



UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CAMPUS VII
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS - CCEA
CURSO DE LICENCIATURA EM COMPUTAÇÃO

DIOGO TEODOZIO FREITAS

**INSEGURANÇA EM *SMARTPHONES*: Uma pesquisa de campo no contexto do
Campus VII da UEPB**

Orientador: Prof. Me. Betoven Oliveira de Andrade.

PATOS – PB

2017

DIOGO TEODOZIO FREITAS

**INSEGURANÇA EM SMARTPHONES: Uma pesquisa de campo no contexto do
Campus VII da UEPB**

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura Em Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Computação.

Área de concentração: Segurança da informação.

Orientador: Prof. Me. Betoven Oliveira de Andrade.

PATOS – PB

2017

É expressamente proibida a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano da dissertação.

F866i Freitas, Diogo Teodozio
Insegurança em smartphones [manuscrito] : uma pesquisa de campo no contexto do Campus VII da UEPB / Diogo Teodozio Freitas. - 2017.
31 p. : il. color.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2017.
"Orientação: Prof. Me. Betoven Oliveira de Andrade, CCEA".

1. Ataque cibernético. 2. Segurança da informação. 3. Smartphone. 4. Campus VII UEPB. I. Título.

21. ed. CDD 005.8

TERMO DE APROVAÇÃO

Diogo Teodozio Freitas

**INSEGURANÇA EM SMARTPHONES: Uma pesquisa de campo no contexto do
Campus VII da UEPB**

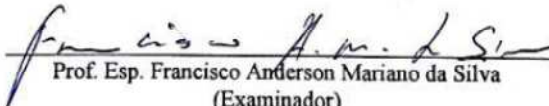
Trabalho de Conclusão de Curso apresentado ao
Curso de Licenciatura em Computação da
Universidade Estadual da Paraíba, em
cumprimento à exigência para obtenção do grau
de Licenciado em Computação

Aprovado em 4 de agosto de 2017

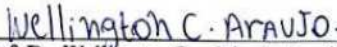
BANCA EXAMINADORA



Prof. Me. Betoven Oliveira de Andrade
(Orientador)



Prof. Esp. Francisco Anderson Mariano da Silva
(Examinador)



Prof. Dr. Wellington Candeia de Araujo
(Examinador)

RESUMO

A utilização de dispositivos móveis em rede cresceu surpreendentemente nos últimos anos, de modo que hoje podemos nos conectar à rede praticamente em qualquer lugar e hora. Contudo, o aumento desta utilização, fez crescer significativamente os ataques destinados a dispositivos móveis, bem como a exposição à malwares, aumentando a vulnerabilidade dos seus usuários. Este trabalho apresenta os resultados de uma pesquisa dividida em dois viés, inicialmente foi desenvolvida uma pesquisa sobre o estado da arte e em seguida uma pesquisa de campo onde entrevistou-se discentes dos cursos de Administração, Computação, Física e Matemática no Campus VII da UEPB, com o intuito de avaliar o nível de cuidados de segurança que estes empregam em seus *smartphones*. A pesquisa revelou, em linhas gerais, que os discentes de Computação e Matemática apresentaram maior descuido que os de Administração e Física, este último o mais cuidadoso. No entanto os discentes de computação foram os menos contaminados com *malwares*, o que sugere que um nível maior de conhecimento técnico na área pode auxiliar a se prevenir de pragas do gênero.

Palavras-chaves: Ataque, Segurança, *Smartphone*, Vulnerabilidade, Campus VII UEPB.

1 INTRODUÇÃO

Com o avanço da tecnologia e a necessidade de dispositivos portáteis e de baixo custo para os consumidores, os dispositivos móveis surgiram e hoje cabem na palma da mão de seus usuários. Na verdade, essa ideia surgiu nos anos 90 com significativas melhorias a partir de 2007. A mobilidade tecnológica em informação e comunicação possibilitou a simplificação do cotidiano para usuários que utilizam esse tipo de praticidade, uma vez que aproximou as pessoas distantes geograficamente com o uso de redes sociais por meio de aplicativos tornando o dia a dia mais simples. O acesso aos dados se tornou viável, sobretudo após o grande aumento das redes locais sem fio (WAN) e dos grandes avanços nas taxas de transmissões de telefonia móvel, com isso informações podem ser obtidas em qualquer momento e em qualquer lugar desde que esteja conectado a uma rede.

Apesar do termo *smartphone* ter sido elaborado na década de 1990 a intenção de adicionar outras funcionalidades aos telefones móveis data de 1983, mas foi em 1994 que o *IBM Simon* o primeiro *smartphone* da história foi lançado (VOLTONI, 2014). Atualmente os *smartphone* possuem poder de processamento e capacidade de memória superiores aos computadores pessoais antigos, época em que o *smartphone* foi projetado, contudo nesse tempo nem se imaginava o quanto a tecnologia avançaria.

Os celulares de hoje estão cada vez mais eficientes e inteligentes, pois caracterizam-se pela reunião de praticidade e acessibilidade comunicativa, em contrapartida proporcionalmente, crescem os riscos e ameaças devido à vulnerabilidade expositiva dessa tecnologia em redes de comunicação. Os usuários acreditam que só porque usam um telefone móvel estão a salvo dos perigos que existiam em Sistemas Operacionais (S.O.) de *desktops* e *laptops*, porém as ameaças cibernéticas estão cada vez mais direcionadas para as tecnologia móvel. Segundo Breno (2004) Conforme o avanço das tecnologias, novos métodos de atrair os cidadãos vão surgindo. Um dos motivos é que os usuários nem sempre estão cientes dos perigos e da vulnerabilidade que o aparelho pode obter.

Tais ameaças, a exemplo do *malware*, caracteriza-se como uma doença, o qual alcança inúmeras pessoas. O objetivo desse software é roubar, modificar, apagar dados, capturar informações, alterar ou impedir o funcionamento do S.O. do usuário

sem que ele saiba. São criados tanto para desktops como para tecnologia móvel, o *malware* é um termo que significa *malicious software* (software malicioso). De acordo com (Alecrim, 2016) "*malware* nada mais é do que um nome criado para quando necessitamos fazer alusão a um software malicioso, seja ele um vírus, um *Worm*, ou um *Spyware*."

Existem inúmeros tipos de *malware* como *Ransomware* que pode bloquear ou limitar o acesso a arquivos, pastas, aplicativos, ou até mesmo impedir o uso do sistema operacional, ou o *Rootkit* que é um *malware* muito ameaçador, ele tem várias aplicações, um exemplo delas é obter dados do usuário, mas o que torna ele tão perigoso é o fato de possuir propensão de se camuflar na detecção por antivírus ou outros softwares de segurança. No âmbito das tecnologias móveis, esses tipos malwares estão direcionados principalmente para os dispositivos com S.O. Android por causa da sua quantidade de usuário.

A quantidade de usuários que utilizam *smartphone* no Brasil vem crescendo exponencialmente. Segundo pesquisa da FGV (Fundação Getúlio Vargas), realizada no ano de 2016, havia no país 168 milhões de smartphones em uso, um crescimento de 9% em relação a 2015 que tinha 152 milhões de celulares inteligentes. Isso confirma que o consumo de smartphones no mercado cresce ano a ano; vale ressaltar que o Brasil é o 6º país com o maior mercado de smartphones no mundo, ficando atrás apenas da China, Estados Unidos, Índia, Japão e Rússia.

Os números de *smartphone* na sociedade Brasileira reflete o quanto os jovens e adultos estão conectados a redes com seus aparelhos. Segundo IBGE (2014), o *smartphone* ultrapassou os PC (computador pessoal) e se tornou o aparelho número 1º para acesso à internet. A pesquisa aponta que os PCS estão em 76,6% das casas, enquanto o *smartphone* está com 80%. A diferença é vasta levando em conta que o mercado de *smartphone* se expandiu em pouco tempo. Hoje os PCs são mais utilizados para trabalho enquanto os smartphones lideram no quesito comunicação, seja via *messenger*, seja via redes sociais. De acordo com Ling (2004) "eles foram adotados rapidamente e 'ligados ao nosso corpo' para uma ampla variedade de práticas sociais, que ultrapassam as funções primárias de comunicação; assim como os elementos do cotidiano, as tecnologias sem fio, e principalmente o celular, são percebidas como instrumentos essenciais da vida contemporânea".

Com relação aos sistemas operacionais para dispositivos móveis, as pesquisas mostram que Android é o sistema operacional mais utilizado no Brasil e no mundo,

seguido do iOS. Segundo a empresa de pesquisas International Data Corporation (IDC) o Android domina o mercado com uma participação de 87,6% em 2016, enquanto o iOS tem o mercado em 11,7%, além desses existem outros sistemas que detêm uma mínima fatia do mercado, cerca de 0,3%. O sistema operacional do iPhone (iOS) foi um dos primeiros a entrar no mercado para o consumidor, mas foi o Android que, promovendo o barateamento de dispositivos de diversas marcas e facilitando o desenvolvimento de novos aplicativos (APPs), conquistou mais a empatia do público alvo. Mesmo o Android tendo seu kernel baseado em um kernel de S.O. relativamente seguro - o Linux, isso não impede a crescente leva de ameaças que surge; na verdade a grande quantidade de usuários é um atrativo para os *crackers* e demais pessoas mal-intencionadas.

Diante do exposto, esta pesquisa foi desenvolvida com a finalidade de promover um estudo acerca de segurança em dispositivos móveis, mais especificamente os *smartphones*, além de investigar o nível de cautela dos estudantes do CAMPUS VII da Universidade Estadual da Paraíba (UEPB), dos cursos de Matemática, Física, Administração e Computação com relação as ameaças mais comuns da supracitada tecnologia móvel.

