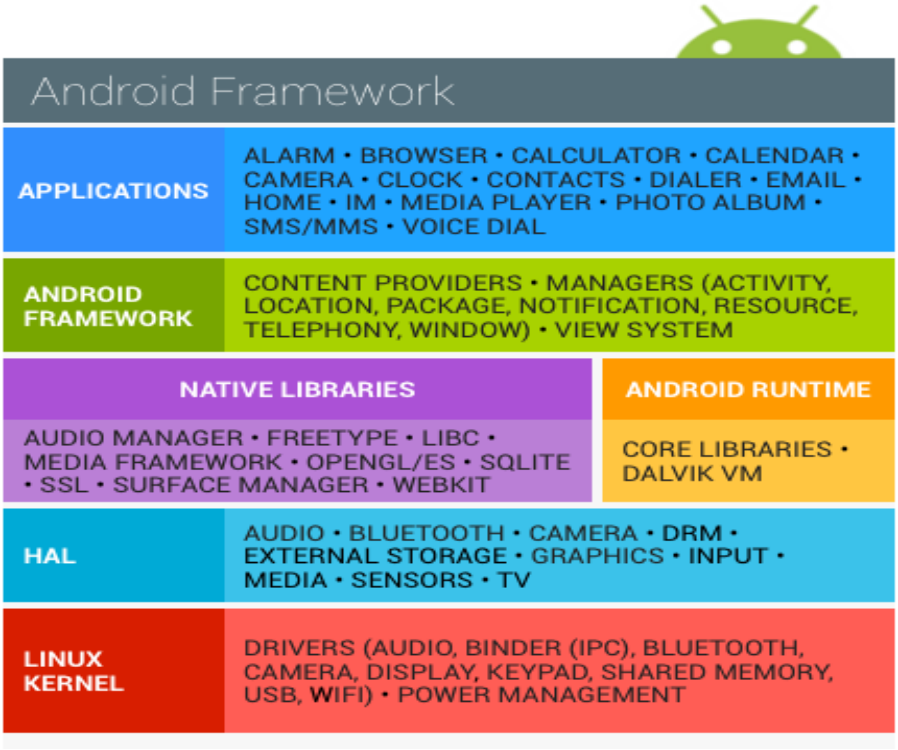
aparelhos celulares atuais sincronizam todas as contas, agendas telefônicas, e-mails e etc. as nossas contas de e-mail e nuvem, com o avanço dessa tecnologia muitas empresas trazem em conjunto a ideia de trabalharem também com seus smartphones, algo que pode ser prático mas perigoso, desta forma tiramos o foco muitas vezes o uso pessoal para o coorporativo e profissional, dificultando mais ainda para quem trabalha com a área da segurança atrelar os dois ambientes em um mesmo, conseguindo prevenir tanto o uso pessoal como o uso profissional, mas com a disseminação dessa ideia, empresas que não tem muito cuidado ou informação em relação a segurança digital não sabem o risco que colocam sua empresa, até mais do que simples dados.

O segundo ponto é o avanço rápido da tecnologia em relação a segurança dos dados e da informação, o avanço dessas tecnologias fazem com que as informações e os dados sucumbam ao meio, se tornando frágeis, fracas e facilmente exploradas, tomando uma visão mais firme, podemos entender que não é possível sempre acompanhar a segurança desses dados ao mesmo tempo da evolução rápida tecnológica no mundo dos smartphones, a cada dia mais os dados ficam mais e mais vulneráveis, temos normas que foram criadas para assegurar esses dados, normas para padronizar e seguir uma linha que previna que seu dispositivo seja comprometido, mas como dito antes, a evolução e a necessidade de dinheiro por parte das empresas que lançam diversas versões por ano de sistemas e modelos de smartphones compromete um pouco a padronização que foi dita para assegurar a informação e os dados.

2.4 PLATAFORMA ANDROID

O android é uma plataforma opensource (uma plataforma que é aberta para que usuários desenvolva para a mesma) composta por sistema operacional, middleware, frameworks de aplicação e algumas aplicações essenciais que provém o funcionamento básico do dispositivo. O esforço inicial para a criação da plataforma foi da Google, que posteriormente, entregou o projeto à Open Handset Alliance, grupo que na época era composto por operadoras, fabricantes de dispositivos e de componentes e fabricantes de softwares. A seguir iremos explicar as camadas da plataforma conforme segue a imagem.

Figura 1 - Android Framework



Fonte: GOOGLE. Arquitetura Android. **source.android**, 2019.

