Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

O sistema Android e suas vulnerabilidades na privacidade dos usuários

NILTON SILVEIRA CORREA JUNIOR

Americana, SP
2017

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

O sistema Android e suas vulnerabilidades na privacidade dos usuários

NILTON SILVEIRA CORREA JUNIOR

niltoncorr@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob a orientação da Profa. Dra. Acácia Ventura.

Área: Fator Humano e Segurança da Informação

Americana, SP
2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

C843s CORREA JUNIOR, Nilton Silveira
O sistema Android e suas vulnerabilidades na privacidade dos usuários. / Nilton Silveira Correa Junior. – Americana, 2017.
45f

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza
Orientador: Profa. Dra.Acácia de Fátima Ventura

1. Segurança em sistemas de informação 2. Android – aplicativos I. VENTURA, Acácia de Fátima II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.518.5
681.519

NILTON SILVEIRA CORREA JUNIOR

O sistema Android e suas vulnerabilidades na privacidade dos usuários

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Fator Humano e Segurança da Informação

Americana, 11 de Dezembro de 2017

Banca Examinadora:

Acácia Ventura (Presidente)
Doutora
FATEC – Americana

Eduardo Antonio Vicentini (Membro)
Mestre
FATEC – Americana

Elton Rafael Maurício da Silva Pereira (Membro)
Mestre
FATEC – Americana

AGRADECIMENTOS

Agradeço ao meu pai Nilton e minha mãe Sandra pela confiança e apoio dado para chegar até aqui, à todos da minha família que me ajudaram nos momentos difíceis e a todo o apoio dado.

Para minha namorada Graziela Ferrari, agradeço por passar os dias me dando forças a continuar e conseguir ir em frente, a todos meus amigos que passaram esse tempo até hoje, se eu amadureci e consegui a culpa é de vocês, muito obrigado.

Um agradecimento especial aos professores e orientadores, Prof. Acácia Ventura, Prof. Maria Cristina Aranda e Prof. Maria Cristina Luz, por guiarem este trabalho, dando ideias, dicas e orientações para que este trabalho fosse possível.

DEDICATÓRIA

A todos que me apoiaram, meus pais, minha família, amigos e professores que estiveram presente no processo deste trabalho.

EPÍGRAFE

“Só se pode alcançar um grande êxito quando nos mantemos fiéis a nós mesmos”.

(Friedrich Nietzsche)

RESUMO

Este trabalho tem como objetivo mostrar a vulnerabilidade de privacidade no sistema operacional *android*, e como seus usuários estão expostos a ameaças diante da exposição de suas informações e o aceite dos termos de uso pré impostos pelo sistema. O estudo aborda a segurança da informação como base e o usuário como o elo mais fraco da segurança. Descreve as vulnerabilidades de segurança, com foco na privacidade. Analisa a vulnerabilidade de privacidade, termos de uso e permissões de acesso, a obrigatoriedade do aceite dos termos e o monitoramento que o sistema emprega utilizando registros. Foi aplicado um questionário nos alunos do quinto semestre do Curso Superior em Segurança da Informação e os dados coletados foram analisados com o auxilio do livro de George Orwell “1984”, observando o ponto do usuário que está sendo monitorado.

Palavras chaves: Privacidade; Segurança da Informação; Vulnerabilidade; *Android*; Termos de Uso; Permissões.

ABSTRACT

This work aims to show the privacy vulnerability in the android operating system, and how its users are exposed to threats by exposing their information and accepting the terms of use pre-imposed by the system. The study addresses information security as the basis and the user as the weakest security link. Describes security vulnerabilities with a focus on privacy. It analyzes the privacy vulnerability, terms of use and access permissions, the mandatory acceptance of the terms and the monitoring that the system employs using records. A questionnaire was applied to the students of the fifth semester of the Higher Course in Information Security and the data collected were analyzed with the help of George Orwell's book "1984", observing the point of the user being monitored.

Keywords: Privacy; Information security; Vulnerability; *Android*; Terms of Use, Permissions.

LISTA DE FIGURAS E DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

Com a ascensão das redes sociais e dispositivas *mobiles*, a vulnerabilidade de privacidade vem sendo bem comentada entre os usuários, sendo assim, a segurança começa a se tornar essencial para o uso desses equipamentos, seja para o usuário corporativo ou apenas usuário comum.

Os dispositivos *mobiles,* mais especificamente, o *Android*, que é abordado neste trabalho, está tomando o lugar dos *desktops* por ser mais prático e acessível. De acordo com a pesquisa realizada pela Opus Software (12/2015, s/p): “No final de 2014 o Brasil já era o 6º mercado mundial de *smartphones*, superado apenas por China, EUA, Índia, Japão e Rússia; 88% dos brasileiros que possuem *smartphone* usam o aparelho para trocar mensagens”.

Foi observado que já no começo de todo o processo do *android*, o mesmo faz a obrigação de um email Google para a utilização e funcionalidade perfeita do sistema e só depois te dá opção para adicionar contas de outros serviços, verificando a “obrigação” de aceitar os termos, caso não for aceito não passará a finalização e não conseguirá utilizar o serviço.

Foi estudada também a vulnerabilidade e ameaças que usuários com ou sem conhecimento dos termos e permissões estão correndo ao trazerem todas suas informações ao público.

A partir do exposto o estudo se **justifica** pela importância de discutir e apresentar ao leitor as vulnerabilidades de privacidade contidas na Política de Privacidade, termos de uso e permissões do Google para o sistema *android,* bem como, destacar pontos de segurança do mesmo e apontar onde o usuário poderia estar protegido ou desprotegido.

Do ponto de vista acadêmico o texto se justifica pelos pilares fundamentais para a segurança de dados, são eles: autenticidade, disponibilidade, integridade, confidencialidade e confiabilidade. Destacando que cada pilar tem seu objetivo o estudo discute as ameaças que tais pilares sofrem e destaca para os usuários,

segurança com relação as suas informações *onlines* e as Políticas de Privacidade do Google apresentando as vulnerabilidades e ameaças que o usuário está exposto.

Já no aspecto social foi observado que a maioria das pessoas utiliza plataformas sociais na internet e que ignoram várias questões, bem como o Google que tem sido o maior influenciador de plataformas pelo seu sistema *android*, é de grande importância ter conhecimento dos termos de uso, privacidade e pensar nas ameaças que podem acarretar ao colocar informações públicas nessas plataformas.

E para o aluno pesquisador, a importância do estudo está nas observações de vários fatores e vulnerabilidades na plataforma, sendo as informações obtidas para a geração de anúncios e informações públicas. Curioso com tecnologia e informação, o interesse foi entender as ameaças e consequências que os usuários atualmente trazem sem ter o conhecimento do que estão colocando de informação. Atualmente o Google vem sendo utilizado praticamente todos os dias pelos usuários e, todas as ferramentas oferecidas tem seu termo de Privacidade e o estudo se propõe a analisar se os usuários estão de acordo com esses Termos ou se querem sabem das consequências e ameaças de colocar suas informações nas plataformas.

O **problema** consistiu nos usuários serem obrigados a aceitarem os termos oferecidos pelo Google, sendo que a plataforma é utilizada por uma parcela grande de usuários no Mundo todo. De acordo com a notícia publicada pelo Jornal “O dia” (17/05/2017 s/p), com o nome: “*ANDROID* ULTRAPASSA MARCA DE 2 BILHÕES DE USUÁRIOS ATIVOS POR MÊS”, e ter observado que o sistema *android* utiliza todas as ferramentas do Google, o usuário fica preso e “obrigado” a aceitar os termos de todas as plataformas oferecidas, caso contrário se limita a aplicativos de terceiros que não são muito utilizados e até mesmo aceitar os termos sem o consentimento para que possa usar as plataformas.

A **pergunta** foi: identificar como a Segurança da Informação pode influenciar usuários a terem o conhecimento da vulnerabilidade de Privacidade?

As **hipóteses** levantadas foram: a) O usuário tem conhecimento dos termos, sabendo das consequências e ameaças, o mesmo não aceita, assim sendo bloqueado à etapa de finalização da conta de algum serviço e acarretando a não utilizar as plataformas, essas que são usadas por bilhões de usuários; b) O usuário desconhece os termos; não têm noção das ameaças e aceita mesmo assim, o que levam seus dados a serem vulneráveis e, c) O usuário que leu os termos, não o aceitando é bloqueado antes do passo de finalização do registro, plataforma/serviço usado mundialmente por uma parcela considerável da população; já o que não leu e não tem noção das ameaças, concordando com os termos, é finalizado o seu registro.

O **objetivo geral** consistiu em estudar as vulnerabilidades da privacidade do usuário do *android*/Google, objetivando analisar esse fator em *smartphones* com sistema operacional *android*, através de uma pesquisa de campo com alunos do quinto semestre, ultimo ano dos cursos de Tecnologia da Informação da FATEC Americana.