1.1 ORGANIZAÇÃO DESTE TRABALHO

Neste capítulo foi apresentado o contexto atual dos smartphones e suas vulnerabilidades, além dos objetivos desta pesquisa. A seguir no segundo capítulo, será apresentada a metodologia que descreve a trajetória percorrida para que a pesquisa fosse desenvolvida. O terceiro capítulo mostra o referencial teórico, o qual permitirá uma melhor compreensão deste trabalho pelos leitores leigos ou servirá de revisão para leitores especialistas. Logo após, no quarto capítulo será abordada a pesquisa no campus VII da UEPB, comparando aspectos de segurança utilizados por discentes de quatro cursos: Computação (Licenciatura e Bacharelado), Administração, Física e Matemática. Por fim, será apresentada a conclusão com o objetivo de finalizar devidamente este trabalho.

2 METODOLOGIA

O objetivo deste trabalho está focado na utilização das tecnologia móvel, enfatizando a segurança no âmbito dos *smartphones*. A pesquisa desenvolvida e apresentada, com relação aos procedimentos técnicos foi subdividida em 2 (duas) etapas:

1. Pesquisa bibliográfica/*sites*: de acordo com Gil (2002) A pesquisa bibliográfica é estruturada especialmente de livros e artigos científicos que embasem e norteiem o pesquisador. No entanto, o tema escolhido exige referência novas, motivo pelo qual esta pesquisa utilizou mais referência de *sites* conceituados.
2. Pesquisa de Campo: de acordo com Lopes (2006) é a “pesquisa em que se realiza uma coleta de dados através de entrevistas, e/ou questionários, observação, in loco, para análise de resultados posteriores”. Esta pesquisa consistiu da aplicação de um questionário junto aos discentes de quatro cursos da UEPB campus VII.

Durante a pesquisa bibliográfica foram coletados e estudados trabalhos recentes, provenientes da internet, artigos e livros; com objetivo de embasar o pesquisador e produzir referencial teórico para uma melhor compreensão deste trabalho pelos leitores leigos ou para servir de revisão para leitores especialistas.

A pesquisa de campo consistiu da aplicação de um questionário junto aos discentes dos cursos de Computação, Administração, Física e Matemática da UEPB campus VII com o objetivo de coletar dados que pudessem avaliar o quanto eles se protegem com relação a segurança em tecnologias móveis e se já foram afetados por intrusão e/ou *malwares*, especificamente em seus smartphones.

As perguntas contidas no questionário aplicado podem ser categorizadas em:

- Utilização de aplicativos e outros recursos de segurança;
- Cuidados com Redes;
- Utilização /qualidade de bloqueios e senhas a recursos e informações;
- Averiguação se o público alvo já adquiriu *malware* ou teve sua privacidade invadida.

O público alvo foram discentes do primeiro ao terceiro período dos quatro cursos do campus VII da UEPB. O questionário foi aplicado a 20 alunos de cada um

dos cursos, totalizando 80 entrevistados. No tocante aos objetivos desta fase da pesquisa:

- Objetivo geral: Avaliar os discentes dos cursos de Computação, Administração, Física e Matemática do campus VII da UEPB com relação ao grau de segurança que os mesmos empregam ao utilizar tecnologia móvel, especificamente *smartphones*;
- Objetivo específico: Avaliar se os discentes do curso de Computação do campus VII da UEPB empregam maior grau de segurança para com os seus *smartphones* com relação aos discentes dos cursos de Administração, Física e Matemática, tendo em vista que os profissionais da computação devem ter, de forma inerente a sua formação, um maior grau de conhecimento com relação a esta área.

3 REFERENCIAL TEÓRICO

Neste capítulo são abordados alguns tópicos importantes para compreensão da temática deste trabalho. Os mesmos servirão de embasamento para leigos e como tópicos de revisão para profissionais e especialistas da área.

3.1 DISPOSITIVOS MÓVEIS

Antigamente para se comunicar com alguém a longa distância era necessário enviar cartas e esperar um durável período de tempo para chegar, afim de que a outra pessoa pudesse enviar sua resposta. Depois de décadas, surgiram os aparelhos de telefone que serviam para conectar duas pessoas distantes geograficamente, posteriormente surgiu os aparelhos celulares que tinham como uma de suas funções fazer ligações para outros, assim como os telefones, contudo a diferença era que um tinha portabilidade e outro não. Nos dias de hoje, com os incríveis avanços tecnológicos os telefones inteligentes (*smartphones*) tem um conjunto de funções que se comparam a um computador de hoje em dia, não só fazem ligações como antigamente, eles desempenham diferentes funções, como acessar a internet e possuem processadores, hardware, memória interna e são capazes de armazenar grande quantidade de arquivos e dados.

Portabilidade – segundo (BICALHO, 2016) a característica de um equipamento que não tem necessidade de usar componentes separados como monitor, teclado e mouse para e pode ser conduzido com facilidade. Um bom exemplo é um notebook, pois já vem com um conjunto de tela, teclado, mouse, *drive* de internet e uma bateria.

Mobilidade – de acordo com (BICALHO, 2006) é a capacidade de um dispositivo móvel ser adequadamente utilizado em movimento, para acesso a internet e/ou outras funcionalidade.

Os telefones celulares tiveram uma evolução significativa a partir da década de 90, contudo, o design dos aparelhos móveis foi projetado no início da época de 1980 pela empresa alemã Frog, em 1983 um aparelho de telefone com funções alternativas foi apresentado e considerado um dos primeiros dispositivos a ter opções além da chamada de telefone (VOLTONI, 2014).

De acordo com (ROBERT, 2014) o IBM Simon foi anunciado em 1992 durante a COMDEX, mas foi em 1994 poucos anos depois que o aparelho foi lançado e se tornou tecnicamente o primeiro smartphone criado, mas, o termo não foi considerado a ele, e sim ao Ericsson R38 que foi prestigiado como o primeiro celular inteligente da história, com o Sistema Operacional Symbian, lançado no ano de 2000 com o preço de U\$\$ 700.

No ano de 2007 durante a MacWorld, Steve Jobs inovou os celulares daquela época apresentando ao mercado o iPhone, o mais revolucionário de todos, ajudou a definir o comércio de celulares inteligentes (*smartphone*), pois se diferenciava de outros pelo fato de remover o teclado físico (utilizando só os dedos para manusear), tinha uma maior facilidade de uso e trazia uma interação entre software e hardware (JORDAO, 2014). A respeito do seu S.O., ele ainda não era o iOS que conhecemos hoje, era uma plataforma baseada em HTML, por isso todas as aplicações seriam Webapps, página de internet que rodaria como aplicativo. Em 2008 nasce o iOS e a App Store, lançado em 9 de junho o iPhone 3G foi o segundo smartphone da Apple com suporte e aplicativos de terceiros, junto com novo sistema operacional iPhone OS 2.0 e conexão 3G.

3.2 HACKER E CRACKER

De alguma maneira as pessoas já ouviram pela mídia que “*hackers*” invadiram sistemas, roubaram informações ou subtraíram dinheiro em contas bancárias, elas

cotejam com pessoas de má índole, pois a mídia desvirtuou a imagem do *hacker* associando-o às pessoas perigosas. Diferentemente do que a mídia tenta transmitir, os *hacker* nem sempre são pessoas más, muitos estão ali para ajudar empresas procurando por erros em seus sistemas, diferente dos *cracker* que tentam achar uma fissura no sistema para poder obter informações ou implantar seus vírus, com a finalidade de prejudicar e conquistar lucro.

Os *hackers* também formam comunidades as quais podem ajudar a sociedade. No ano (2016) o presidente da Agência Nacional de Telecomunicações (Anatel), João Rezende, afirmou que a agência não irá regular ou controlar os modelos de negócio das empresas prestadoras de acesso à internet, ou seja, as operadoras tem o poder de limitar ou não a internet fixa. Em oposição a medida da Anatel de regulamentar a comercialização da internet fixa em pacotes (o que prejudicaria estudantes e várias classes da população brasileira), um grupo de *hackers* (Anonymous) invadiu o site da Anatel, e divulgou nas redes os dados pessoais do presidente da Anatel, e também declarou guerra contra as operadoras se continuassem com essa ideia, chamando a iniciativa de “OpOperadoras”.

De acordo com (LEITÃO, 2010) o termo *hacker* é dedicado a toda e qualquer pessoa que possui interesse e um alto conhecimento nessa área, de maneira que a mesma saiba identificar brechas e elaborar softwares e/ou hardwares de computadores, ou seja, desenvolver funcionalidades novas ou adaptando as antigas.

O termo *cracker* é usado para definir uma pessoa que possui alto nível de conhecimento na área. Entretanto, esses protagonistas não utilizam seu aprendizado para o bem, pois, invadem, pirateiam e até manipulam sistemas operacionais a seu favor. Assim, muitos têm prioridade de enfatizar mais o funcionamento do programa, pois são responsáveis na quebra de segurança do software, criando os cracks, com isso possibilitando a pirataria (LEITAO,2010).

Os *hackers* têm seu próprio modo e atitudes dentro de uma ética própria, para diferenciar essa forma e ética, foi criado uma classificação para distingui-los denominada de “chapéus”. De acordo com (TACIO, 2010) os chapéus oficiais foram criados por *hacker*, e outros foram por usuários comuns, uns por motivo de diversão e outros para discernir uma ação *hacker* específica. Os chapéus White Hat (chapéu branco), Black Hat (chapéu preto) e o Gray Hat são os mais conhecidos pela comunidade *hackers* dentre os vários que existem. Ainda de acordo com (TACIO, 2010):

- *White Hat* (Chapéu branco) – É o *hacker* ético e que trabalha dentro da lei, profissional em segurança da informação, ele invade com o intuito de achar brechas em um sistema ou software, avisando ao administrador a vulnerabilidade para que seja corrigida.
- *Black Hat* (Chapéu preto) – É o *hacker* que não tem ética e que inflige as leis, são os bandidos cibernéticos, usam sua inteligência para ludibriar pessoas, invadir computador/*smartphone*, acabar com sistemas e criar malware, essas pessoas que agem no lado negro da rede não são consideradas *hacker* e sim como um *cracker*.
- *Gray Hat* (Chapéu cinza) – É o *hacker* que fica " em cima do muro ", pois não cometem crimes, igual aos *White hats*, contudo, se uma empresa tiver uma brecha no seu sistema, os *Gray hats* não avisam a existência da vulnerabilidade e nem tentam corrigi-la, sem contar que eles ficam observando os dados que são inseridos, e as vezes até divulgam, pois na concepção deles não estão cometendo crime.
- Hactivista – São motivados por questões ideológicas tanto políticas quanto religiosas que julgam válidas para eles e geralmente tem como objetivo revelar ao mundo informações sobre os problemas existente.
- *Lammer (Script Kiddie)* – São pessoas amadoras que utilizam softwares desenvolvido por "*Black hat/ Cracker*" para realizarem seus ataques, sem saber nada do que está fazendo, pois dispõem de nenhum ou pouco conhecimento sobre tecnologia avançada.