Na camada superior encontram-se as aplicações essenciais para o provimento de funções básicas do dispositivo. Estas aplicações vêm pré-instaladas e, temos como alguns exemplos: serviços de voz, serviços de SMS/MMS, e-mail, calendário, navegador web e agenda. Entretanto, os OEMs (Original Equipament Manufacturer) têm a liberdade de inserir seus próprios aplicativos no dispositivo pelos mais diversos motivos. As aplicações de terceiros que são instaladas pelo usuário através das lojas, depuração USB, ADB (Android Debug Bridge), ou por meio da execução de um APK (Android Application Package) armazenados na memória interna ou em um cartão SD, também ficam nesta camada. Entretanto essas duas últimas opções demandam ser ativadas nas configurações do aparelho pelo próprio usuário, as aplicações desta camada são compostas pelos componentes responsáveis pelo provimento das mais diversas funcionalidades suportadas pela API do Android. São estas: Activities, Broadcast Receivers, Services e Content Providers.

O framework de aplicações é composto por código compilado para a máquina virtual Dalvik – que foi desenvolvido para rodar de maneira eficiente em plataformas utilizadas por dispositivos móveis – e provê grande variedade de serviços para os aplicativos desenvolvidos para esta plataforma. Nesta camada encontramos módulos como o provedor de serviços de localização, de gerenciamento de Activities e de Content Providers

A camada middleware é responsável por implementar os serviços que serão disponibilizados para o framework de aplicação e para as aplicações. Esta camada é composta por diversas bibliotecas nativas que são compiladas de forma exclusiva para cada dispositivo e provém as mais diversas funcionalidades, tais quais, acesso à tela gráfica, engine de renderização web, acesso à base de dados relacional e estabelecimento de canal SSL/TLS.

O sistema operacional por sua vez traz em seu núcleo o Kernel do Linux, que é o responsável pela abstração do hardware e pelo provimento de interfaces para o gerenciamento deste hardware através dos drivers do dispositivo. Nesta camada são aplicados alguns dos controles de segurança referentes ao confinamento de aplicações, afora alguns outros que fazem parte desta esta é uma das camadas mais importantes quando falamos sobre a segurança do sistema.

A plataforma android foi concebida de tal modo que a sua segurança pudesse ser alterada pelos desenvolvedores, porém, não dependesse exclusivamente destes. Sua arquitetura de segurança permite que controles sejam aplicados de forma transparente ao desenvolvedor, ou seja, este processo contém um grande nível de abstração. Isso é alcançado pelo confinamento de aplicações, pelo esquema de permissões – tanto do sistema de arquivos chamados de API, que preza a segurança por default – e pelo mecanismo de IPC (Inter-Process Communication), que também aplica as permissões para conceder acesso ou não entre os diferentes componentes.

2.5 APLICAÇÕES MOBILE

Uma aplicação ou aplicativo, como é comumente chamado, é um software desenvolvido através de uma linguagem de programação para ser instalado em smartphones ou tablets. São adquiridos através de lojas de aplicações on-line, que

podem ou não ser seguras, atualmente cerca de 700 mil aplicativos podem ser encontrados em uma loja de aplicativos, estima-se que mais da metade destes nunca nem se quer foram baixados.

2.6 SEGURANÇA DE APLICAÇÕES

> Com a crescente preocupação com segurança, os sistemas operacionais estão sendo concebidos com segurança embutida no processo de desenvolvimento, práticas de desenvolvimento seguro vêm sendo seguidas, afora serem criados/aplicados controles de segurança a fim de dificultar ou impossibilitar explorações ao sistema. Ademais, existe uma quantidade muito maior de aplicativos difundidos no mercado do que sistemas operacionais, e a quantidade de desenvolvedores de SOs é muito inferior à de desenvolvedores de aplicativos, além de que os primeiros normalmente são muito mais experientes e possuem um conhecimento de computação muito mais consistente do que os últimos. Disso resulta uma quantidade muito maior de aplicativos vulneráveis do que de SOs. (BRAGA, A. et al, 2012, p.19)

Como vimos em 2.4, o sistema Android nos permite confinar aplicações por meio de uma modificação no sistema de permissões de usuário tradicional do Linux. De forma direta, cada aplicação roda como se fosse o próprio usuário, ou seja, possui um UID exclusivo e um diretório próprio para armazenar dados que são restritos pelo esquema de permissões do sistema que é restrito apenas a ela.

Um mecanismo de segurança eficaz, além de impossibilitar o acesso entre as aplicações deveria também limitar o acesso das aplicações às chamadas de API mais críticas, afim de assegurar o princípio do menor privilégio, de modo que aplicações que tem o intuito de prover lazer e diversão aos usuários não sejam capazes de acessar funções como rede Wi-Fi, bluetooth, câmera, serviços de GPS, funções de telefonia, SMS/MMS e de dados de rede no celular.

Tendo em vista todos esses detalhes, foi criado um esquema de permissões que limitam o acesso das aplicações a chamadas de API. Esse esquema é chamado de Manifest Permissions, isso é dado pelo fato de que as permissões são especificadas no arquivo AndroidManifest.xml que vem distribuído junto com o aplicativo. Sendo assim, caso haja alguma vulnerabilidade dentro da aplicação que permita uma exploração, o código injetado estará confinado apenas ao ambiente da mesma aplicação e só terá os privilégios que esta possuir.