Os **objetivos específicos** foram: a) fazer um levantamento bibliográfico sobre segurança da informação, destacando a importância do estudo das vulnerabilidades apresentadas no Google; b) Estudar o sistema operacional *android* para *smartphones*, visando identificar a vulnerabilidade de privacidade, pontuando: termos de uso, acessos efetuados pelos usuários e o desconhecimento pelos mesmos das políticas de privacidade, através de uma pesquisa de campo, buscando compreender as vulnerabilidades a que estão submetidos quando inserem dados em redes sociais/*smartphones*, baseado no sistema Google e, c) Discutir as teorias estudadas atrelando-as aos dados colhidos na pesquisa de campo, ressaltando a importância de o usuário conhecer suas vulnerabilidades, bem como as consequências de deixar informações particulares se tornarem públicas.

O **método** utilizado foi o hipotético-dedutivo que para Gil (1999, p.30):

> Das hipóteses formuladas, deduzem-se consequências que deverão ser testadas ou falseadas. Falsear significa tornar falsas as consequências deduzidas das hipóteses. Enquanto no método dedutivo se procura a todo custo confirmar a hipótese, no método

> hipotético-dedutivo, ao contrário, procuram-se evidências empíricas para derrubá-la.

A **pesquisa** foi classificada de acordo com sua natureza como básica: “Objetiva gerar conhecimentos novos, úteis para o avanço da Ciência, sem aplicação prática prevista. Envolve verdades e interesses universais.” (GERHARDT e SILVEIRA, 2009, p.34).

Do ponto de vista da forma de abordagem do problema, foi utilizada a pesquisa Qualitativa que para (DESLAURIERS, 1991, p. 58 apud GERHARDT; SILVEIRA, 2009, p. 32):

> Na pesquisa qualitativa, o cientista é ao mesmo tempo o sujeito e o objeto de suas pesquisas. O desenvolvimento da pesquisa é imprevisível. O conhecimento do pesquisador é parcial e limitado. O objetivo da amostra é de produzir informações aprofundadas e ilustrativas: seja ela pequena ou grande, o que importa é que ela seja capaz de produzir novas informações.

E também foi utilizada a pesquisa Quantitativa, esclarece Fonseca (2002, p. 20 apud GERHARDT; SILVEIRA, 2009, p. 33): “[...] A pesquisa quantitativa se centra na objetividade. Influenciada pelo positivismo, considera que a realidade só pode ser compreendida com base na análise de dados brutos, recolhidos com o auxílio de instrumentos padronizados e neutros [...]”.

Para que os objetivos fossem atingidos foi utilizada a pesquisa descritiva que segundo GIL (2008, p. 28):

> As pesquisas deste tipo têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados.

Para os procedimentos técnicos utilizou estudo de caso que “é caracterizado pelo estudo profundo e exaustivo de um ou de poucos objetos, de maneira a permitir o seu conhecimento amplo e detalhado, tarefa praticamente impossível mediante os outros tipos de delineamentos considerados”. (GIL, 2008, p.57).

Este trabalho foi desenvolvido em três capítulos, em que o **primeiro** conceitua a teoria da segurança da informação, a importância do usuário e vulnerabilidades conhecidas para a compreensão do leitor ao fundamento da segurança e as maiores vulnerabilidades de segurança atualmente; o **segundo** estuda o conceito do sistema operacional *android* e sua vulnerabilidade de privacidade, permissão e termos de uso, com base no estudo de caso realizado; o **terceiro** conclui às considerações finais.

1 SEGURANÇA DA INFORMAÇÃO E SUAS VULNERABILIDADES

Atualmente a informação está se expandindo de forma muito intensa na *web*. Usuários compartilham informações a todo o tempo, gerando riscos para si mesmos, usuários, que sempre foram e sempre serão os elos mais frágeis da segurança, assim colocam informações públicas na *web* sem saber as consequências às quais estão correndo e as ameaças que essas informações públicas podem trazer no meio digital. Neste capítulo serão abordados conceitos de segurança da informação e seus pilares essenciais juntamente com o fator humano e as vulnerabilidades existentes.

1.1 SEGURANÇA DA INFORMAÇÃO

"Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição". (ARAUJO, 2008, s/p).

A segurança da informação é uma área que estuda e preserva informações, dados e arquivos de uma empresa/usuário, desde simples informações até informações de maior relevância. De acordo com Sêmola (2003, p. 43): "A segurança da informação é tida como uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade".

A norma NBR ISO/IEC 17799 (ABNT, 2005, p. ix) afirma que a Segurança da Informação é: "Especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades".

Os usuários têm grande importância em relação à segurança da informação, pois são considerados elementos chave, contribuindo e fazendo parte de uma parcela de informações. Estar ou usar um ambiente de tecnologia exige os cuidados e medidas para guardar as informações com segurança.

> No ambiente de tecnologia as informações também podem ser alvo de ações criminosas [...] É muito mais produtivo, e muitas vezes mais seguro, fazer uma transação pela Internet do que ter de se dirigir fisicamente a uma agência de instituição financeira [...] Você é responsável pelos acessos que realiza na Internet [...] Um dos primeiros locais onde qualquer pessoa de fora da organização pode obter informação é no lixo. Damos gratuitamente muitas informações da organização ao jogá-las no lixo. (FONTES, 2005, p 45).

1.1.1 Pilares da Segurança da Informação

A segurança da informação está relacionada à proteção quanto a vários tipos de ameaças. Ao se falar em segurança da informação devem-se levar em consideração os vários papéis que a englobam. Existem cinco pilares essenciais para a segurança da informação, porém neste trabalho serão focados apenas três deles (integridade, disponibilidade e confidencialidade), pois tem ligação direta com as questões aqui discutidas.

De acordo com a ABNT (2005), os pilares de Segurança da Informação são:

- **Integridade** é a garantia da exatidão e completeza da informação e dos métodos de processamento
- **Disponibilidade** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário
- **Confidencialidade** é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

Outros autores citam mais dois pilares como essenciais, como Sêmola (2011) que cita:

- **Autenticidade**: é a garantia de que a informação é oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal
- **Não repúdio**: é a garantida de que a informação chegará ao destino certo e não será repudiada.

Observa-se que os pilares sofrem quebras com a vulnerabilidade de Privacidade, Dantas (2011, p. 11) diz: “Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja

legítima e permaneça consistente”. A quebra é feita às informações que os usuários deixam públicas levando-a ao uso indevido por qualquer pessoa, o usuário inclui as informações em uma plataforma e não imagina que elas possam ser modificadas para fazer algum mal ou denegrir sua imagem.

É importante destacar na vulnerabilidade de privacidade a quebra da confidencialidade que para Dantas (2011, p. 14), é: “[...] a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.”

A quebra da confidencialidade acontece pelo fato dos usuários não terem conhecimento do que estão disponibilizando publicamente e o que os termos de uso dizem a respeito da divulgação das informações públicas.

1.1.2 Fator Humano na Segurança da Informação

Partindo da segurança da informação, pode-se perceber que o fator humano na segurança pesa em relação à parte física e lógica, pois a tecnologia é operada por mentes e ações humanas. Pensa-se, muitas vezes, na estrutura física e lógica e se esquece que o usuário é a chave de tudo, sem um conhecimento adequado ele pode levar tudo a perder com alguns atos.

Sêmola (2003, p. 18) diz: “A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.”.

As considerações do autor podem ser melhor representada pela Figura 1:

Figura 1 - Representação da divisão da segurança em camadas

Fonte: Teleco.

1.2 VULNERABILIDADES

Vulnerabilidades são fragilidades que de alguma forma podem vir a provocar danos e consequências. A ABNT (2005) define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Também podendo ser aplicado a pessoas e grupos sociais.

1.2.1 A exploração de vulnerabilidades

Mesmo com o avanço da tecnologia, as vulnerabilidades têm sido exploradas por todos. Começando pelos primórdios da humanidade as vulnerabilidades já eram exploradas pelos povos para conseguir um objetivo. Naquela época era para sobrevivência, nos dias atuais não é diferente, tirando o fato de existir uma civilização moderna com tecnologias, mas mesmo assim a maioria das pessoas explora alguma vulnerabilidade para conseguir algo. Vulnerabilidades estão em todos os lugares, seja em locais, objetos e na tecnologia. Procurar vulnerabilidades não é crime, porém existem tipos de consequências, existem àqueles que buscam a vulnerabilidade para criar um relatório para ajudar a empresa envolvida e também existem os que procuram para causar dano e, se feito terá consequências de lei do país.

São conhecidos como *hackers* os que procuram vulnerabilidades, mas não a exploram, relatam para um órgão competente ou para a própria empresa vulnerável, e também os *crackers* que exploram vulnerabilidades para causar danos nas

informações, roubo e fraude. Segundo a lei Carolina Dieckmann 12.737 Art. 154A (BRASIL, 2012, s/p):

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave [...]

1.2.2 Vulnerabilidades de segurança

Beal (2005, *apud* DANTAS, 2011, p. 26) define a vulnerabilidade como uma fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque e para Sêmola (2003, *apud* DANTAS, 2011, p. 26), as vulnerabilidades são fragilidades presentes ou associadas aos ativos de informação, que, ao serem exploradas, permitem a ocorrência de incidente na segurança da informação.