3.3 MALWARE

As ameaças para computadores em seus anos iniciais não eram tão eficientes como as ameaças para os dispositivos móveis de hoje, os quais estão se desenvolvendo extremamente rápido em relação aos antigos. Esses dispositivos são mais eficientes em coletar e agrupar informações quando comparado aos PCs, pois adquirem dados em abundância tanto pessoais quanto financeiros e, por isso, o foco dos crackers hoje são os dispositivos móveis, principalmente para roubar dados financeiros (NOVAES, 2014).

Segundo Fred Cohen (1984) “Um vírus de computador é um programa que pode infectar outro programa de computador através da modificação dele de forma a incluir uma cópia de si mesmo.”

Vírus são softwares maliciosos que podem suprimir dados, obter informações, modificar ou obstruir o funcionamento do S.O., conseguem ocasionar dores de cabeça para grandes empresas, instituições e a usuários domésticos (RAFAELA, 2013). Há softwares similares, como *worms*, *cavalo de troia*, *spywares* e *ransomwares*. Atualmente, algumas pessoas chamam qualquer software malicioso de vírus, sendo o vírus apenas uma classe deles. Logo a expressão *malware* foi idealizada para engloba-los, cujo significado é a fusão das palavras *malicious* e *software* (software malicioso) (ALECRIM, 2016).

Os tipos de malware mais utilizado para dispositivos móveis são:

- Cavalo de troia (trojan) – Esse *malware* normalmente se passa por outro software efetuando ações que o usuário não dá autorização, como acesso remoto ao dispositivo (LEMONNIER, 2015). Um exemplo é o Azacub. De acordo com a Kaspersky (2015) Foi desenvolvido para dispositivos móveis que utilizam Android, esse tipo de malware obtém dados bancários dos usuários para adquirir rendimento financeiro.
- *Ransomware* – De acordo com (CARDOSO, 2016) O *ransomware* é um tipo de *malware* que bloqueia o acesso do usuário ao sistema infectado e cobra uma quantia em dinheiro para libera-lo, normalmente utilizando a moeda virtual bitcoin, o que torna quase impossível de detectar o malfeitor que pode vir a adquirir o valor. Ex.: *Simplocker* primeiro *ransomware* móvel que criptografava imagem, vídeos e documentos gerando chaves únicas para cada aparelho infectado tornando difícil de descriptografá-lo.
- *Spywares* – O próprio nome já incumbe, software espião, ou seja, programa que permite vigiar atividades online, comunicações e roubar informações a partir de um smartphone. Segundo (ALECRIM, 2016) *spywares* são softwares que contaminam um computador/ dispositivo móvel para espreitar os usuários ou obter informações sobre eles. Com o objetivo de espionar, os *spywares* normalmente vêm encastado em softwares cujo a fonte é duvidosa.

3.4 ATAQUES DE REDE

Ataques de rede tem inúmeros objetivos, tendo em vista diferentes alvos e aplicando variadas técnicas (como por exemplo, *malware* instalado no dispositivo com intuito de transmitir informações para o criminoso, *backdoor* e ataques de procura de chaves), assim qualquer computador ou dispositivo conectado à rede pode ser alvo de um ataque. Dentre eles, podemos destacar os mais populares:

Backdoor – Conhecido também como porta dos fundos por fazer analogia a um ataque pelos fundos de uma casa por onde ocorre a invasão, sem que o dono saiba, logo, são programas maliciosos (*malware*) que aproveitam as falhas de segurança do sistema operacional ou de um aplicativo, permitindo o controle de usuários remotos de longa distância, obtendo suas informações sem que o mesmo saiba (NOVAES, 2014);

Man in the middle (MITM) – É um ataque em que o invasor intercepta os dados de troca de conversa entre suas vítimas. O *cracker* utiliza as falhas de um roteador WiFi como mecanismo para poder capturar as conversas ou simplesmente se passa por um ponto de acesso e o coloca com um título conhecido pelo usuário, assim vigiando todo seu tráfego na rede, podendo substituir ou modificar as mensagens sem que a vítima saiba (MALENKOVICH, 2013);

Botnet – Segundo (NOVAES, 2014) É conhecido como rede de computadores zumbis pelo fato de muitos computadores contaminados por malwares estejam interligados para atacar um mesmo alvo específico conduzido por um “chefe”. São adquiridos por e-mails falsos, por amigos já infectados ou de links cuja fonte é desconhecida fazendo download automático de um arquivo com extensão .exe;

DDoS (Distributed Denial of Service) Attack – De acordo com (THIAGO, 2012) É uma maneira de sobrecarregar o sistema com o intuito de derruba-lo, tem como objetivo tornar indisponível para o usuário uma página ou algum software que esteja conectado à rede. Para que o ataque tenha sucesso, os *cracker* precisam criar uma rede zumbi (Botnet), de maneira que eles possam ser controlados por um *host* “chefe”.

Phishing – Um dos ataques mais comum e bem sucedido praticado pelos cibercriminosos. De acordo com (POZZEBON, 2014) Tem por finalidade a tentativa de obter informações do usuário, como senhas bancárias e números de cartão de crédito, por meio de fraudes eletrônicas, basicamente se passa por uma pessoa de sua confiança ou uma empresa reconhecida popularmente, enviando um e-mail, correio eletrônico ou sms pedindo para acessar o link.

3.5 VPN

Rede Privada Virtual (*Virtual Private Network - VPN*), é uma rede que conecta dois computadores por meio de túneis criptografados, criados através da internet públicas ou privadas mantendo os tráfegos dos dados seguro entre uma rede corporativas ou uma rede de usuários remotos (CELESTINO, 2005, p. 34).

Esses pacotes são enviados por meio de redes públicas, internet, utilizando um processo conhecido por “tunelamento” (*tunneling*), que simula uma conexão ponto a ponto em um túnel privado preservando as informações trocadas entre eles em virtude da encriptação dos dados. Conforme Felipe (2015) uma VPN proporciona que o usuário navegue de forma anônima em lugares onde o acesso do conteúdo (site, aplicativo) não possa ser utilizado.

As vantagens da VPN é que diminuem muito o custo em comparação às redes dedicadas, isso é devido ao fato das VPN aplicarem a internet como conexão através dos hosts e gateways diminuindo a tarifa de implementação. Outra vantagem é que a utilização da VPN permite que seus usuários acessem conteúdos indisponível na internet em países cujo o governo é autocrático e limita seus cidadãos ao acesso (GARRET, 2015). Uma das desvantagens é que o cliente precisa ter uma rede com velocidade alta, pois quando o usuário se conecta a uma VPN ele passa a utilizar uma rede local (LAN) como se estivesse dentro dela. Uma VPN também pode assegurar que seus dados não serão capturados pelo gerenciador de uma rede *wi-fi* pública.

Alguns aplicativos de VPN bem avaliados na Google Play, para Android, é o Turbo VPN, VPN Master, Betternet VPN, entre outros de uma lista ampla. Todos são grátis (boa parte é grátis, mas disponibiliza pagamentos de assinaturas mensais ou anuais, que dão acesso a recursos melhores). Já para iOS existem: IPvanish, ExpressVPN, VYPR VPN, entre outros.

3.6 SEGURANÇA EM REDES

Nos dias de hoje é habitual sair de casa e encontrar vários lugares com redes Wi-Fi com acesso livres ou pagos dependendo do local. Há algum tempo não se

encontrava muitos locais com acesso *wi-fi* grátis, hoje por outro lado, estão presentes em shoppings, lanchonetes, bares, cafeterias, universidades, aeroportos, entre outros locais. Contudo, usar conexões públicas pode deixar suas informações vulneráveis, isso porque em locais de acesso à rede pública, qualquer pessoa pode se conectar e usar a internet, principalmente as pessoas que têm más intenções de obter seus dados para fins ilícitos.

Algumas medidas preventivas são necessárias para sua segurança de privacidade em redes *wi-fi* públicas, com isso evitando que você seja um alvo fácil dos cibercriminosos, tais medidas são:

- Evitar conexão automática em redes *wi-fi* públicas – De acordo com (CAROLINE, 2013) é bom verificar se o seu dispositivo está conectando automaticamente à internet ao encontrar uma rede *wi-fi* pública. Caso esteja, desabilite, pois assim evita pessoas mal intencionadas querendo roubar suas informações.
- Utilização de VPN – É a maneira mais segura para acessar uma rede *wi-fi* pública, já que ela garante privacidade em um tráfego de dados com criptografia (GABRIELA, 2016).
- Instalação de antivírus – É relevante instalar um antivírus para se defender de malwares transferidos para o seu dispositivo por meio de uma rede *wi-fi* pública, pois assim será alertado pelo mesmo quando alguém tentar sujeitar o aparelho.
- É importante certificar-se de acessar endereços com conexão segura – Observe se o endereço tem a presença do HTTPS ou de um pequeno ícone de cadeado na barra de endereço do seu navegador, pois são protocolos de segurança com uma conexão criptografada.

Outras medidas de prevenção são utilizar aplicativos seguros que ofereçam proteções nas comunicações estabelecidas dos dados pessoais, assim prevenindo possíveis furtos de informações futuras. Logo, os aplicativos mencionados a posterior auxiliam na proteção de informações pessoais e, estão disponíveis para serem baixados para *smartphones* com S.O Android na loja do play store da google.