O esquema funciona de maneira similar à:

1. O desenvolvedor lista no AndroidManifest.xml todas as permissões necessárias para o funcionamento da aplicação;
2. Durante a instalação desta, o usuário é alertado sobre as permissões sendo requisitadas, tendo a opção de aceitá-las ou não; a. Modelo tudo ou nada. Ou o usuário aceito e utiliza a aplicação ou nega e a aplicação não é instalada.
3. Após a aceitação do usuário, a aplicação é instalada e passa a desfrutar das permissões que lhe foram atribuídas. O usuário não é mais informado sobre as permissões sendo utilizadas;
4. É possível, por meio das configurações do sistema, visualizar as permissões atribuídas a cada aplicação instalada;
5. O usuário também pode desabilitar globalmente algumas funcionalidades, tais como: Wi-Fi, Bluetooth, serviços de localização, GPS e rede celular.
6. A maior crítica sobre este método de delegar responsabilidade ao usuário, está no fato de que estes mal leem mensagens com cunho informativo, pois as consideram como empecilhos que o impedem de utilizar os aplicativos e acabam, por fim, aceitando a todos os termos sem nem mesmo saber do que se tratam.

2.7 PERMISSÕES DE APIS

> Existem duas faces quando se trata dessas permissões. A primeira é quando se está utilizando APIs e serviços disponibilizados pelo sistema. Neste caso é necessário levantar quais permissões são requeridas pelas funcionalidades sendo utilizadas a fim de incluí-las no Manifest do aplicativo. A segunda é quando se está disponibilizando serviços. Neste caso, é necessário assegurar que os componentes e aplicações utilizando-os possuem as devidas permissões para realizar as operações sendo fornecidas. (BRAGA, A. et al, 2012, p.19)

Algumas permissões são deixadas como responsabilidade do Kernel do sistema, por exemplo, permissões que acessam a internet. Ao solicitar uma permissão de acesso à internet, o UID da aplicação é adicionado a um grupo chamado INET, tornando possível o acesso às chamadas de sistema associadas.

O Android possui algumas permissões default, que são dividias em 4 categorias, chamadas por níveis de proteção, são estas:

1. Normal - categoria de permissões, que são aceitas automaticamente durante a instalação pelo fato de não resultarem em violação de segurança. Exemplos de permissões incluem: SET_ALARM, SET_WALLPAPER, VIBRATE, FLASHLIGHT, KILL_BACKGROUND_PROCESSES e READ_SETTINGS;
2. Dangerous - permissões que realmente impactam na segurança do usuário e do dispositivo. Essas permissões são informadas ao usuário em tempo de instalação e só são delegadas caso este o aceite. Exemplos incluem: ACCESS_FINE_LOCATION, READ_CALL_LOG, CAMERA, INTERNET e WRITE_SETTINGS;
3. Signature - uma permissão nessa categoria é automaticamente concedida a aplicações assinadas como o mesmo certificado digital da aplicação que a criou, caso contrário, ela é negada. Esse nível de proteção permite o compartilhamento de dados entre aplicações do mesmo desenvolvedor, entretanto, a maior motivação para esse nível é o controle de permissões extremamente críticas. Como tais permissões são criadas por aplicações pré-instaladas, as mesmas só poderão ser acessadas por código assinado pelo fabricante. Exemplos incluem: DEVICE_POWER, HARDWARE_TEST e INJECT_EVENTS;
4. SignatureOrSystem - similar ao nível Signature, contudo, inclui também código da imagem do sistema, ou seja, uma permissão nesse nível é concedida tanto se for requisitada por uma aplicação assinada com o mesmo certificado da aplicação que a criou, como se o for por código que faz parte da imagem do sistema. Concebido visando permitir que os diversos provedores de aplicações do sistema - OHA, fabricante e operadora - possam obter algumas permissões chave. Dentre as permissões nesses níveis encontram-se: ACCESS_CACHE_FILESYSTEM, ACCESS_DOWNLOAD_MANAGER, BACKUP, CALL_PRIVILEGED, DELETE_PACKAGES e SET_TIME.

Além destes 4 grupos de permissões default, o desenvolvedor pode criar seu próprio grupo de permissões, afim de criar controles para acessar serviços

providos por suas próprias aplicações. A figura 2 abaixo ilustra a criação de uma permissão.

Figura 2 – Criação de uma permissão no android manifest

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
   package="com.android.app.myapp" >
   <uses-permission android:name="android.permission.INTERNET" />
   ...
</manifest>
```

Fonte: BRAGA, A. Introdução à Segurança de Dispositivos Móveis Modernos. **researchgate**, 2019.

Já a figura 3 nos mostra a maneira de especificar uma permissão para o funcionamento correto da aplicação.

Figura 3 – Especificando uma permissão para um usuário

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
   package="com.me.app.myapp" >
   <permission android:name="com.me.app.myapp.permission.MY_ACTIVITY"
      android:label="@string/permlab_MyActivity"
      android:description="@string/permdesc_MyActivity"
      android:permissionGroup="android.permission-group.COST_MONEY"
      android:protectionLevel="dangerous" />
   ...
</manifest>
```

Fonte: BRAGA, A. Introdução à Segurança de Dispositivos Móveis Modernos. **researchgate**, 2019.