> Vulnerabilidades são fragilidades que podem provocar danos decorrentes da utilização de dados em qualquer fase do ciclo de vida das informações. Como podem ser verificadas, as vulnerabilidades estão relacionadas diretamente com as fragilidades. DANTAS (2011, p. 26).

As invasões se tornam muito comuns quando a vulnerabilidade é padrão, em *web*, observam-se ameaças comuns há vários anos, pois a aplicação nunca será 100% segura de acordo com o avanço de novas tecnologias e novos métodos. De

acordo com a Tabela 1, os dez riscos de segurança mais críticos em aplicações *web*, top 10 da *OWASP* em 2013*:*

Tabela 1: OWASP – Principais invasões em 2013

A1 – Injeção de código
A2 – Quebra de autenticação e Gerenciamento de Sessão
A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos
A5 – Configuração Incorreta de Segurança
A6 – Exposição de Dados Sensíveis
A7 – Falta de Função para Controle do Nível de Acesso
A8 – Cross-Site Request Forgery (CSRF)
A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos

Fonte: OWASP TOP 10 (2013, p. 5).

1.2.3 Vulnerabilidades de tecnologia

Vulnerabilidades na Tecnologia da Informação (TI) são vulnerabilidades locais para conseguir informações físicas da empresa, isso é feito por uma pessoa que consegue obter seu objetivo (Engenharia Social), como também conseguir por meio do computador ou dispositivos móveis, procurando em softwares internos ou na *web*.

Os atacantes procuram vulnerabilidades em códigos fonte de programas. Apesar de não serem rápidos e eficazes, os códigos estão cada vez mais complexos e criptografados, mas quando conseguem o acesso a vulnerabilidade pode obter informações importantes para mudarem alguma característica do sistema/página ou controle total dos mesmos.

> Para se ter uma idéia (sic) mais clara do mundo real, no período de 2001 a 2006, o número de vulnerabilidades em sistemas reportado

> ao *Common Vulnerabilities and Exposures*, simplesmente, triplicou. O estouro de pilha, campeão da lista por muitos anos consecutivos, perdeu o lugar, a partir de 2005, para vulnerabilidades de injeção de código, como *o cross-site scriping* e *injeção SQL* [...] (UTO; Melo, 2015).

1.2.4 Vulnerabilidade humana

O desconhecido acaba gerando preocupação, a vulnerabilidade humana é uma preocupação à Segurança da Informação, pois mesmo nos tempos de hoje em que a tecnologia está avançando cada vez mais, muitas pessoas ainda não tem conhecimento de como utilizar de forma segura, o que acaba gerando preocupação a especialistas. Para Dantas (2011, p. 28) a origem da vulnerabilidade humana é a:

> [...] Falta de capacitação específica para a execução das atividades inerentes às funções de cada um; falta de consciência de segurança diante das atividades de rotina; erros; omissões; descontentamento; desleixo na elaboração e segredo de senhas no ambiente de trabalho; não utilização de criptografia na comunicação de informações de elevada criticidade, quando possuídas na empresa.

1.2.5 Vulnerabilidades de privacidade

Muitas vezes, os usuários sabem e conseguem entender as vulnerabilidades comuns à Segurança da Informação e acabam esquecendo-se ou não se preocupando com a ascensão das redes e mídias sociais que levam ao surgimento de novos tipos de vulnerabilidades, muitas delas atingindo a privacidade desses usuários.

Ao realizar uma busca utilizando um algoritmo simples de pesquisa, o usuário deixa seu rastro por onde passou, o que pesquisou e do que precisa, deixando assim um banco de dados de informação a seu respeito, para posteriormente empresas ou pessoas usarem e ganharem dinheiro em cima disso, por exemplo: buscando “como trocar fralda do meu filho”. Na figura 2 observa-se um trecho dessa pesquisa:

Figura 2: Pesquisa no buscador Google

Fonte: Próprio autor.

O buscador consegue obter vastas informações sobre a pessoa e gera um tipo de log da vida da pessoa, como é observado no Google My Activies. O Google My Activies que será melhor abordado no capítulo 2 deste trabalho é uma ferramenta desenvolvida pelo Google para o usuário ter controle de tudo o que faz e vê, deixando tudo registrado em sua página de históricos.

Essa vulnerabilidade está crescendo muito e os usuários precisam ficar em alerta quanto a isso, pois sua privacidade está sendo monitorada e registrada, e caso caia em mãos erradas, toda sua vida está lá podendo ser usado contra. Essa vulnerabilidade de privacidade é, muitas vezes, ignorada ou passa despercebida pelo usuário.

1.2.6 Vulnerabilidade de permissão

É necessário entender que a privacidade, muitas vezes, não é o que se quer, e na internet muito menos, os usuários são bombardeados de termos de uso e permissões que nem sequer ler e isso acarreta uma falha grotesca de privacidade, como observado na Figura 3, a imagem de permissões de uso de Microfone em um smartphone *android*.

Figura 3: Permissões do Microfone em smartphone Android

Fonte: Android.

Não é só em periféricos e equipamentos que as pessoas estão vulneráveis. Segundo pesquisa realizada por Rudd (2015 s/p):

> Um britânico tem sua imagem filmada ou fotografada mais de 300 vezes ao dia. Essa exposição a que estamos sujeitos tem várias aplicações, como em lojas ou supermercados, que, através do reconhecimento facial ou por outro meio, como câmeras de vigilância, conseguem personalizar ofertas e produtos para determinados clientes, mas também abrem espaço para pessoas mal-intencionadas capturarem os seus dados e depois os utilizarem de maneiras escusas.

Podemos observar que todos estão propícios a vulnerabilidades, e como o *android* é um dos sistemas operacionais mais utilizados e de código aberto, temos como consequência à vulnerabilidade de privacidade, termos e permissão imposta pelo sistema.

2 ANDROID

O capitulo abordará sobre o *android* e seu código aberto, vulnerabilidade de privacidade em relação às permissões, termos de uso e sua obrigação de aceite, com foco no estudo de caso realizado na turma do 5º semestre do curso de Tecnologia de Segurança da Informação, analisando os resultados relacionando com base no livro 1984 de George Orwell.

2.1 ANDROID E CÓDIGO ABERTO

O *android* é um sistema operacional baseado em Linux desenvolvido pela Google, de acordo com dados da consultoria IDC, 95% dos *smartphones* comercializados entre junho e julho de 2016 rodavam o sistema *android*.

Quando liga o *smartphone* a primeira coisa a carregar é o sistema operacional, ele é responsável por interligar todo o *hardware*, *softwares* e acessórios, cria uma conexão entre a memória, disco, e a interface para o usuário com os aplicativos e programas.

Hoje o *android* está em sua versão 7.0 (Nougat), e de acordo com (*Android*, 2016, s/p) todas as versões do *android* são: 1.6 Donut; 2.1 Eclair; 2.2 Froyo; 2.3 Gingerbread; 3.0 Honeycomb; 4.0 Ice Cream Sandwich; 4.1 Jelly Bean; 4.4 KitKat; 5.0 Lollipop; 6.0 Marshmallow e, 7.0 Nougat.

Como o *android* utiliza *Kernel* Linux, que é responsável por gerenciar todos os processos acaba a ser muito vulnerável, pois existe a possibilidade de ser alterado pelo *Kernel*, por ser de código aberto. Inserção de códigos maliciosos e alteração de permissões são uma das vulnerabilidades mais comuns atualmente

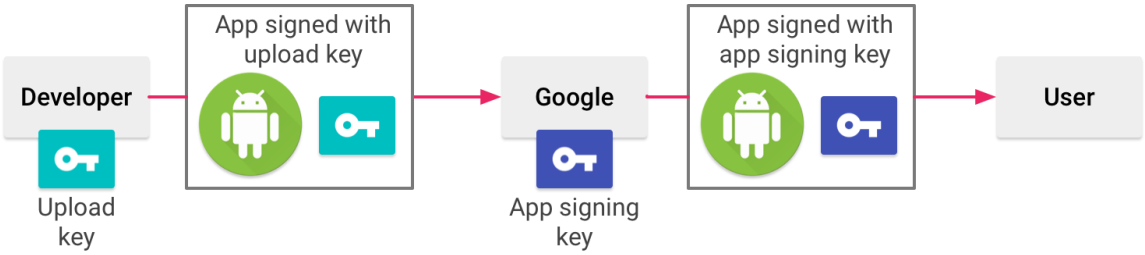
Pereira e Silva (2009, p. 4) ressaltam:

> Como é executado em um kernel Linux, toda vez que um aplicativo for instalado em uma estação *Android*, é criado um novo usuário Linux para aquele programa, com diretórios que serão usados pelo aplicativo, mas somente para aquele usuário Linux. Como os aplicativos ficam completamente isolados uns dos outros, qualquer

> tentativa de acessar informações de outro aplicativo precisa ser explicitamente autorizada pelo usuário, podendo ser negada a instalação do aplicativo, ou autorizada a instalação, mas controlando as permissões que este aplicativo poderá ter através de um mecanismo de permissão.

Em contrapartida todas as aplicações precisam ter um certificado de chave privada de criptografia digital que ressalta um pouco a segurança e cria uma confiança a mais para seus usuários.