- Orbot – Utiliza proxy com Tor para criptografar o seu tráfego da internet usando uma série de caminhos alternativos de computadores por todo o mundo.

- Orfox (Browser) – Desenvolvido com o mesmo código do navegador Tor, baseado também no navegador Firefox, mas com pequenas modificações a fim de melhorar a privacidade.
- Pixelknot – Esconde mensagem em uma figura, que somente seus amigos com uma senha poderão destravar sua mensagem, outros só conseguirão ver somente uma imagem normal.

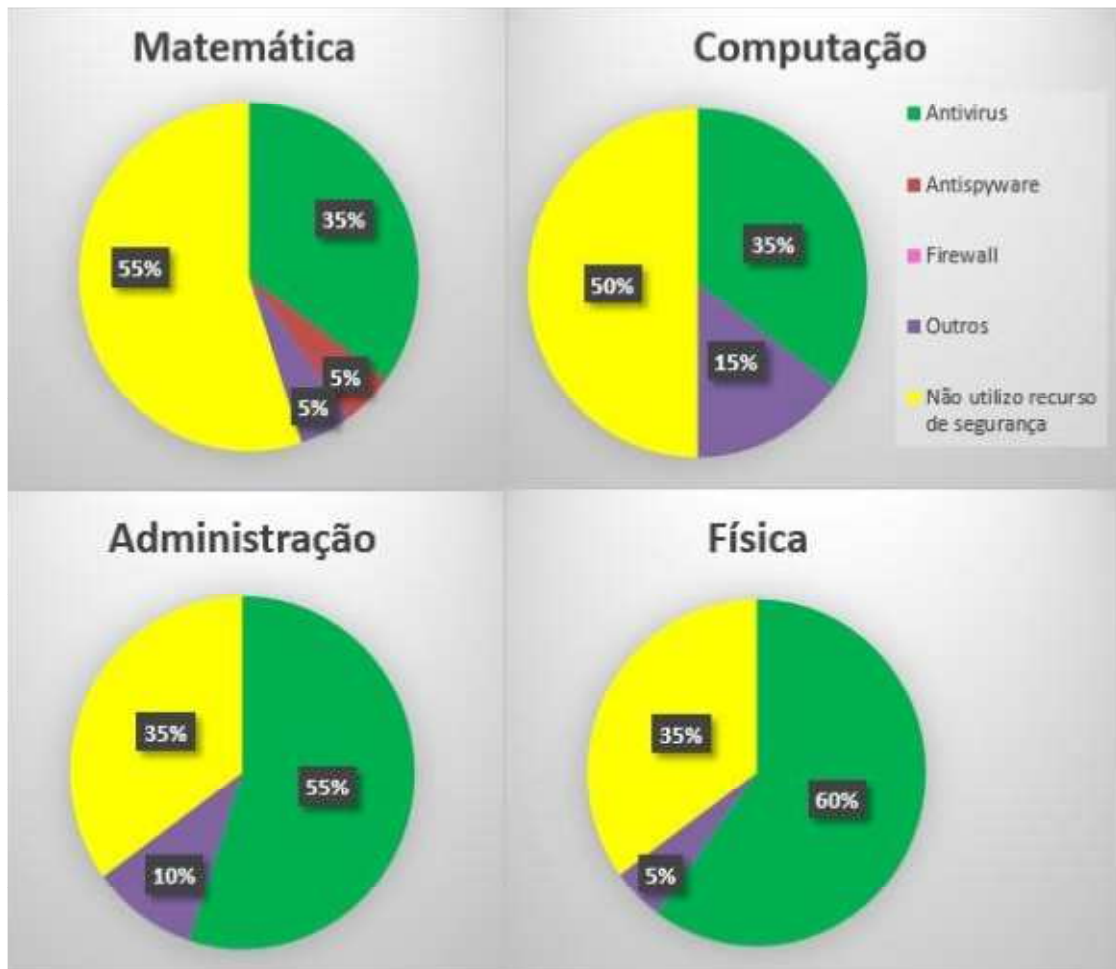
4 PESQUISA DE CAMPO

Neste capítulo são apresentados os dados da pesquisa de campo, além da análise dos mesmos, para cada um dos 9 questionamentos aplicados aos discentes do campus VII da UEPB para os cursos de Licenciatura em Matemática, Bacharelado (e Licenciatura) em Computação, Bacharelado em Administração e Licenciatura em Física; serão apresentados os gráficos e em seguida a respectiva análise. As categorias dos questionamentos são: i) utilização de aplicativos e outros recursos de segurança, ii) cuidados com redes, iii) utilização/qualidade de bloqueios e senhas a recursos e informações e iv) averiguação se o público alvo já adquiriu malware ou teve sua privacidade invadida. Os subtópicos a seguir fazem concordância as categorias de perguntas supracitadas.

4.1 Utilização de Aplicativos e Outros Recursos de Segurança

Primeira pergunta: "Você utiliza algum recurso de Segurança em seu *smartphone*?"

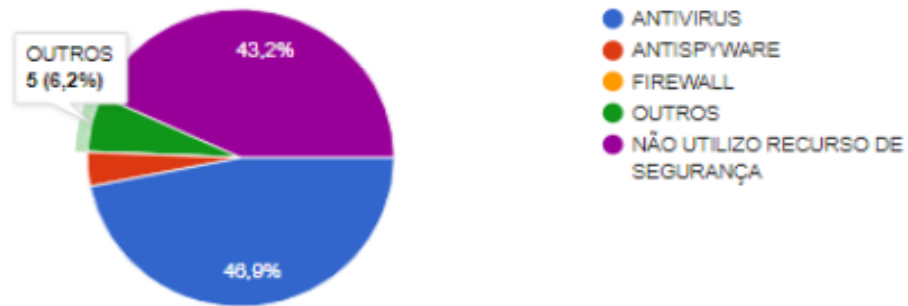
Gráfico 4.1 - Utilização de recursos de segurança em smartphones por curso.



Fonte: Diogo (2017).

De acordo com os gráficos da Figura 4.1, metade ou mais dos entrevistados nos cursos de Física e Matemática não utilizam nenhum meio para proteger-se contra ameaças de dispositivos móveis, número que é reduzido a 35% para os cursos de Administração e Computação. Outra informação importante extraída do gráfico é que a forma de proteção mais utilizada nos smartphones para todos os cursos é o antivírus (confirmado na Figura 4.2) e que o curso de Computação lidera em número de usuários deste recurso de proteção, isto pode ocorrer devido um possível maior interesse/conhecimento acerca das ameaças. Observa-se ainda, na Figura 4.2 que em todos os cursos apenas um entrevistado utiliza *antispyware* e nenhum se preocupa com *firewall*.

Gráfico 4.2 - Utilização de recursos de segurança em smartphones em todos os cursos.

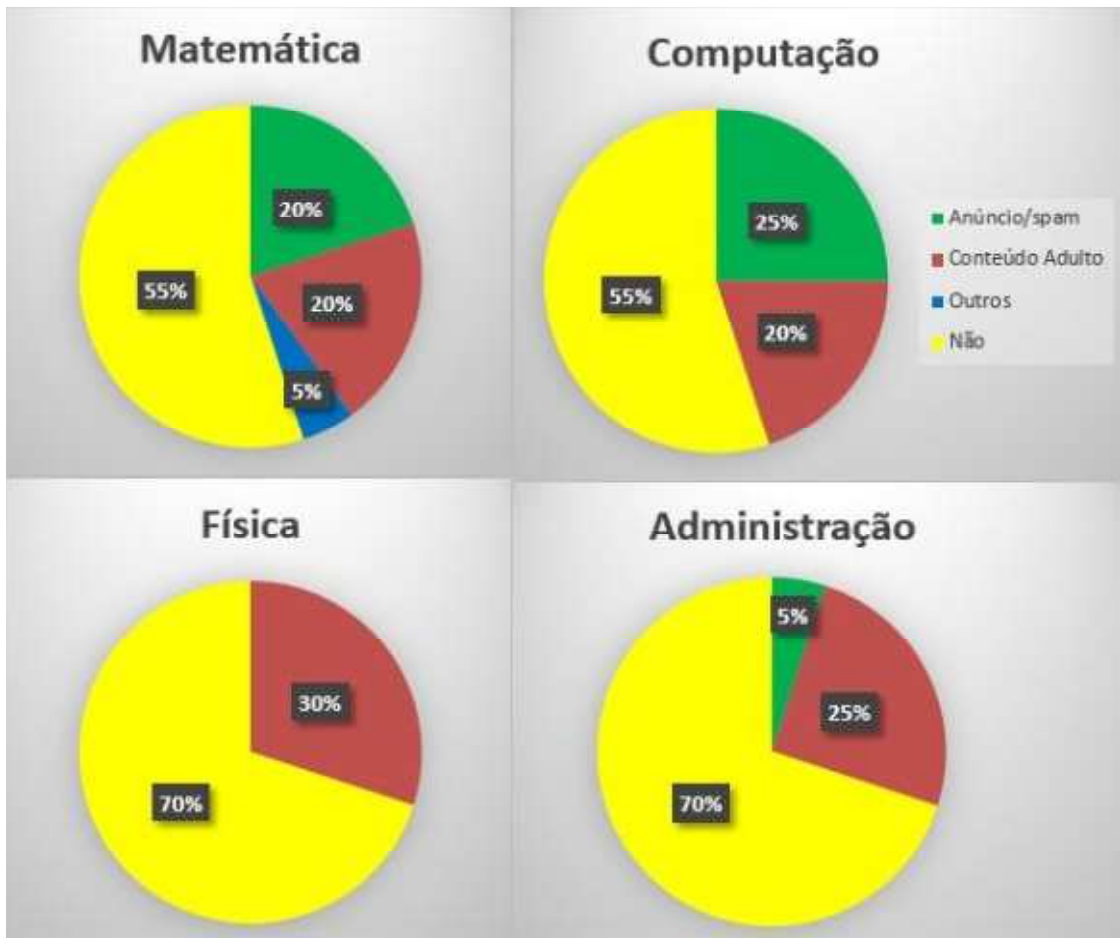


Fonte: Diogo (2017).