2.8 FLUTTER

Flutter é uma SDK para desenvolvimento mobile lançada em 2017 pela Google, capaz de criar apps para Android e iOS com um único código. O framework foi totalmente desenvolvido em Dart, uma linguagem de propósito geral criada pela Google e muito similar a C# e Java, compilando código nativo para ARM e x86 (HENRIQUE, 2018).

Além disso, ele possui um renderizador Mobile First que é acelerado pela GPU para que haja consistência da UI entre as plataformas e o dispositivo. Pensando na comodidade para desenvolvedores a Google anunciou um novo framework durante o Mobile World Congress 2018, foi chamado de Flutter e será a linguagem usada neste projeto.

Com este framework é possível criar aplicações multiplataformas de forma muito mais rápida, e com um design fácil de ser modificado e adaptado à particularidade do projeto.

O Flutter possui compatibilidade com ambientes de desenvolvimento como Android Studio, Visual Studio Code e até mesmo Xcode. É uma linguagem baseada em Dart, pois acredita-se que esta é a linguagem “certa” para o tipo de desenvolvimento em questão, o mobile.

2.9 DART

Dart é a linguagem de programação orientada a objetos que também é utilizada no Flutter e que pode ser utilizada tanto do lado do cliente quanto do lado do servidor (DIAS, 2018).

O Flutter é escrito em Dart, uma linguagem concisa, fortemente tipificada e orientada a objetos. Dart tem semelhança a linguagens como Swift, C#, Java e JS (ABRANCHES, 2018).

Dart é mais adequado ao desenvolvimento mobile porque, seu desempenho, tanto no desenvolvimento, quanto em produção suporta a compilação JIT (Just in Time) e a AOT (Ahead of time).

A JIT possibilita que o Flutter recompile o código no dispositivo, enquanto o aplicativo está aberto e rodando, o que faz com que a aplicação não perca o estado de desenvolvimento o que gera um ciclo de desenvolvimento mais rápido e produtivo, possibilitando um carregamento expresso do aplicativo.

Já na compilação AOT, bibliotecas e funções utilizadas pelo código do aplicativo são compilados no código ARM nativo de cada plataforma.

2.10 VISUAL STUDIO CODE

Em 2015 foi lançado pela Microsoft um editor de código destinado ao desenvolvimento de aplicações web chamado de Visual Studio Code, ou simplesmente VSCode. Anunciada durante o Build, evento voltado a desenvolvedores que ocorre nos Estados Unidos anualmente, trata-se de uma ferramenta leve e multiplataforma que está disponível tanto para Windows, quanto para Mac OS e Linux

e atende a uma gama enorme de projetos, não apenas ASP.NET, como também Node.js. Adicionalmente, o editor possui suporte à sintaxe de diversas linguagens como Python, Ruby, C++.

Apesar de seu nome ser semelhante a outro ambiente de desenvolvimento suas semelhanças acabam por aí, este editor tem mais características parecidas com outro ambiente chamado Sublime Text, com funcionalidades otimizadas para certas tarefas.

3 GUIA EDUCACIONAL DE PERMISSÕES ANDROID

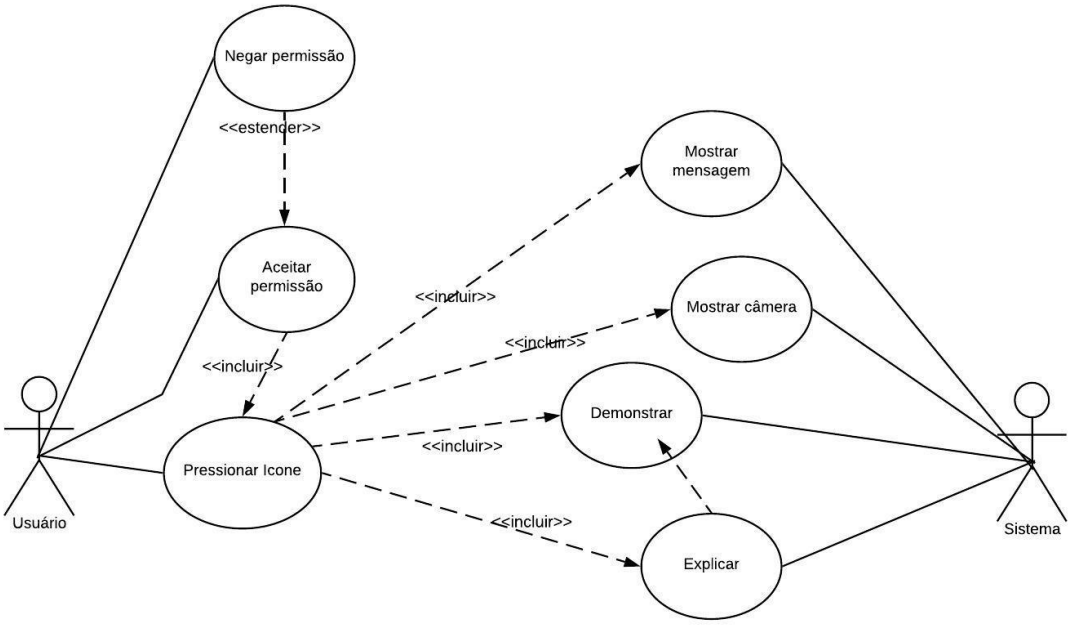
O aplicativo será voltado para a segurança e informação do usuário tendo em mente que queremos conscientizar as pessoas dos perigos que existem em aplicativos maliciosos ou simplesmente mal desenvolvidos, o objetivo do projeto é criar uma aplicação mobile inicialmente desenvolvida para a plataforma Android com o intuito de conscientizar o usuário e mostrar ao mesmo o que acontece por traz do uso das aplicações que são instalados diariamente dando demonstrações e informações.