Figura 4: Assinatura de Aplicativo do Google



Fonte: Android Google Developer.

2.2 SEGURANÇA APLICADA

Sabe-se que o Google tem como meta fazer do *android* a plataforma mais segura do mundo, porém existem contrapartidas, de acordo com Rachad Alao (Gerente de engenharia do Google) (acesso em: 04/10/2017 s/p): “As atualizações regulares oferecem mais do que simples melhorias e correções. Elas proporcionam uma sensação de segurança reforçada aos nossos clientes.”.

A Segurança sempre foi um foco para os desenvolvedores e por ser um sistema de código aberto, é compartilhado o código fonte para correções e emitido um boletim de segurança com os usuários e estabelecem atualizações mensais de correções. Vendo de outro lado como o código é compartilhado, poderia ser analisado por um usuário mal intencionado para descobrir falhas semelhantes.

2.3 SEGURANÇA HUMANA NO *ANDROID*

Em todas as aplicações existem vulnerabilidades, é impossível ser 100% seguro, porém o usuário é o elo mais fraco da Segurança, é impossível saber tudo o que acontece no meio da tecnologia.

A interface do *android* facilita qualquer pessoa utilizar sem medo e enigmas, e essa facilitação pode causar confiança aos usuários que consequentemente traz vulnerabilidades e ameaças, como os próprios termos de uso que são colocados em todas as plataformas do *android* para os usuários terem conhecimento como as mais acessadas: Gmail, Google Fotos, Youtube.

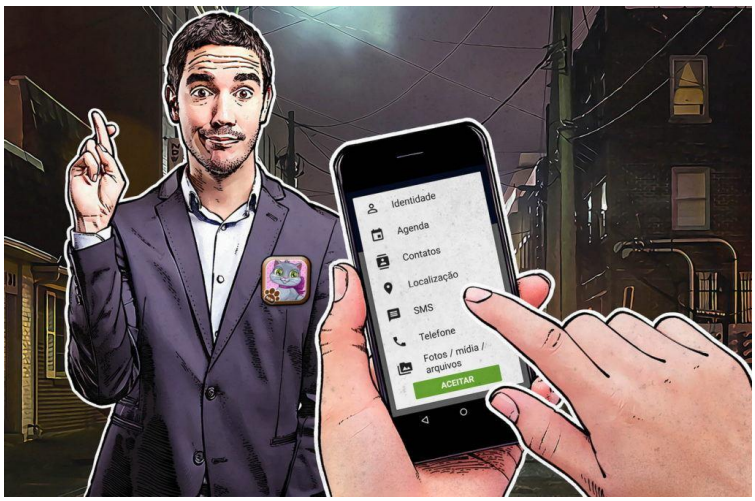
2.4 PERMISSÕES DE ACESSO

Os usuários precisam tomar cuidado em relação a deixar suas informações públicas na rede, porém não é só isso que devem se atentar, como dito, os termos de uso são importantíssimos para saber que tipos de permissão estão dando a aplicativos, podendo ser de terceiros ou até mesmo oficial. De acordo com uma nota realizada pelo Centro de Computação da Unicamp (2017, s/p) “Um novo tipo de *ransomware* para *Android* foi descoberto pela empresa de segurança McAfee. Trata-se de um vírus de resgate que sequestra dados pessoais e ameaça compartilhar com os contatos caso não seja realizado um pagamento.”.

Esse *ransomware* estava presente em aplicativos de terceiros como *(Wallpaper Blur HD* e *Cleaner Pro*) e quando instalados ativavam permissões de controle total ao sistema, como ver fotos, ligações, localização, contatos entre praticamente todas as plataformas. Os atacantes cobravam até U$ 50 dos usuários para não divulgarem suas informações. Especialistas orientam a tomar total cuidado a baixar aplicativos de terceiros e verificar permissões dos mesmos.

As permissões ficam explicitas na tela do usuário, como mostra a Figura 5, porém, muitas pessoas, não têm a informação que isso possa ser uma ameaça e que realmente essas permissões possam causar danos às suas informações.

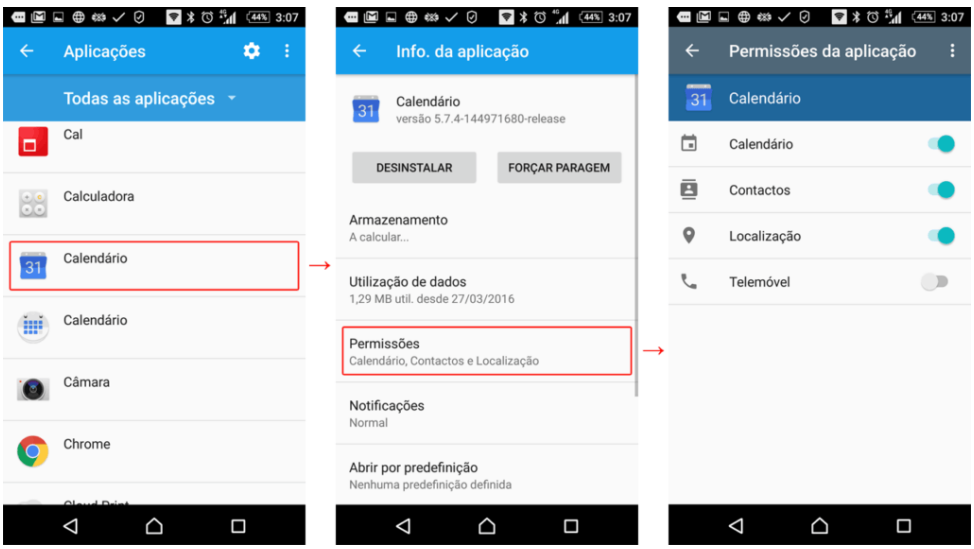
Figura 5: Ilustração de permissão de acesso no android



Fonte: KaperSky.

Na versão do android 6 acima, as configurações de permissões para cada aplicativo é possível, demanda um conhecimento um pouco mais avançado, porém, é possível mudar permissões para cada aplicativo instalado no android. Mas se a permissão for retirada, o aplicativo pode não funcionar da maneira correta e erros podem aparecer na tela, como observado na figura abaixo.

Figura 6: Tela de configuração de permissões no android



Fonte: Kapersky.

2.5 OBRIGAÇÃO DOS TERMOS DE USO E PRIVACIDADE

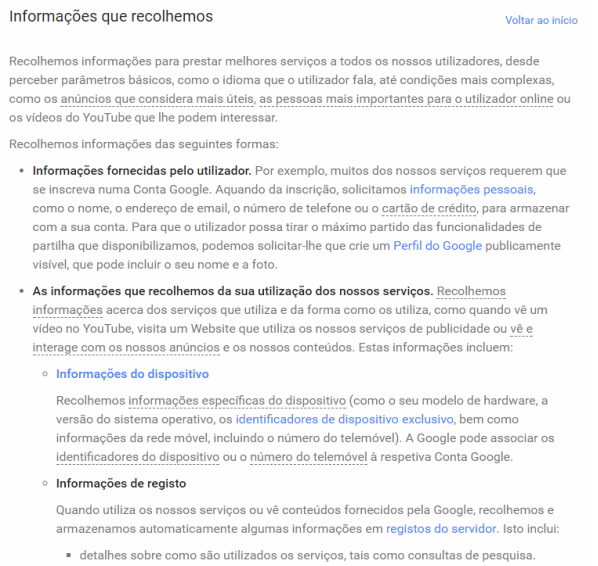
Os termos de uso foram e sempre serão apenas leitura indesejada aos usuários, como a pesquisa feita neste trabalho irá mostrar resultados, observa-se que a maioria das pessoas não lêem os termos que são impostos a cada plataforma, plataformas mundialmente usadas. Mesmo o Google tornando a leitura mais dinâmica, os usuários já tornaram uma cultura de não ler os termos, já se torna automático passar sem ler, até porque atualmente as pessoas estão com mais pressa para realizarem suas tarefas.

De acordo com uma notícia realizada pela Tecnologia do Ig em 2016:

> [...]40% dos usuários brasileiros não leem termos de uso ao instalar aplicativos [...] Para a Kaspersky Lab, responsável pela pesquisa, o usuário pode expor sua privacidade e as informações salvas no smartphone a ameaças virtuais quando não lê os contratos de licença ou as mensagens durante a instalação. Alguns aplicativos podem afetar a privacidade do usuário, iniciar a instalação de outros programas ou até mesmo alterar a configuração do sistema de maneira legal caso o usuário tenha autorizado o acesso durante a instalação.

A figura 7 mostra um trecho dos Termos de Privacidade do Google ao criar uma conta Gmail.

Figura 7: Política de Privacidade da Google



Informações que recolhemos

Voltar ao início

Recolhemos informações para prestar melhores serviços a todos os nossos utilizadores, desde perceber parâmetros básicos, como o idioma que o utilizador fala, até condições mais complexas, como os anúncios que considera mais úteis, as pessoas mais importantes para o utilizador online ou os vídeos do YouTube que lhe podem interessar.