4.2 Cuidados com Redes

Segunda pergunta: "Em seu *smartphone*, você acessa páginas desconhecidas as quais acredita que possam ser potencialmente perigosas (oriundas de pesquisa, com propostas atrativas etc.)?"

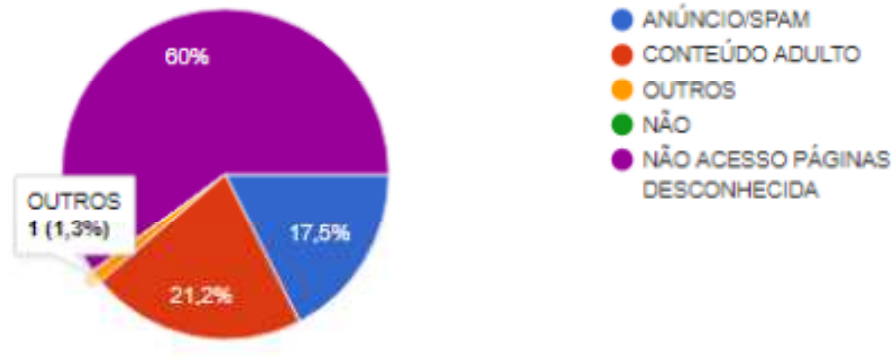
Gráfico 4.3 - Acesso às páginas desconhecidas potencialmente perigosas por curso.



Fonte: Diogo (2017).

De acordo com o gráfico da Figura 4.3 a maioria dos entrevistados em todos os cursos afirmaram não acessar páginas desconhecidas as quais acreditam que possam ser potencialmente perigosas. Entre todos os cursos as páginas de conteúdo adulto seguem como o segundo item mais marcado neste questionamento. Outro dado interessante é que muitos discentes de Computação e Matemática acessam anúncios/spam.

Gráfico 4.4 - Acesso às páginas desconhecidas potencialmente perigosas em todos os cursos.



Fonte: Diogo (2017).

Terceira pergunta: " Você utiliza conexões públicas desconhecidas em seu *smartphone*? "

Gráfico 4.5 - Acesso a conexões públicas desconhecidas por curso.



Fonte: Diogo (2017).

Gráfico 4.6 - Acesso a conexões públicas desconhecidas para todos os cursos.

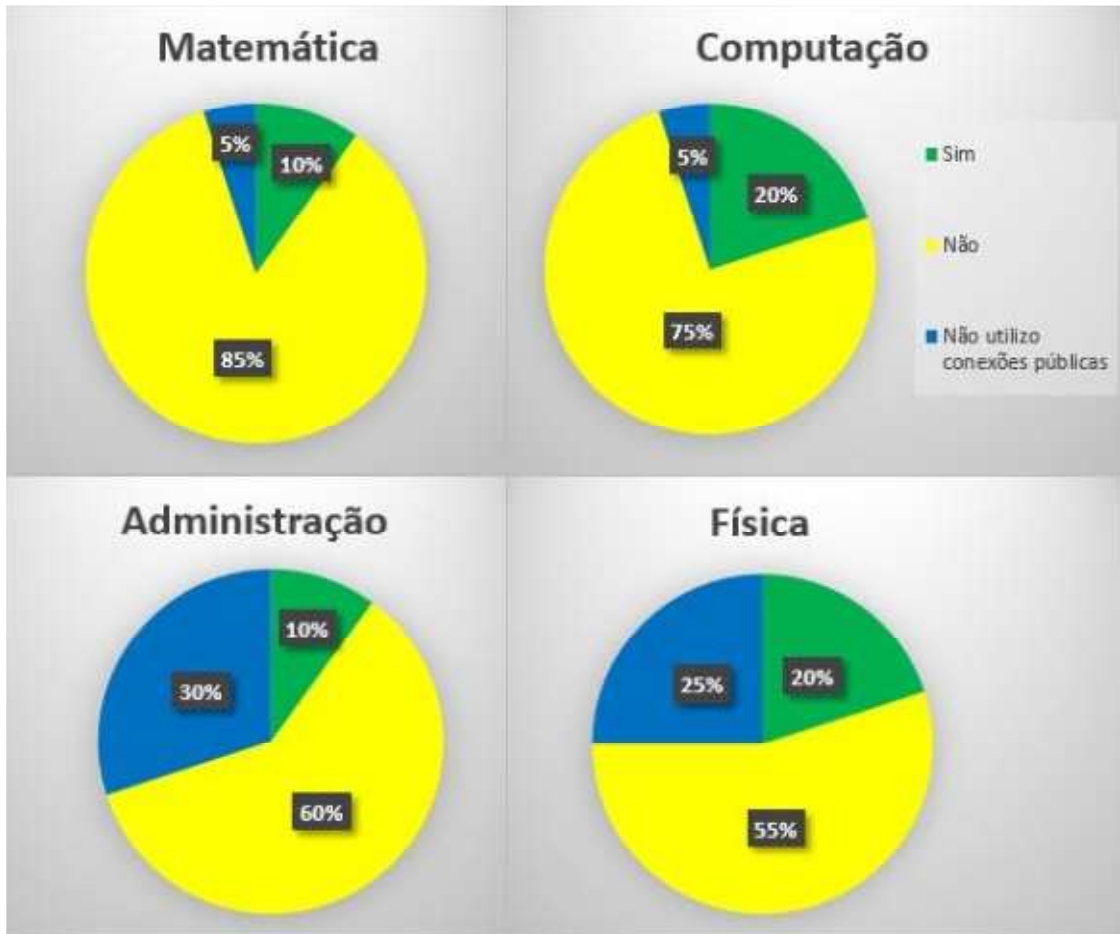


Fonte: Diogo (2017).

Conforme os gráficos das Figuras 4.5 e 4.6 pode ser observado que entre os cursos de Administração e Física a maioria não utilizam conexões públicas desconhecidas, por outro lado, tanto Computação como Matemática parecem se importar menos ao navegar por conexões desconhecidas, possivelmente por acreditarem que sabem melhor se proteger, por serem pertencentes/próximos a área de TI.

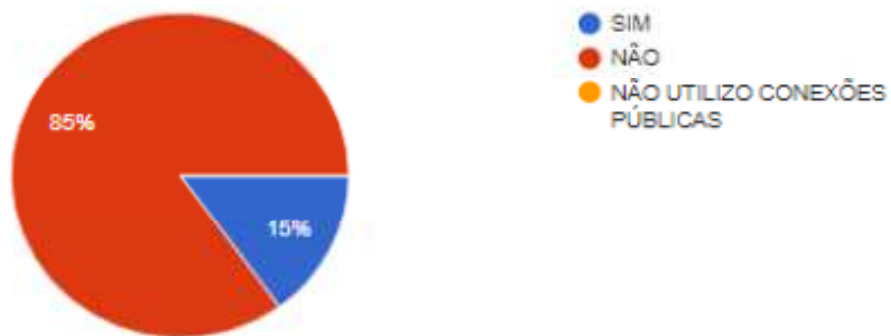
Quarta pergunta: "Em locais com conexões públicas conhecidas, você utiliza em seu *Smartphone* algum meio para proteger suas informações? "

Gráfico 4.7 - Meios de proteção em conexões públicas conhecidas por curso.



Fonte: Diogo (2017).

Gráfico 4.8 - Meios de proteção em conexões públicas conhecidas para todos os cursos.



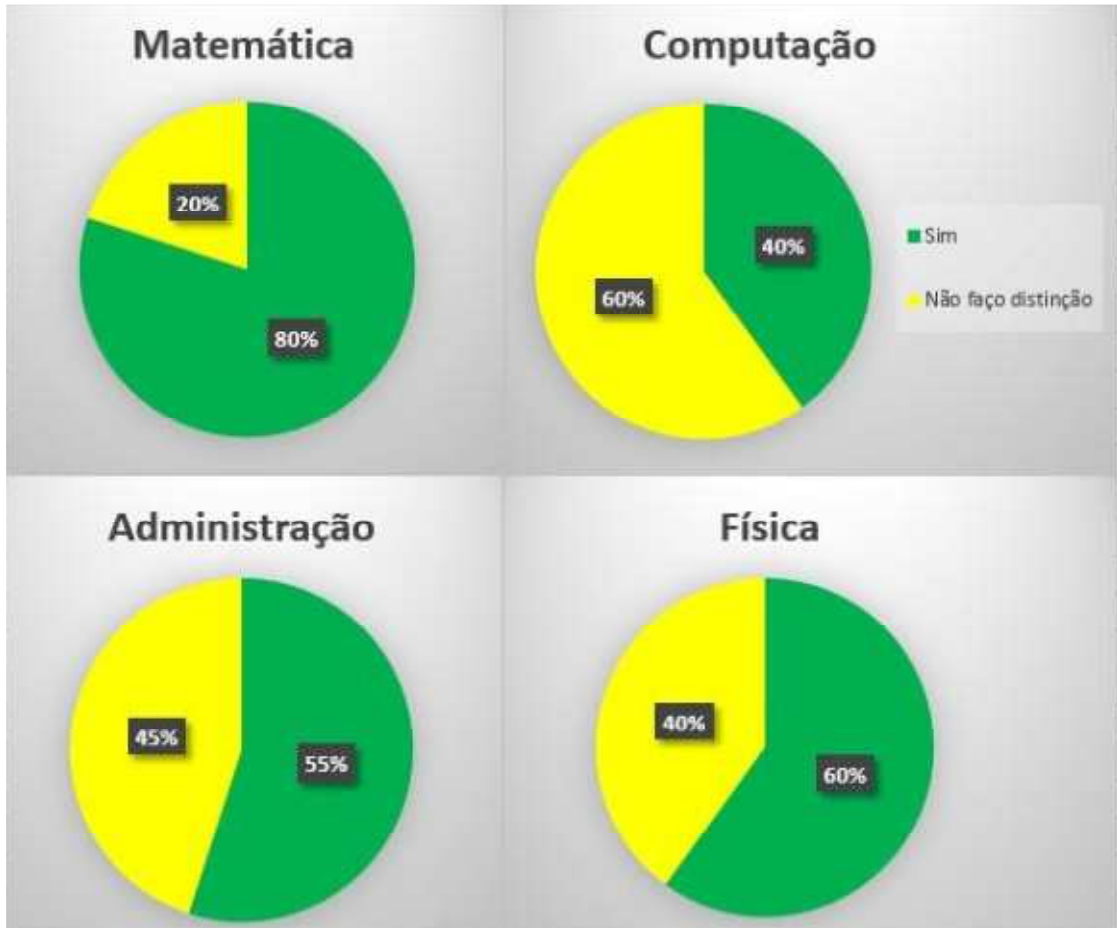
Fonte: Diogo (2017).