Como já foi citado em 2.4 no framework Android existem diversas permissões em alguns níveis diferentes, e certos aplicativos ao serem instalados acabam ganhando acesso a tais permissões causando assim vulnerabilidades nas informações ou simplesmente abrindo portas para acessos em outras funções, o objetivo do projeto é trazer essas informações aos usuários de maneira simples e clara, pois muitos não sabem o perigo das permissões, que muitas vezes forçam o usuário a autorizar o acesso, fazendo com que a aplicação não abra ou não funcione corretamente até o usuário ceder e consequentemente, se o aplicativo for malicioso o usuário coloca todas as informações, todo seu smartphone em risco, podendo trazer sérios danos a vida pessoal e ao dispositivo móvel do mesmo.

3.1 DIAGRAMA DE CASOS DE USO

Este diagrama mostra os casos de uso que descrevem as principais funcionalidades do aplicativo e como o sistema reage caso a permissão ao acesso dos dados do mesmo seja concedida ou não.

Figura 4 - Diagrama de casos de uso

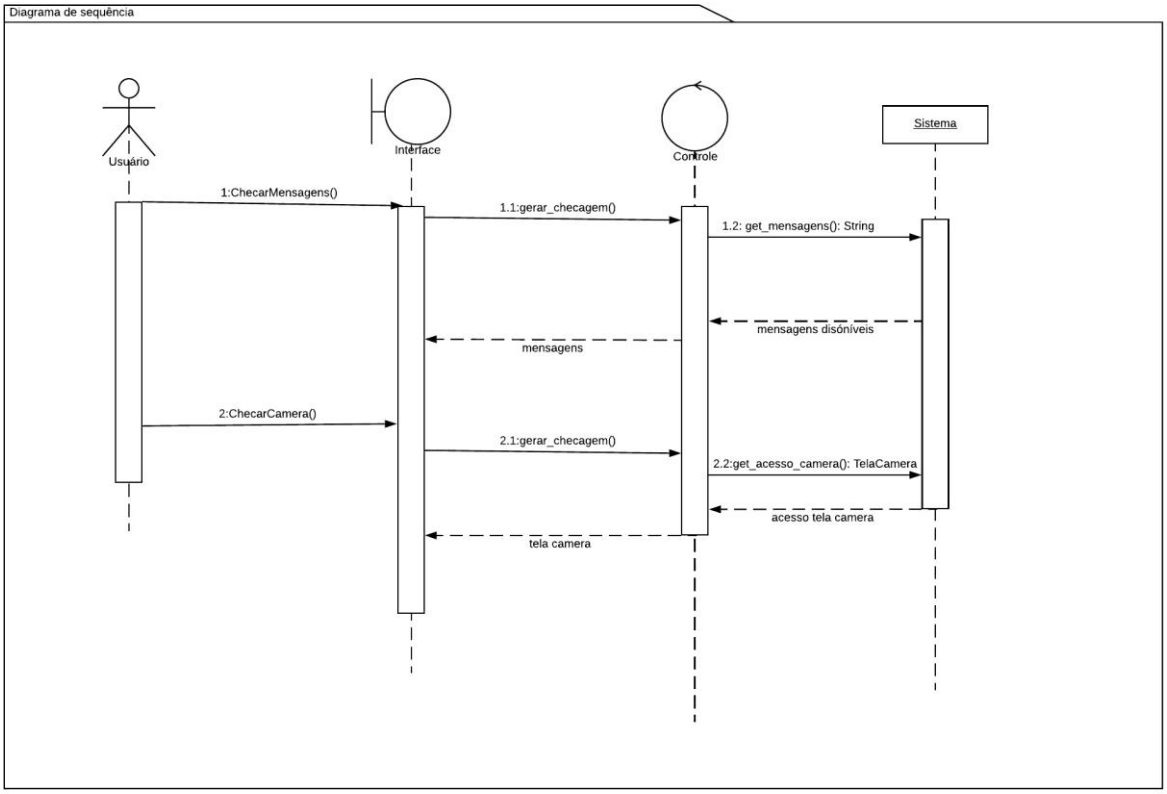


Fonte: (autoria própria)