Recolhemos informações das seguintes formas:

- **Informações fornecidas pelo utilizador.** Por exemplo, muitos dos nossos serviços requerem que se inscreva numa Conta Google. Aquando da inscrição, solicitamos informações pessoais, como o nome, o endereço de email, o número de telefone ou o cartão de crédito, para armazenar com a sua conta. Para que o utilizador possa tirar o máximo partido das funcionalidades de partilha que disponibilizamos, podemos solicitar-lhe que crie um Perfil do Google publicamente visível, que pode incluir o seu nome e a foto.
- **As informações que recolhemos da sua utilização dos nossos serviços.** Recolhemos informações acerca dos serviços que utiliza e da forma como os utiliza, como quando vê um vídeo no YouTube, visita um Website que utiliza os nossos serviços de publicidade ou vê e interage com os nossos anúncios e os nossos conteúdos. Estas informações incluem:
  - Informações do dispositivo

    Recolhemos informações específicas do dispositivo (como o seu modelo de hardware, a versão do sistema operativo, os identificadores de dispositivo exclusivo, bem como informações da rede móvel, incluindo o número do telemóvel). A Google pode associar os identificadores do dispositivo ou o número do telemóvel à respetiva Conta Google.
  - **Informações de registo**

    Quando utiliza os nossos serviços ou vê conteúdos fornecidos pela Google, recolhemos e armazenamos automaticamente algumas informações em registos do servidor. Isto inclui:
    - detalhes sobre como são utilizados os serviços, tais como consultas de pesquisa.

Fonte: Google Gmail.

2.6 ESTUDO DE CASO

2.6.1 Sujeitos da pesquisa

O estudo foi realizado com foco nos Termos de uso aplicado aos usuários e a obrigação de aceitar sem concordar, a obrigação se da ao uso popular e pré imposto nos *smartphones*, o usuário tem a escolha de mudar, porém os mais leigos não conhecem a opção. O foco também se deu a vulnerabilidade de permissões as quais os usuários estão sujeitos a concordar com as permissões pré impostas também em suas plataformas.

Para a realização da pesquisa, optou-se em aplicar um pequeno questionário (Apêndice 1) com 06 questões fechadas em 29 alunos regularmente matriculadas no 5º semestre do curso Superior de Tecnologia em Segurança da Informação da Fatec Americana e que utilizam o sistema operacional *android*.

A população escolhida se deu em função de considerar, que os alunos do 5º Semestre terem conhecimento mais elevado sobre segurança, vulnerabilidade e privacidade de dados, do que os semestres anteriores.

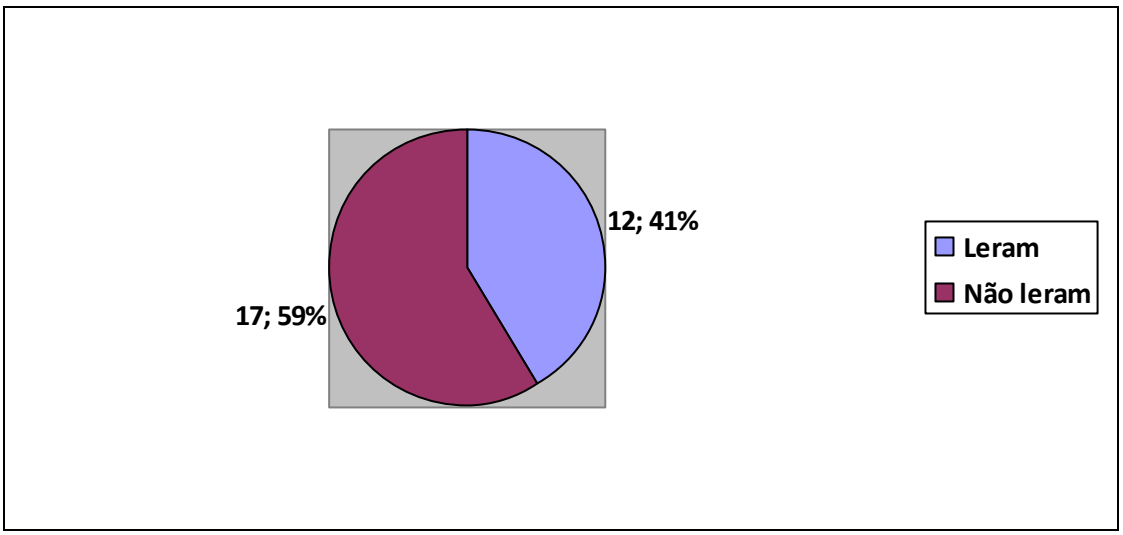
2.6.2 Dados da pesquisa

Os dados foram apresentados em gráficos, cujos nomes são os mesmos das questões feitas. No tocante ao sexo: 26 do sexo masculino e 3 do feminino. Os mesmos não consideram o sexo, em função de ser dispare.

Sobre a primeira pergunta, que foi sobre a utilização de alguma plataforma do *android,* afirmar-se que 100% utiliza alguma plataforma do *android*, como Gmail, Google Plus, Google Play entre outros...

A segunda pergunta é a quem utiliza as plataformas dizer se já leram os termos de privacidade/uso de alguma delas e o resultado foi: 12 alunos leram o termo de alguma plataforma e 17 não leram os termos.

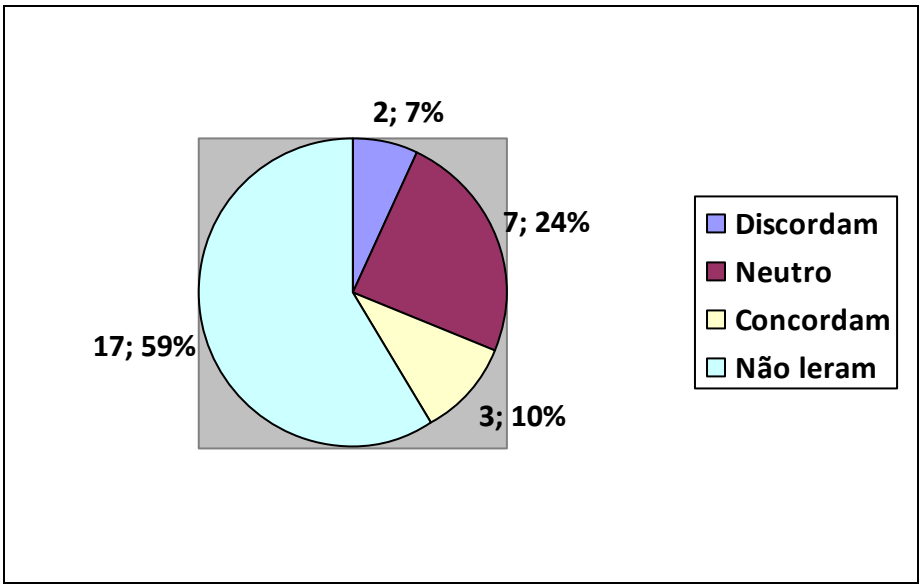
Gráfico 1: leitura dos termos de uso pelos alunos



Fonte: elaborado pelo autor

A terceira pergunta é sobre a opinião dos que leram o termo de uso e o resultado foi: 2 alunos discordam dos termos, 7 alunos são neutros em relação a opinião dos termos, 3 alunos concordam com os termos e 17 alunos não leram os termos.

Gráfico 2: opinião sobre os termos de uso

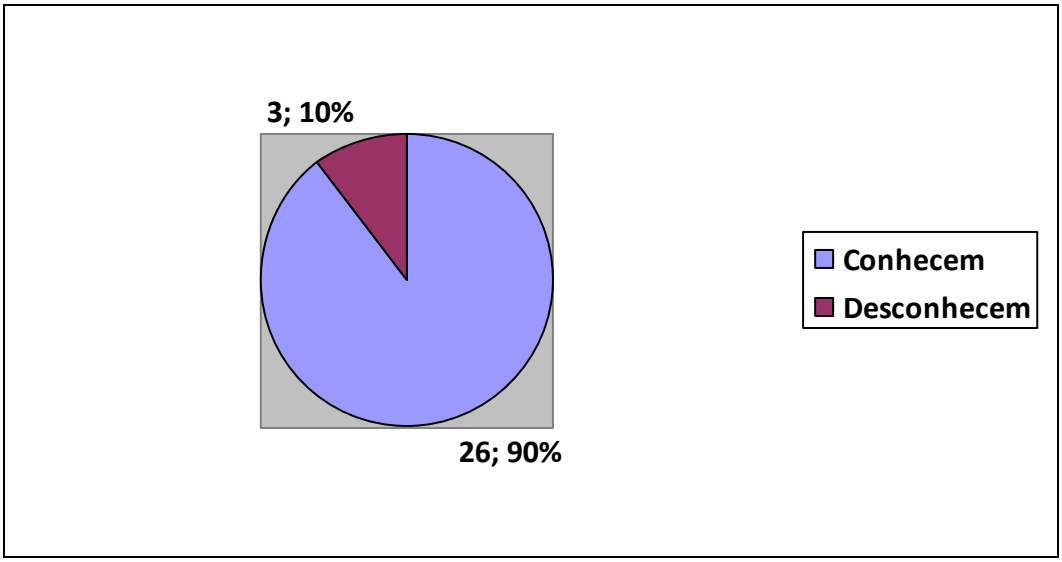


Fonte: elaborado pelo autor

A quarta pergunta discute o conhecimento dos alunos em relação às permissões no *android* (microfone, câmera, gps, aplicativos...) e o resultado foi: 26

alunos conhecem as permissões e 3 alunos desconhecem as permissões de aplicativos no *android*.