De acordo com os gráficos das Figuras 4.7 e 4.8 a maioria dos entrevistados em todos os cursos não utilizam meios para proteger suas informações desde que navegando em conexões públicas as quais conheça. É importante atentar ainda que

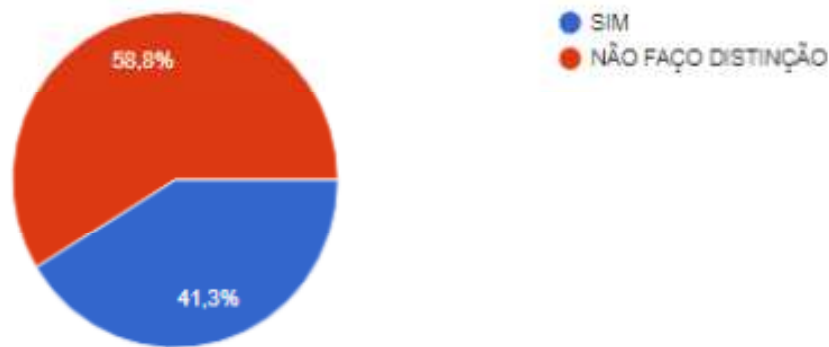
Física e Administração estão entre os que menos utilizam estas conexões públicas, embora que conhecidas.

Quinta pergunta: "Quando está navegando pela rede, através de seu *Smartphone*, você dá preferência a sites que tem a presença do HTTPS ou um pequeno ícone de cadeado? "

Gráfico 4.9 - Preferência por sites com HTTPS por cursos.



Fonte: Diogo (2017).

Gráfico 4.10 - Preferência por sites com HTTPS para todos os cursos.

Fonte: Diogo (2017).

Segundo os gráficos das Figuras 4.9 e 4.10 os cursos de Computação, Matemática e Administração não dão prioridade a sites com presença de HTTPS, por consequência disso podem ser alvos de sites potencialmente perigosos, com isso comprometendo a integridade do seu dispositivo sem saberem. Já no curso de Física 60% dos entrevistados usam sites que indiquem ser mais seguros para acesso.

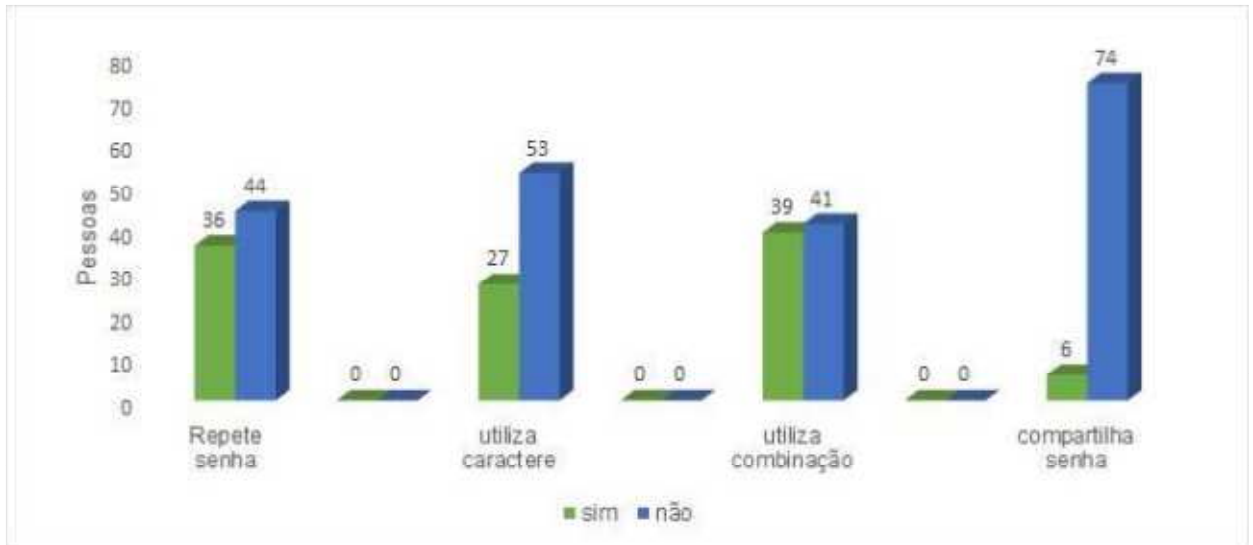
4.3 Utilização/qualidade de bloqueios e senhas a recursos e informações

Sexta pergunta: "Com relação as senhas utilizadas em seu *smartphone*"

Quadro 1 – Questionário da sexta pergunta.

Repete senhas entre diversos serviços/aplicativo	SIM []	NÃO []
Utiliza caractere especiais	SIM []	NÃO []
Utiliza combinação de letras maiúsculas e minúsculas	SIM []	NÃO []
Compartilha senhas por redes sócias ou aplicativos	SIM []	NÃO []

Fonte: Diogo (2017).

Gráfico 4.11 - Utilização de práticas de segurança com a relação de senhas, todos os cursos.

Fonte: Diogo (2017).

Quadro 1.1 – Utilização de práticas de segurança com a relação de senhas, por curso.

	Repete senhas		Caractere especial		Combinação letra		Compartilha senhas	
	Sim	Não	Sim	Não	Sim	Não	Sim	Não
Administração	8	12	8	12	10	10	1	19
Computação	12	8	6	14	10	10	4	16
Física	6	14	8	12	11	9	0	20
Matemática	9	10	6	14	9	11	2	18

Fonte: Diogo (2017).

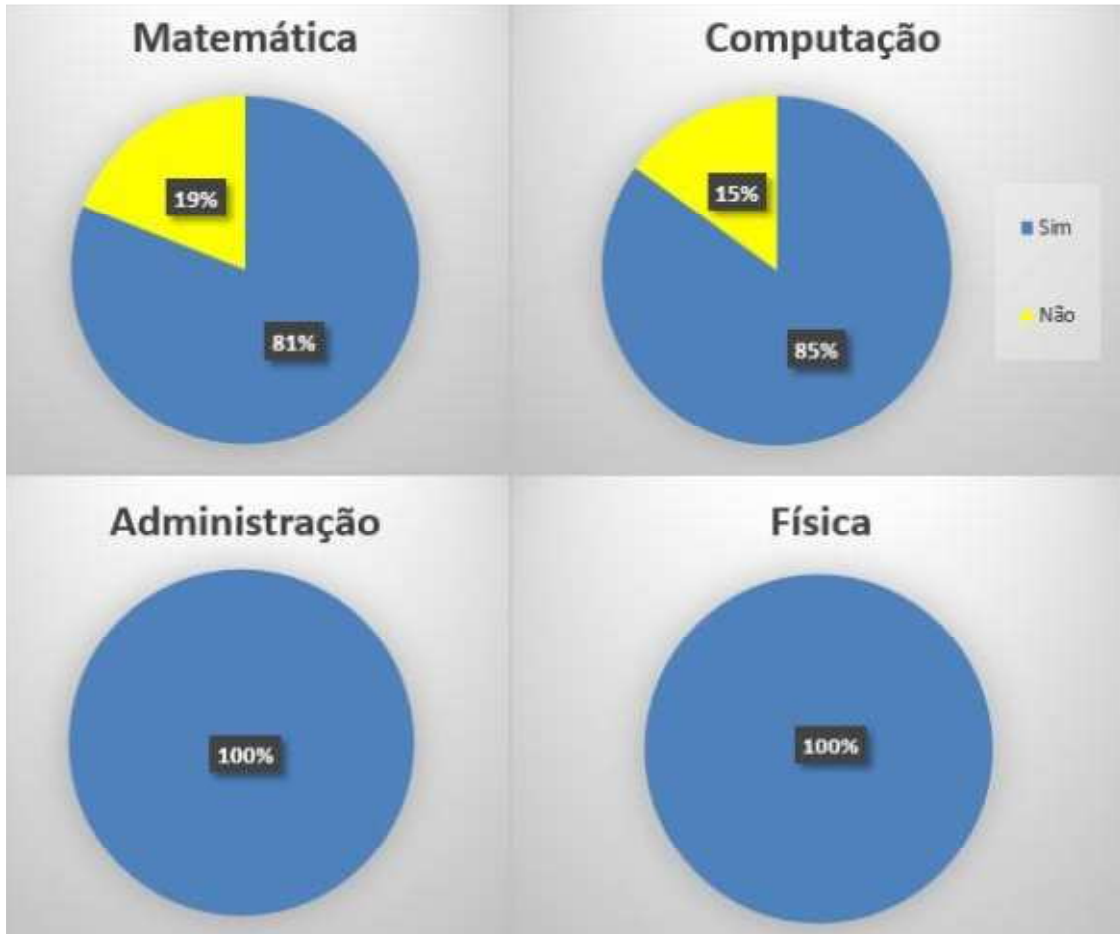
A Figura 4.11 mostra o gráfico geral (todos os cursos) acerca de senhas. Percebe-se que uma pequena maioria não repete senhas, ou seja, ainda há um descuido muito grande com essa atitude essencial em segurança. Já com relação a utilização de caracteres especiais, esta prática é muito importante para dificultar ataques *brute force*, no entanto, a maioria dos entrevistados não utilizam esta prática. Já a combinação de letras maiúsculas e minúsculas praticamente divide os entrevistados. Com relação ao compartilhamento de senhas, ao menos esta prática é largamente evitada entre os entrevistados.