3.2 DIAGRAMA DE SEQUENCIA

Este diagrama explica a sequência de ações tomadas durante o uso do aplicativo

Figura 5 - diagrama de sequência

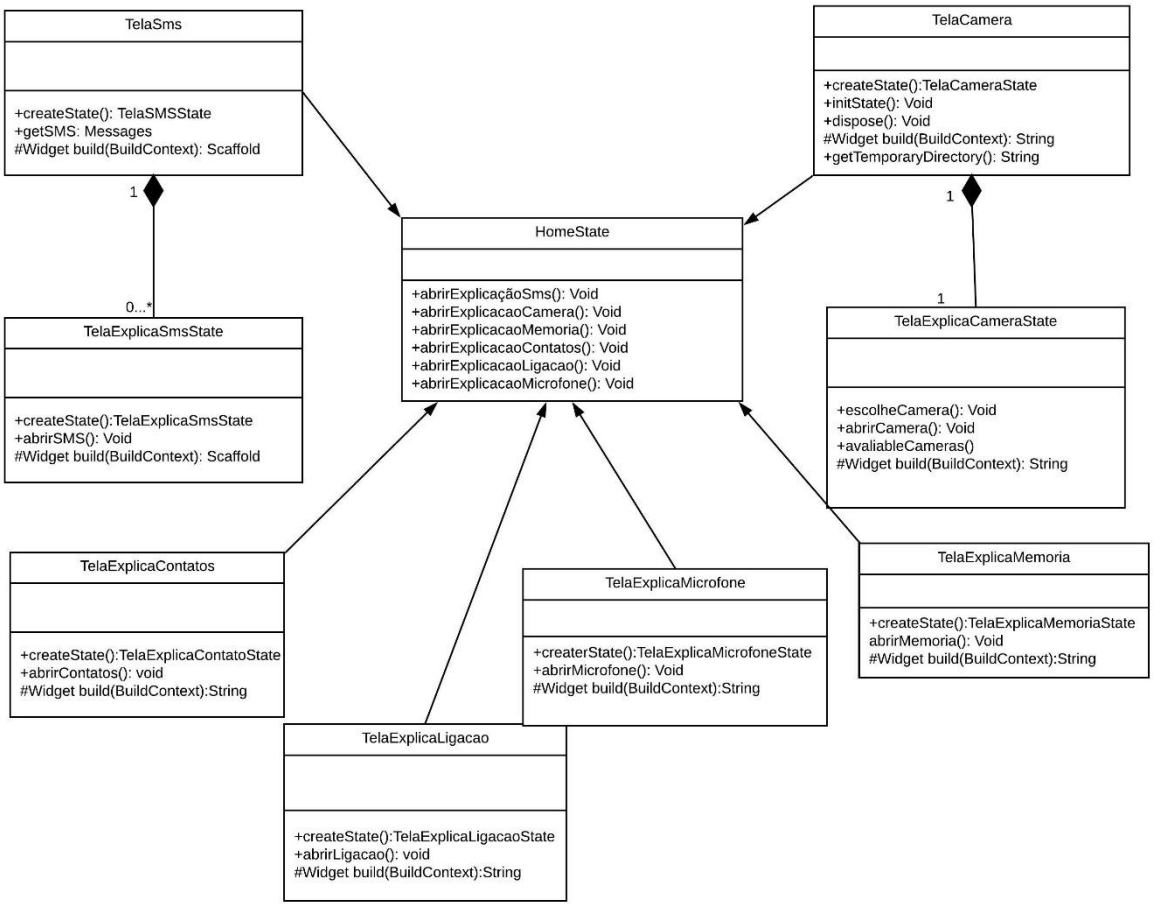


Fonte: (autoria própria)

3.3 DIAGRAMA DE CLASSES

Este diagrama ilustra as classes utilizadas durante a programação e a estrutura do código para melhor entendimento de seu funcionamento.