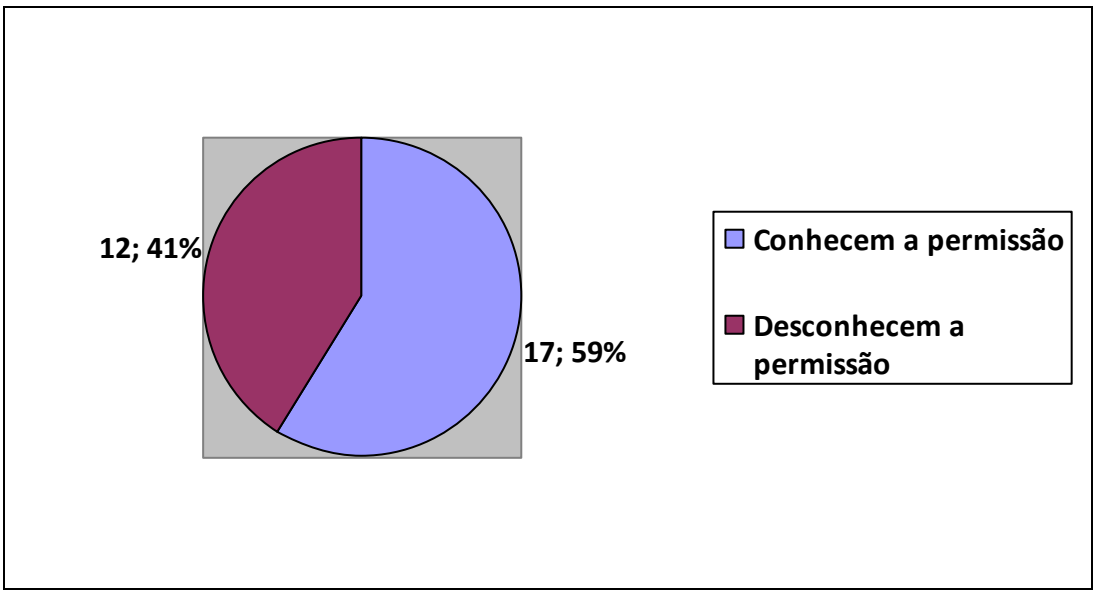
Gráfico 3: conhecimento das permissões do android



Fonte: elaborado pelo autor

A quinta pergunta é sobre o conhecimento dos alunos sobre o *android* gravar áudio a qualquer momento sem a confirmação do utilizador e o resultado foi: 17 alunos sabem da permissão e 12 alunos não sabem da permissão.

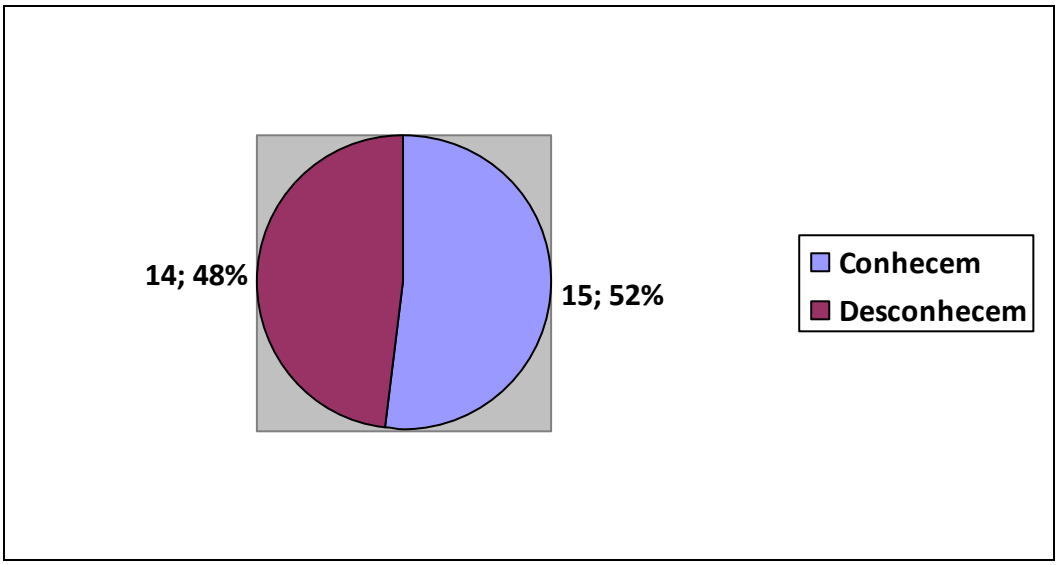
Gráfico 4: conhecimento da permissão de áudio no *android*



Fonte: elaborado pelo autor

A sexta e ultima pergunta é sobre o conhecimento do Google *My Activies* (Minhas atividades) e o resultado foi: 15 alunos conhecem e 14 alunos não conhecem.

Gráfico 5: conhecimento do Google *My Activies*



Fonte: elaborado pelo autor

2.6.3 Análise dos dados

Para a análise dos dados foi utilizado como material auxiliar o livro “1984” de George Orwell, escrito em 1948 e publicado em 1949, que, de acordo com a Companhia das Letras (acesso em: 25/11/2017): “[...] é um dos romances mais influentes do século XX, um inquestionável clássico moderno. (...) é uma obra magistral que ainda se impõe como uma poderosa reflexão ficcional sobre a essência nefasta de qualquer forma de poder totalitário”.

Foi exatamente a “essência nefasta” que chamou a atenção para utiliza-lo na análise, pois se considerou que o Google apresenta tal reflexão, em função dos seus Termos serem totalitários.

A partir dos resultados obtidos na pesquisa sobre vulnerabilidade e privacidade nos Termos e Permissões, considerando o ponto da leitura dos termos dessas plataformas, os resultados mostram uma proporção dividida aos que leram e aos que não leram os termos (12 alunos leram os termos e 17 alunos não leram), pode-se dizer, que mesmo lendo se submetem a plataforma. Em relação à opinião

sobre termos, obteve-se o resultado de: 2 alunos discordam, 7 são neutros, 3 concordam. Concordando, sendo neutros ou não tendo lido os mesmos, sendo a assim, os pesquisados, em sua totalidade utilizam as plataformas.

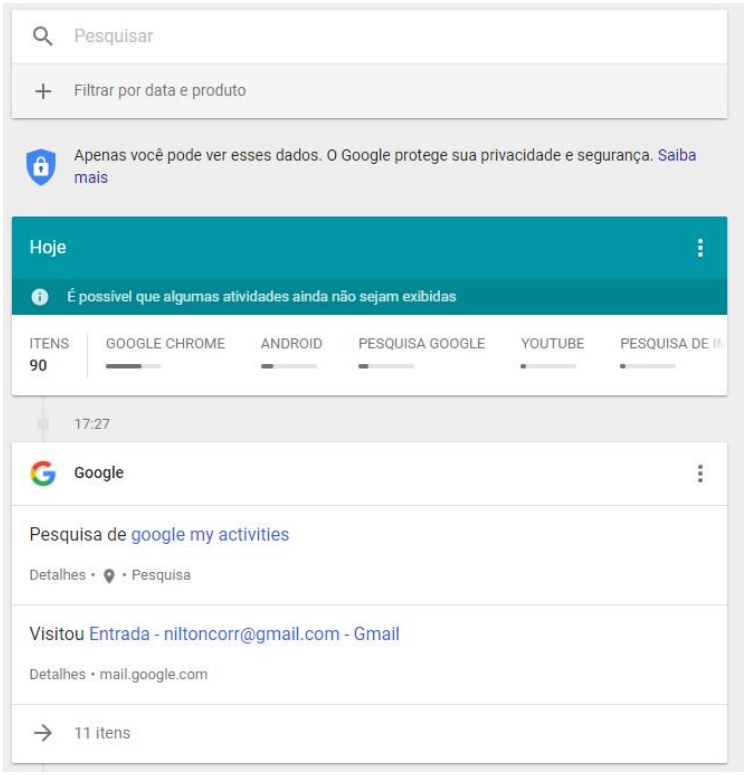
Acredita-se que possa inferir, que, mesmo sendo “obrigados” pelas plataformas a aceitarem, o fazem em função de maior parte dos indivíduos de sua geração utilizar; já que vem pré impostos quando se adquire um *smartphone android*. O que, afirma-se que “vivem aprisionados” em uma engrenagem totalitária tecnológica, que no caso do personagem principal da obra “1984”, Winston encontrava-se aprisionado a uma sociedade dominada pelo Estado, onde: “[...] tudo é feito coletivamente, mas cada qual vive sozinho. Ninguém escapa à vigilância do Grande Irmão, a mais famosa personificação literária de um poder cínico e cruel ao infinito, além de vazio de sentido histórico”. (COMPANHIA DAS LETRAS, acesso em: 25/11/2017).