O quadro 1.1 revela que quem mais repete e compartilha senhas são os discentes de Computação e quem menos faz uso das duas práticas são os de Física. Sobre os caracteres especiais em senhas, quem mais usa são os alunos de

Administração e Física. Acerca da combinação de letras nas senhas os números são mais ou menos divididos.

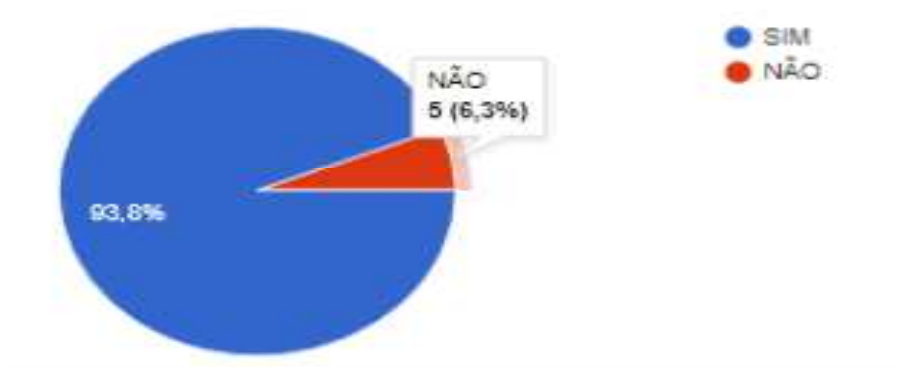
Sétima pergunta: "Utiliza algum meio de bloqueio de acesso a recursos e informações em seu *smartphone* (bloqueio a aplicativos e arquivos, outros bloqueios) "

Gráfico 4.12 - Utilização de meios de bloqueio a recursos e informações por curso.



Fonte: Diogo (2017).

Gráfico 4.13 - Utilização de meios de bloqueio a recursos e informações para todos os cursos.



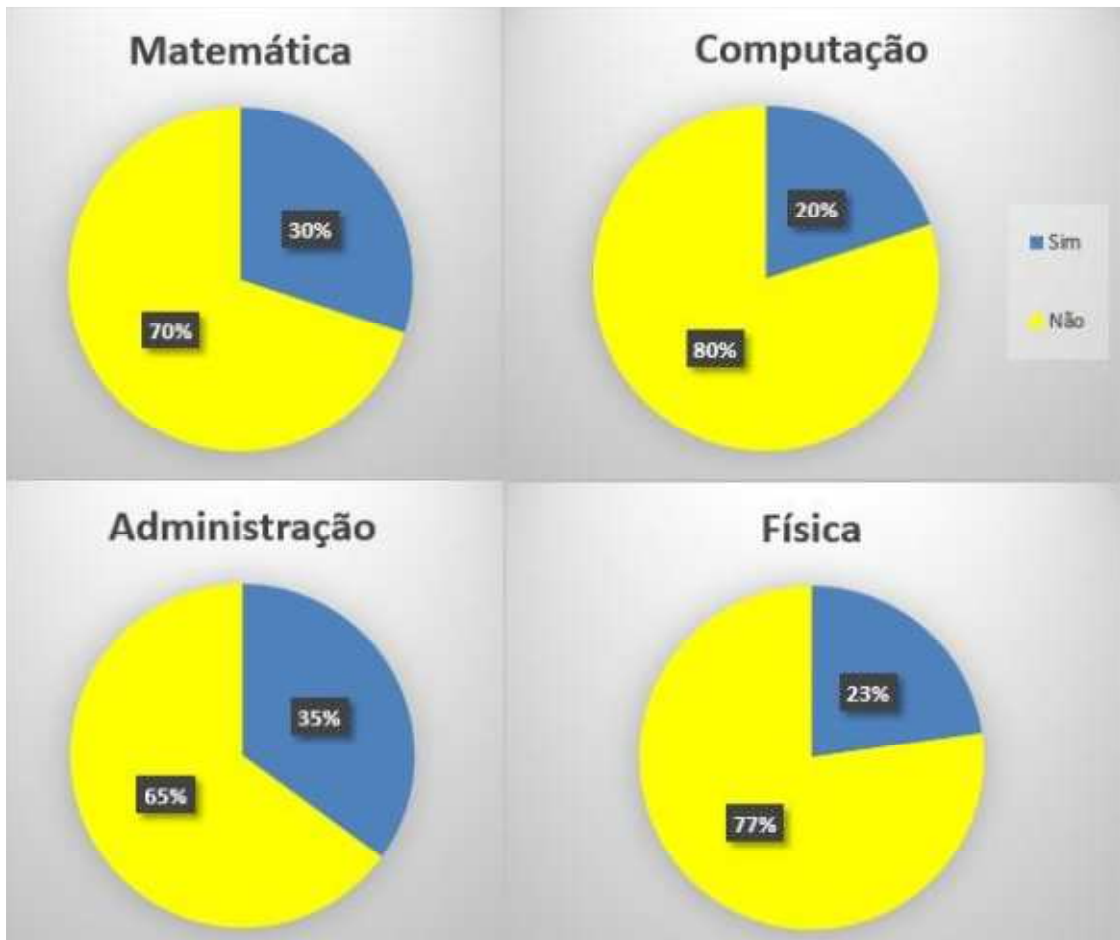
Fonte: Diogo (2017).

De acordo com os gráficos das Figuras 4.11 e 4.12 todos os entrevistados (100%) entre os cursos de Física e Administração utilizam meio de bloqueio para se proteger contra acessos a informações e recursos em seus smartphones, a totalidade da soma utiliza tela de bloqueio e outros aplicativos para impossibilitar o acesso a arquivos, documentos e fotos do seu smartphone mantendo sua privacidade. Pode ser observado também que entre os cursos de Computação e Matemática, boa parte desfruta de aplicativos de bloqueios, já uma pequena parte não utiliza nem um tipo de artifício para tal finalidade.

4.4- Averiguação se o público alvo já adquiriu malware ou teve sua privacidade invadida.

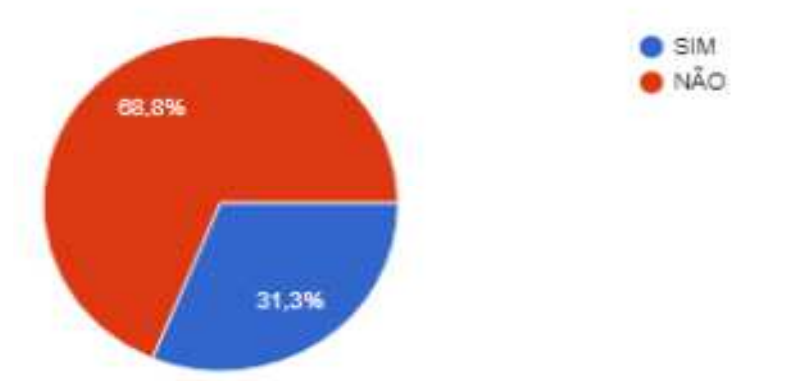
Oitava pergunta: "Você já adquiriu algum *Malware* em seu *smartphone*?"

Gráfico 4.14 - Acerca da aquisição de malware por curso.



Fonte: Diogo (2017).

Gráfico 4.15 - Acerca da aquisição de malware para todos os cursos.



Fonte: Diogo (2017).

De acordo com os gráficos das Figuras 4.15 e 4.16 a maioria dos entrevistados em todos os cursos nunca adquiriu *malware*. Há também a possibilidade de que alguns entre os entrevistados desconheçam que contraíram algum tipo de software

malicioso. Outra informação importante é o curso onde houve menos smartphones contagiados foi o de Computação.

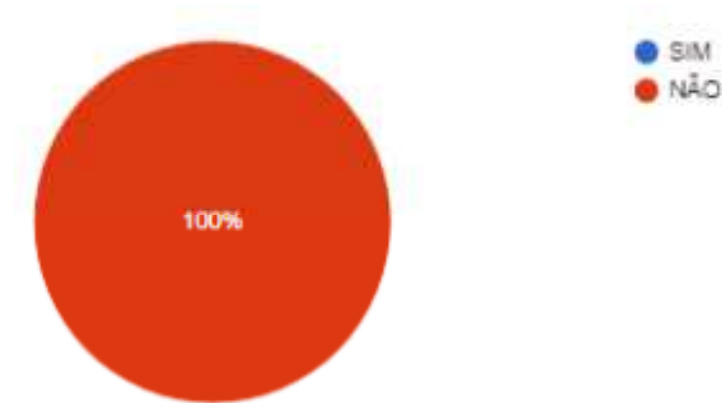
Nona pergunta: "Você já teve sua privacidade invadida através de seu *smartphone*?"

Gráfico 4.16 - Possibilidade da invasão do smartphone por curso.



Fonte: Diogo (2017).

Gráfico 4.17 - Possibilidade da invasão do smartphone para todos os cursos.



Fonte: Diogo (2017).

De acordo com o gráfico da Figura 4.17 e 4.18, 100% de todos os entrevistados em todos os cursos afirmou que nunca teve sua privacidade invadida através dos seus aparelhos. No entanto, existe a possibilidade de que alguns dos *smartphones* dos entrevistados já tenham sido (ou estejam sendo) invadidos.