Figura 6 - Diagrama de classes

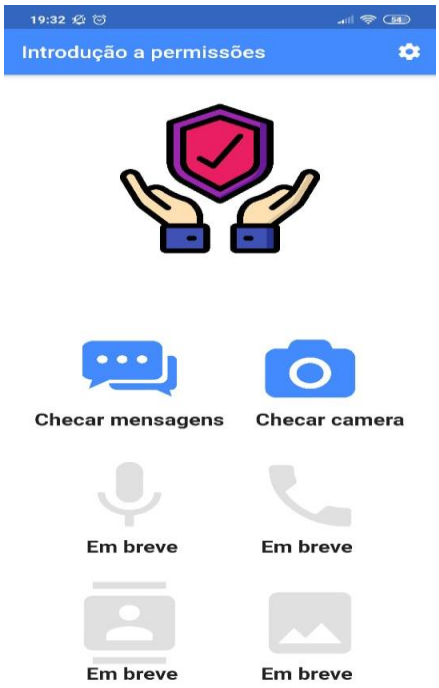


Fonte: (Autoria própria)

3.4 ESCOPO DO PROJETO

Sua principal característica é trazer uma introdução, um guia educacional das permissões dos aplicativos de dispositivos móveis na plataforma Android, trazemos os ícones das aplicações que serão introduzidas ao usuário com demonstrações e textos explicando as mesmas, como funcionam, o que elas podem ter acesso e o que pode ser feito a partir do mesmo, como desvio dessas informações, roubos de dados pessoais e até mesmo acesso a contas do usuário que será o alvo. Como mostrado na figura 7 temos uma tela inicial.

Figura 7 – Tela inicial

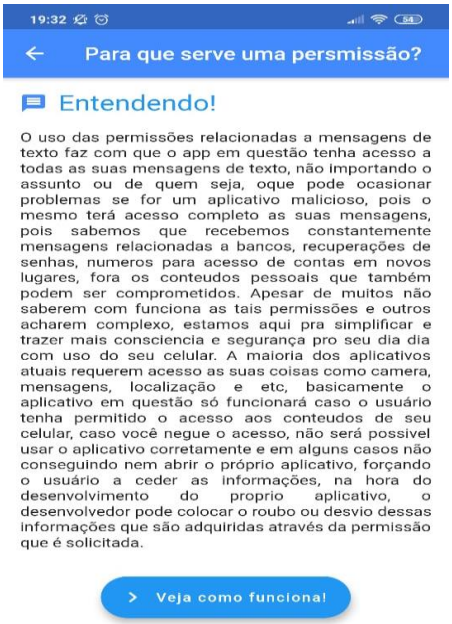


Fonte: Autoria própria

Nesta tela visualiza-se o logo do aplicativo juntamente com as permissões que serão checadas e introduzidas ao usuário, como mostrado na tela, temos mensagens e câmera, os outros serão adicionados com o tempo.

Na figura 8 temos a segunda tela, a introdução ao usuário das informações do uso das permissões de SMS (serviço de mensagem de texto) e abaixo o botão para a demonstração de como funciona.

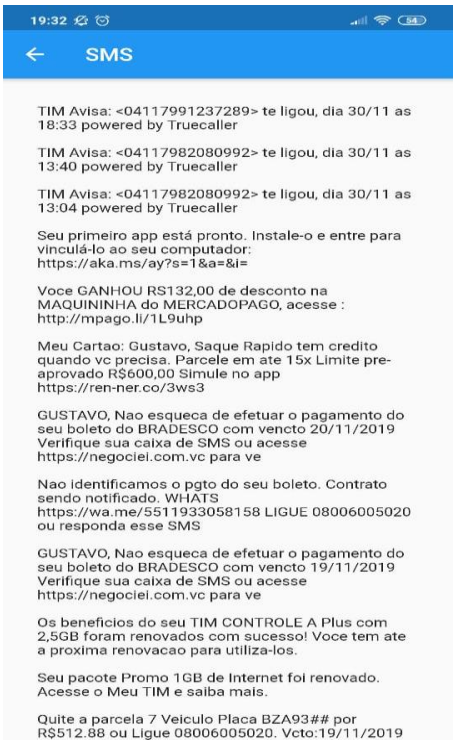
Figura 8 – Entendendo como funciona a permissão de SMS



Fonte: Autoria própria

Ao pressionar o botão “Veja como funciona!” na figura 8 as últimas mensagens do usuário serão disponibilizadas na tela como mostrado na figura 9, todas as mensagens que foram recebidas, não importando o assunto ou quem seja que tenha enviado a mensagem ao usuário.

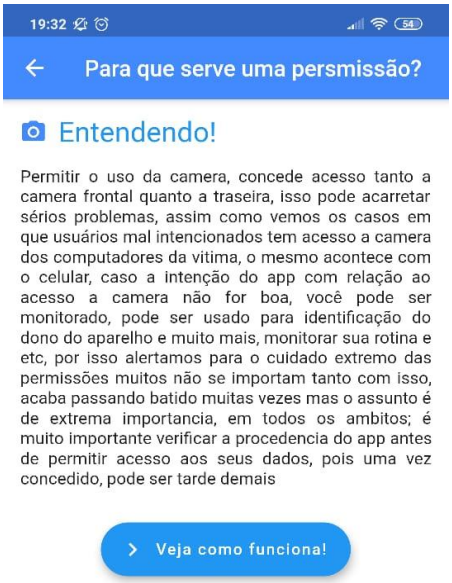
Figura 9 – Checagem dos SMS disponíveis no aparelho



Fonte: Autoria própria

Pressionando o ícone da câmera mostrado na figura 7, abrimos uma tela com informações sobre as permissões da câmera e um botão para o usuário acessar a câmera que é redirecionada para a tela do aplicativo como mostrado na figura 10 podendo tirar uma foto, a mesma é congelada e exibida em seguida ao usuário.