O estudo revelou junto com os termos de privacidade/uso a questão da permissão aos aplicativos nativos e de terceiros, observou-se que 26 sujeitos conhecem as permissões e 3 desconhecem, observando que mesmo a maioria conhecendo-as, porém, somente 17 alunos sabem que o sistema *android* pode gravar áudio a qualquer momento sem a confirmação do proprietário do equipamento e 12 desconhecem a permissão.

A última pergunta se deu ao conhecimento do Google *My Activies* (Minhas atividades), a pesquisa revelou que 15 alunos conhecem a plataforma e 14 desconhecem.

O Google *My Activies* é uma plataforma desenvolvida pelo Google para controle do usuário, todo usuário portador do sistema operacional *android* com conta no Google é criado uma página chamada Minhas Atividades em que se registram tudo que o usuário fez, pesquisou, visitou e chamou. A plataforma cria um *log* de tudo, a figura 8 mostra um exemplo das atividades registradas nesta plataforma.

Figura 8 – Registros do Google *My Activies*



Fonte: Próprio Autor.

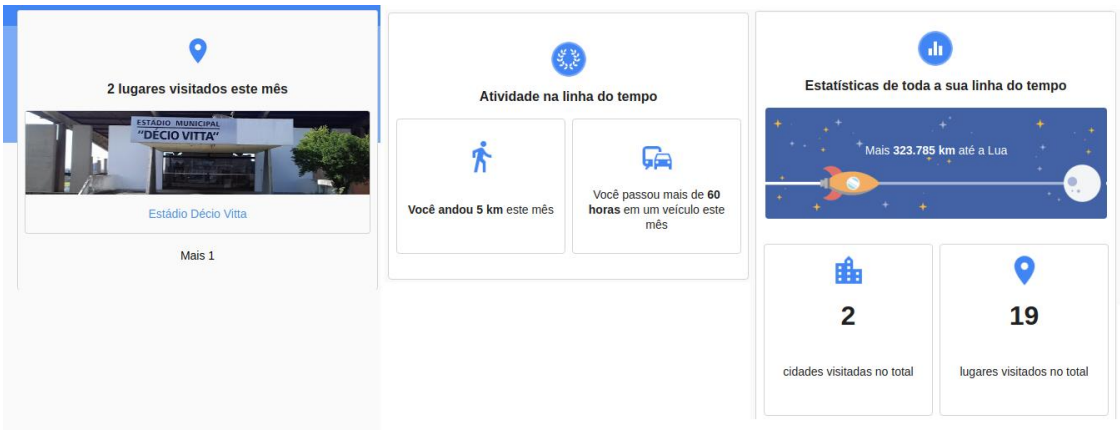
Além de pesquisas e históricos de visualização ele também registra o histórico de localização e áudio, que para o autor é de extrema importância ao fato da falta de privacidade a relação do utilizador. Foi analisado na pesquisa que praticamente metade dos alunos pesquisados não conhece, salienta-se que em um curso de Tecnologia de Segurança da Informação, 5º Semestre, o número seja significativo para o desconhecimento.

Em um artigo realizado pela “Uol Tecnologia” (2016 s/p) tem-se: “[...] Já o Google confirmou gravar os comandos de voz dos usuários e usar os áudios para pesquisas internas, como previsto nos termos de uso do serviço. Segundo a empresa, as informações não são usadas nem vendidas para fins comerciais”. Portanto, se metade dos alunos do curso de Tecnologia da Segurança da Informação desconhecem essa plataforma, pode-se supor que poucos usuários leigos irão conhecer, e se esse acesso cair em mãos de pessoas mal intencionadas, as mesmas terão acesso completo à vida do usuário, como, áudios gravados em momentos aleatórios, histórico completo de cidades que a pessoa visitou, trajetos

marcados como rotina, o mal intencionado tem a rotina das pessoas na mão e pode fazer o que quiser com isso.

Abaixo estão algumas imagens sobre o monitoramento e registro de localização de uma aluna do Curso de Análise e Desenvolvimento de Sistemas.

Figura 9 – Histórico de localização e monitoramento do *My Activies*



Fonte: Rafaela, aluna do curso de ADS.

A partir do exposto, considera-se importante algumas considerações, tais como:

- Winstom Smith (personagem principal de “1984”) representa o cidadão comum vigiado pelas teletelas e pelas diretrizes do Partido, os sujeitos da pesquisa representam os cidadãos com conhecimentos tecnológicos vigiados, como a Rafaela, vigiados com ou sem autorização pelo Google, que parece reduzir o indivíduo em uma peça que serve de massa de manobra a seus sistemas e ao mercado consumidor.

- Winstom Smith diz que o partido controla o futuro, presente e passado das pessoas, exatamente como se pensou no Google ao observar os dados da pesquisa.

- O ofício de Winston era transformar a realidade, pois trabalhava no Ministério da Verdade, razão de ter dito: “liberdade é poder escrever que dois mais dois são quatro. As fábricas russas ainda contêm placas com o

> lema: dois mais dois são cinco se o partido quiser”. O que diz respeito a importância de poder optar na não aceitação dos termos das plataformas do sistema *android* e poder utilizar os serviços.

Entretanto, existe a possibilidade de retirar o assistente de voz e os registros do *My Activies* para estar um pouco distante da vulnerabilidade, porém o “Uol Tecnologia” (2016 s/p): “[...] aponta Teixeira, essa opção está longe de garantir a privacidade total de seus dados. Você teria que deixar de usar a internet, já que muitos sites usam os famosos cookies."

Além de trabalhar *offline* com as permissões de GPS para mapear a localização, a solução seria não usar o *smartphone*, já que os registros podem ser gravados sem conexão com a internet.

3 CONSIDERAÇÕES FINAIS

Nos dias atuais as pessoas estão mais vulneráveis que há alguns anos; na área de Tecnologia da Informação existem inúmeras vulnerabilidades, porém, com a maior exposição da vida privada nos meios digitais, as vulnerabilidades de privacidade tem maior relevância. Além da exposição, acabam sendo monitoradas por veículos que, muitas vezes, podem estar coletando sua informação para fins lucrativos ou de espionagem.

Além disso, de acordo com o estudo de caso realizado com alunos do Curso Superior de Segurança da Informação, observou-se que desconhecem os termos de uso e permissões de acesso de plataformas que utilizam em seu *smartphone*, isso acaba acarretando uma obrigatoriedade de aceite somente para usar a plataforma, já que o *android* é um dos sistemas operacionais mais usados no Mundo, essa obrigação faz com que as pessoas aceitem e passem pelo registro das plataformas sem lerem e desconhecendo o que o desenvolvedor pode fazer com suas informações.

A partir da apresentação e análise dos dados, observamos que, com o decorrer do tempo, a informação está crescendo de maneira rápida, a vida está se tornando digital, com isso temos que prestar atenção em alguns aspectos deixados para trás em relação à privacidade e a informação pública. Além das vulnerabilidades comuns que afetam apenas as pessoas com ligação ao mundo tecnológico, atualmente os usuários comuns estão sendo afetados sem saberem, como as pessoas estão sempre utilizando dispositivos conectados, elas estão se submetendo a passar suas vidas reais para o digital, com *smartphones* capturando e registrando suas vidas e até mesmo as próprias pessoas jogando sua vida em redes sociais e plataformas públicas.

Com o estudo, podemos dizer que as plataformas do sistema tornam os usuários vulneráveis, de acordo com seus termos e permissões pré estabelecidas e impostas ao usuário aceitar, também estão frágeis ao monitoramento feito no sistema, pois além de muitos usuários não conhecerem a ferramenta de registro,

pessoas mal intencionadas podem conseguir esse acesso e usar contra o usuário, além da informação estar sendo registrada a todo instante.

Ao pensarmos no livro 1984 de George Orwell, podemos dizer que estamos sendo observados a todo tempo e até podemos ser manipulados em função de tanta exposição, como foi abordado neste trabalho, o Google *My Activies* tem uma relação forte com a “Teletela” quando pensamos na vigilância direta.

O objetivo geral foi atingido, pois o estudo objetiva-se a coleta de dados e a análise dos alunos do 5º Semestre de Segurança da Informação em relação a vulnerabilidade de privacidade, termos e permissões que são impostos pelo Google.

A pergunta “identificar como a Segurança da Informação pode influenciar usuários a terem o conhecimento da vulnerabilidade de Privacidade?” foi respondida por meio da análise realizada pela pesquisa, ao mesmo tempo orientando os usuários a terem o conhecimento da vulnerabilidade de Privacidade.

“O Usuário que leu os termos, não o aceitando é bloqueado antes do passo de finalização do registro, plataforma/serviço usado mundialmente por uma parcela considerável da população; já o que não leu e não tem noção das ameaças, concordando com os termos, é finalizado o seu registro.” é a hipótese verdadeira analisada pelo estudo.

A justificativa se torna correta, analisando todos os pontos das vulnerabilidades, com enfoque na Privacidade, usando a pesquisa analisada e como material auxiliar o livro “1984” de George Orwell para a explicação da imposição feita nos termos e permissões das plataformas do Google no sistema *android*.

Como possíveis pesquisas futuras, sugerimos um caminho por meio da frase: “Viveremos uma era em que a liberdade de pensamento será de início um pecado mortal e mais tarde uma abstração sem sentido”, disse Orwell. As teletelas do livro são ferramentas de controle. Estão em todo canto. Transmitem mensagens e monitoram ao mesmo tempo.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDROID DEVELOPERS. **Versões.** Disponível em: <http://developer.*android*.com> Acesso em: 04 out. 2017

ARAUJO, Nonata Silva. **Segurança da Informação (TI).** Disponível em:< http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/>. Acesso em: 20 set. 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

_____. NBR ISO/IEC 27002:2005. **Tecnologia da informação** – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 mar. 2017.

COMPANHIA DAS LETRAS. **1984 George Orwell.** Disponível em: <https://www.companhiadasletras.com.br/detalhe.php?codigo=12562>. Acesso em 25 nov. 2017.

DANTAS, Marcus. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda/PE: Livro Rápido, 2011, p. 10-39

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. 6. ed. São Paulo: Saraiva, 2005, p. 45-120.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. Porto Alegre/RS: UFRGS, 2009, p. 31-43

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6a ed. São Paulo: Atlas, 2008, p. 20-60

GOOGLE. **Bem-vindo à Política de Privacidade da Google.** Disponível em: < https://www.google.com.br/intl/pt/policies/privacy/>. Acesso em: 04 out. 2017.

_____. **Seus Dados e Privacidade.** Disponível em: <https://privacy.google.com/intl/pt-BR/your-data.html>. Acesso em: 20 mar. 2017.

GUIA DO ESTUDANTE. **Saiba mais sobre o livro 1984, de George Orwell.** Disponível em: <https://guiadoestudante.abril.com.br/estudo/saiba-mais-sobre-o-livro-1984-de-george-orwell/>. Acesso em: 25 nov. 2017.

JORNAL O DIA. ***Android* ultrapassa marca de 2 bilhões de usuários ativos por mês**. (17/05/2017). Disponível em: <http://odia.ig.com.br/mundoeciencia/2017-05-17/*android*-ultrapassa-marca-de-2-bilhoes-de-usuarios-ativos-por-mes.html>. Acesso em: 14 set. 2017.

KAPERSKY. **Tudo sobre permissões dos aplicativos no Android.** Disponível em: <https://www.kaspersky.com.br/blog/tudo-sobre-permissoes-dos-aplicativos-no-android/7147/>. Acesso em: 04 out. 2017.

OPUS SOFTWARE. **Estatísticas de uso de celular no Brasil.** (2016). Disponível em: <https://www.opus-software.com.br/estatisticas-uso-celular-brasil/>. Acesso em: 30 ago. 2017.

PEREIRA, Lucio Camilo Oliva; SILVA, Michel Lourenço da. ***Android* para Desenvolvedores**. Rio de Janeiro: Brasport, 2009.

REDESEGURA. **Gerenciamento de vulnerabilidades**. Disponível em: <http://www.redesegura.com.br/gerenciamento-de-vulnerabilidades/>. Acesso em: 24 fev. 2017.

RESEARCHGATE. **Vulnerabilidades em aplicações *web* e mecanismos de proteção**. Disponível em: <https://www.researchgate.net/ profile/Sandro_ Melo/publication/ 266445537_Captulo_6_Vulnerabilidades_em_ Aplicaes_ *Web*_ e_Mecanismos_de_Proteo/links/55b0e3c708ae092e964fb3d5.pdf> Acesso em: 24 fev. 2017.

RUDD, Matt. **Say cheese**. The Sunday Times, Londres. (jun. 2015). Disponível em: <http://www.thetimes.co.uk/article/say-cheese-lhkwwhp0zj>. Acesso em: 20 mar. 2017.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

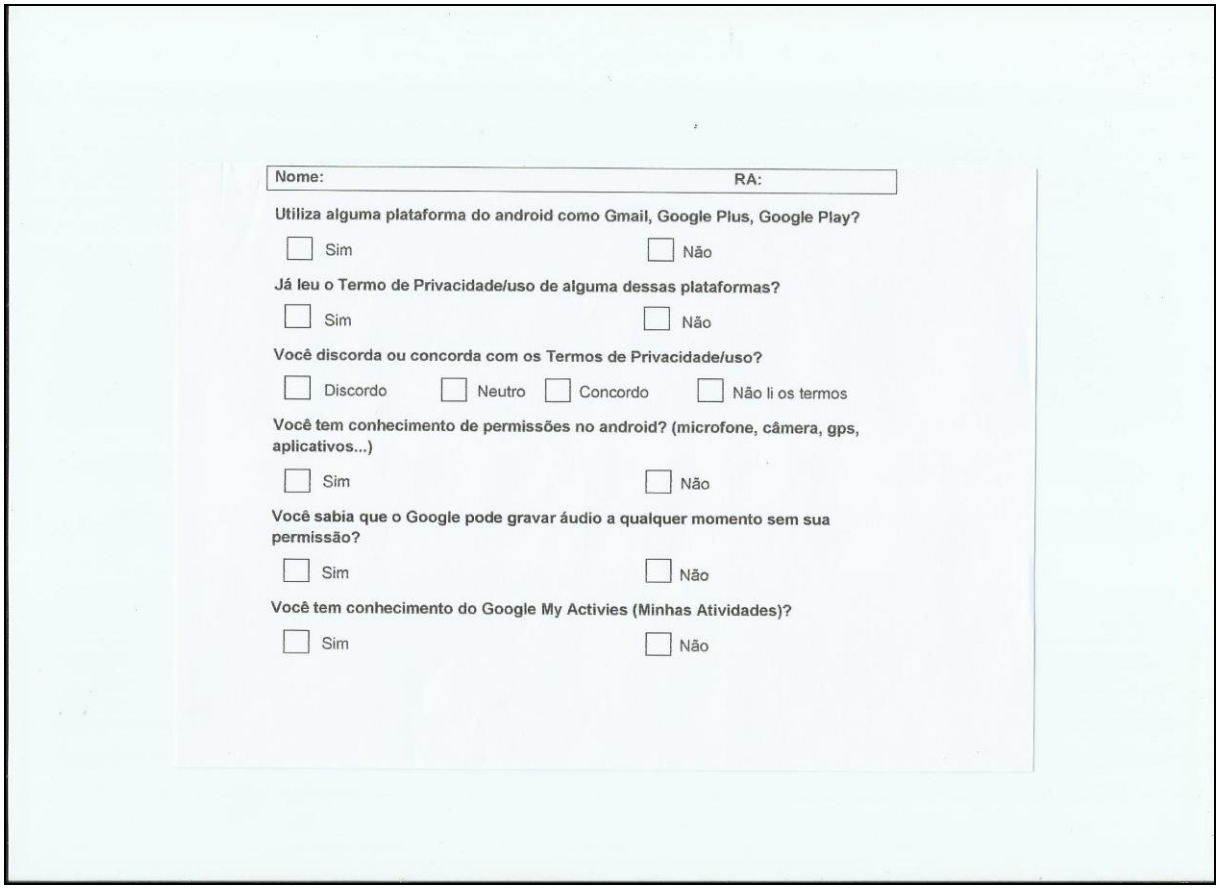
TECNOBLOG. **95,5% dos smartphones vendidos no Brasil são Androids.** Disponível em: <https://tecnoblog.net/203749/android-ios-market-share-brasil-3t-2016/>. Acesso em: 04 out. 2017.

TECNOLOGIA UOL. **Google, Apple, Facebook: as empresas ouvem o que você fala?** Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2016/10/17/google-apple-facebook-eles-ouvem-o-que-voce-fala.htm>. Acesso em: 04 out. 2017.

TELECO. **Redes de Computadores I:** Segurança da Informação. Disponível em: < http://www.teleco.com.br/tutoriais/tutorialitil/pagina_2.asp>. Acesso em: 28 set. 2017.

TRUSTSING. **Conhecendo as vulnerabilidades *web*.** Disponível em: <https://www.trustsign.com.br/portal/blog/conhecendo-as-vulnerabilidades-*web*/> Acesso em: 24 fev. 2017.

APÊNDICE A – Questionário do Estudo de Caso



Nome: RA:

Utiliza alguma plataforma do android como Gmail, Google Plus, Google Play?

☐ Sim ☐ Não

Já leu o Termo de Privacidade/uso de alguma dessas plataformas?

☐ Sim ☐ Não

Você discorda ou concorda com os Termos de Privacidade/uso?

☐ Discordo ☐ Neutro ☐ Concordo ☐ Não li os termos

Você tem conhecimento de permissões no android? (microfone, câmera, gps, aplicativos...)

☐ Sim ☐ Não

Você sabia que o Google pode gravar áudio a qualquer momento sem sua permissão?

☐ Sim ☐ Não

Você tem conhecimento do Google My Activies (Minhas Atividades)?

☐ Sim ☐ Não