Figura 10 – Entendendo como funciona a permissão de Câmera



Fonte: (autoria própria)

4 CONCLUSÃO

Com muitos estudos relacionados à segurança da informação, TICs (Tecnologias da informação e comunicação) e entender como as pessoas usam seus smartphones, foi desenvolvido um guia educacional e informativo para trazer conhecimento e entendimento sobre os problemas relacionado as permissões. A segurança da informação é de extrema importância quando se trata da evolução massiva da tecnologia, a mesma pode acarretar uma série de problemas, de perigos, comprometer suas informações, seus dados, tendo em vista esses problemas todos, o guia informativo foi desenvolvido com o propósito de conscientizar as pessoas, trazer demonstrações de forma simples, não complexa, mostrando que é possível evitar certas situações problemáticas.

Satisfeito o objetivo de criar um guia educacional e informativo sobre a segurança da informação no mundo dos dispositivos móveis o aplicativo satisfaz aquilo que foi proposto, trazendo um conjunto demonstrativo e explicativo para o usuário, que pode levar a redução dos riscos que existem no mundo da tecnologia. Tendo em vista uma futura evolução, é visto que a implementação de mais funções sobre a segurança da informação, como testes de conhecimento após toda a informação que é levada ao mesmo e a demonstração de outras funções relacionadas as permissões e segurança dos dados e da informação que é carregada diariamente dentro do dispositivo móvel.

5 REFERENCIAS BIBLIOGRÁFICAS

Afonso, V. (2019). ***Tendências do mercado nacional: procurando malware em aplicações Android***.Disponível em: http://www.brunoribas.com.br/sc/2016-1/apresentacoes/muriel/artigo-android.pdf, Acesso em 12 de 04 de 2019

Braga, A. (2019). ***Introdução à Segurança de Dispositivos Móveis Modernos*****.** Disponível em: https://www.researchgate.net/profile/Alexandre_Braga2/publication/273458482_Introducao_a_Seguranca_de_Dispositivos_Moveis_Modernos-Um_Estudo_de_Caso_em_Android/links/5655d51808aeafc2aabe2c6b/Introducao-a-Seguranca-de-Dispositivos-Moveis-Modernos-Um-Estudo-de-Caso-em-Android.pdf Acesso em 12 de 04 de 2019

Americo, J. (2018). ***Entenda mais sobre as permissões que os aplicativos pedem nos smartphones*****. (2019)**. Disponível em: https://olhardigital.com.br/lu-explica/noticia/entenda-mais-sobre-as-permissoes-que-os-aplicativos-pedem-nos-smartphones/74500 Acesso em 24 de 05 de 2019

Google. (2019). ***Arquitetura Android***. Disponível em: < https://source.android.com/devices/architecture> Acesso em 23 de 04 de 2019

google. (2019). *Secure an Android Device*. Disponível em: https://source.android.com/security Acesso em 23 de 04 de 2019

Medeiros, A. (2019). ***ANÁLISE DE SEGURANÇA NA PLATAFORMA ANDROID***. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2014-Sombra_Helder.pdf Acesso em 12 de 04 de 2019

Microsoft. (2019). ***Introdução ao visual studio code***., disponível em: https://www.devmedia.com.br/introducao-ao-visual-studio-code/34418 Acesso em 25 de 05 de 2019

Novo, T. (2019). ***SEGURANÇA DA INFORMAÇÃO NO USO DE SMARTPHONES EM AMBIENTE CORPORATIVO****.* Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/809/1/CT_TELEINFO_XX_2012_12.pdf Acesso em 23 de 04 de 2019

Pulsus. (2019). ***Os sistemas mais vulneráveis para invasões em smartphones em 2017***. Disponível em: https://pulsus.mobi/os-sistemas-mais-vulneraveis-para-invasoes-em-smartphones-em-2017/ Acesso em 20 de 03 de 2019

Schse, N. (2019). ***Avaliação comparativa do modelo de segurança do Android***. Disponível em: https://bdigital.ufp.pt/bitstream/10284/1960/2/DM_12464.pdf Acesso em 12 de 04 de 2019

Souza, L. C. (2019). ***Os novos vilões da sua privacidade: as permissões dos seus aplicativos – Parte 1: smartphones***. Disponível em: https://blog.avast.com/pt-br/os-novos-viloes-da-sua-privacidade-as-permissoes-dos-seus-aplicativos-parte-1-smartphones Acesso em 23 de 05 de 2019