5 CONSIDERAÇÕES FINAIS

A partir de 2007 houve aumento considerável no desenvolvimento e utilização dos *smartphones* em todo o mundo, desse modo vivemos cada vez mais em um globo em que a tecnologia está ligada diretamente no nosso dia a dia, tornando-se um hábito frenético. Hoje podemos nos conectar à rede mundial praticamente em qualquer lugar utilizando as tecnologias móveis, onde possa existir qualquer espécie de conexão com a internet. Nesse seguimento, a acessibilidade proporcionou um aumento das comunicações sociais através das tecnologias móveis, como as conversas virtuais por intermédio de aplicativos, em razão disso houve um aumento substancial de usuários em tecnologia móveis, da mesma maneira cresceu muito o número de ameaças de ataques a esses dispositivos.

Desde então os cibercriminosos tem se direcionado para as tecnologias móveis especialmente para os sistemas operacionais Android, em decorrência de ser o mais utilizado entre os usuários ocasionando um aumento substancial de *malware*, logo, deve-se ter uma maior consciência e conhecimento entre os usuários sobre segurança, visto que os seus *smartphones* contêm dados pessoais, como fotos, vídeos e senhas, os quais os tornam atraentes para os cibercriminosos que desejam

alcançar benefícios econômicos ou só prejudicar o seu alvo. Diante disso motivou-se esta pesquisa, a qual foi realizada no Campus VII da Universidade Estadual da Paraíba, comparando o nível de proteção tomado pelos discentes dos cursos de Administração, Computação, Física e Matemática com a finalidade de obter informações sobre o nível de segurança empregado em seus Smartphones.

Os dados da pesquisa de campo aplicada através de um questionário revelaram que, no tocante a softwares de proteção o mais utilizado é o antivírus, sobretudo no curso de Computação. No tocante a páginas potencialmente perigosas, a maioria dos entrevistados não acessam, principalmente os discentes dos cursos de Administração e Física; grande parcela em todos os cursos acessam páginas potencialmente perigosas de conteúdo adulto. Poucos alunos de Administração e Física fazem uso de conexões públicas desconhecidas, o inverso ocorre para Computação e Matemática.

Já em redes públicas conhecidas, a maioria dos entrevistados não utiliza nenhuma proteção; os que menos utilizam conexões públicas de qualquer natureza (conhecidas ou não) são de Administração e Física. Todos os cursos acessam sites seguros HTTPS ao navegarem na internet, mas apenas os alunos de Física dão mais preferência a esses sites. Apenas alguns poucos discentes de Computação e Matemática, entre todos os entrevistados, não utilizam bloqueios a informações e recursos, como bloqueios de tela e aplicativos. Todos os discentes entrevistados afirmaram que nunca tiveram seus *smartphones* invadidos. Computação é o curso em que as pessoas mais repetem e compartilham senhas, Física o inverso. Quem mais utiliza caracteres especiais em senhas é Administração e Física. Sobre a combinação de letras maiúsculas e minúsculas em senhas os números da pesquisa são divididos. Apesar de um maior descuido com segurança por parte dos discentes de Computação em relação aos dos demais Cursos, Computação foi o curso que menos entrevistados foram contaminados por *malwares*, o que revela que um conhecimento técnico na área pode ser bastante eficiente na proteção em redes e tecnologias móveis.

Para pesquisas futuras seria interessante fazer um teste de invasão de redes no contexto do Campus VII da UEPB para saber o grau de segurança dos smartphones, onde umas amostras de dispositivos de pessoas voluntárias seriam submetidas, à vista disso poderia aplicar-se essa mesma pesquisa entre os cursos e analisar se os discentes mantêm-se prevenidos quando o assunto é segurança em rede, no seu dispositivo móvel.

ABSTRACT

The use of mobile devices on the network has grown surprisingly in recent years, so that today we can connect to the network practically anywhere and time. However, increased usage has significantly increased attacks on mobile devices, as well as exposure to malware, increasing the vulnerability of its users. This paper presents the results of a research divided into two bias, was initially developed a research on the state of the art and then a field research where students of the courses of Administration, Computing, Physics and Mathematics were interviewed in Campus VII of the UEPB, with the intention of evaluating the level of security care that they use in their smartphones. The research revealed, in general lines, that the students of computation and mathematics presented more neglect than those of Administration and Physics, the latter the most careful. However, computing students were the least contaminated with Malware, suggesting that a higher level of technical knowledge in the area could help prevent pest of the genus.

Keywords: Attack, Security, *Smartphone*, Vulnerability, Campus VII UEPB.

7 REFERÊNCIAS

ALECRIM, Ermeson. **Malwares: o que são e como agem**. Disponível em <<https://www.infowester.com/malwares.php>>. Acessado em 02 dezembro de 2016.

CAPELAS, Bruno. **Brasil chega a 168 milhões de smartphones em uso**. Disponível em <<http://link.estadao.com.br/noticias/gadget,brasil-chega-a-168-milhoes-de-smartphones-em-uso,10000047873>>. Acessado em 05 de dezembro de 2016.

CARDOSO, Pedro. **O que é ransomware**. Disponível em <<http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>>. Acessado em 17 de janeiro de 2017.

CARMONA, Lisandro de Souza. **Evolução do ransomware móvel**. Disponível em <<https://blog.avast.com/pt-br/the-evolution-of-mobile-ransomware-1>>. Acessado em 17 de janeiro de 2017.

COHEN, FRED. **Computer Viruses: Theory and Experiments**. PROCEEDINGS OF THE 7TH NATIONAL COMPUTER SECURITY CONFERENCE, pp. 240 - 263, 1984.

FISZMAN, GABRIELLA. **Wifi grátis: como usar uma rede pública com segurança**. Disponível em <<http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/06/wi-fi-gratis-como-usar-uma-rede-publica-com-seguranca.html>>. Acessado em 30 de janeiro de 2017.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. Antonio Carlos Gil. – 4.ed.- São Paulo: Atlas, 2002.

GARRET, Filipe. **O que é VPN? Saiba tudo sobre a rede virtual**. Disponível em <<http://www.techtudo.com.br/noticias/noticia/2015/11/o-que-e-vpn-saiba-tudo-sobre-rede-virtual-privada.html>>. Acessado em 03 de janeiro de 2017.

INTERNATIONAL DATA CORPORATION. **Smartphone OS Market share**. Disponível em <<http://www.idc.com/prodserv/smartphone-os-market-share.jsp>>. Acessado em 10 de janeiro de 2017.

JORDÃO, Fabio. **Há 7 anos, o primeiro iPhone era anunciado**. Disponível em <<https://www.tecmundo.com.br/iphone/48924-ha-7-anos-o-primeiro-iphone-era-anunciado.htm>>. Acessado em 13 de fevereiro de 2017.

LEITÃO, Glenio marques filho. **Hacker e crackers na internet: as duas faces da moeda** Disponível em <http://www.insite.pro.br/2010/janeiro/hackers_crackers_internet.pdf>. Acessado em 22 de janeiro de 2017.

MALENKOVICH, Serge. **O que é um ataque Man-in-the-Middle**. Disponível em <<https://blog.kaspersky.com.br/what-is-a-man-in-the-middle-attack/462/>>. Acessado em 04 de fevereiro de 2017.

NOVAES, Rafael. **Os malwares que mais fazem vítimas no Brasil e no mundo**. Disponível em <<http://www.psafes.com/blog/os-malwares-mais-fazem-vitimas-no-brasil-no-mundo/>>. Acessado em 17 de janeiro de 2017.

NOVAES, Rafael. **Botnet x Backdoor: o que são e como se prevenir**. Disponível em <<http://www.psafes.com/blog/botnet-x-backdoor-sao-como-prevenir/>>. Acessado em 02 de fevereiro de 2017.

Olhar Digital. **Brasil é o 6º país com maior número de smartphones no mundo**. Disponível em <<https://olhardigital.com.br/noticia/sexta-lugar-em-numero-de-smartphones-brasil-tem-38-8-milhoes-de-aparelhos/46052>>. Acessado em 07 de dezembro de 2016.

POZZEBOM, Rafaela. **O que é vírus de computador**. Disponível em <<https://www.oficinadanet.com.br/post/10977-o-que-e-virus-de-computador>>. Acessado em 05 de janeiro de 2017.

POZZEBOM, Rafaela. **Diferença entre: vírus, spam, spywares, worm, phishing, botnet, rookit**. Disponível em <<https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit>>. Acessado em 31 de janeiro de 2017.

RIBEIRO, Carolina. **Confira dicas para navegar com segurança em redes Wi-Fi públicas**. Disponível em <<http://www.techtudo.com.br/artigos/noticia/2013/02/confira-dicas-para-navegar-com-seguranca-em-redes-wi-fi-publicas.html>>. Acessado em 29 de janeiro de 2017.

RÚBIA, Sandra da silva. **O consumo de smartphone entre jovens de camadas populares.** Disponível em <<http://revistazcultural.pacc.ufrj.br/o-consumo-de-smartphone-entre-jovens-de-camadas-populares/>>. Acessado em 09 de dezembro de 2016.

SIMÕES, Helton Gomes. **Smartphone passa pc e vira aparelho nº 1 para acessar internet no Brasil.** Disponível em <<http://g1.globo.com/tecnologia/noticia/2016/04/smartphone-passa-pc-e-vira-aparelho-n-1-para-acessar-internet-no-brasil.html>>. Acessado em 09 de dezembro de 2016.

SZYMANSKI, Thiago. **Os 4 ataques hackers mais comuns da web.** Disponível em <<https://www.tecmundo.com.br/ataque-hacker/19600-os-4-ataques-hackers-mais-comuns-da-web.htm>>. Acessado em 28 de janeiro de 2017.

SOROKANICH, Robert. **IBM Simon o smartphone original, completou 20 anos de vida.** Disponível em <<http://gizmodo.uol.com.br/20-anos-ibm-simon/>>. Acessado em 13 de fevereiro de 2017.

TINOCO, Celso. **Vantagens e Desvantagens das VPNs.** Disponível em <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2015_2/Seguranca/conteudo/Redes-Privadas-Virtuais-VPN/Vantagens-e-Desvantagens.html>. Acessado em 05 de janeiro de 2017.

VOLTONI, Ramon. **Conheça o primeiro smartphone da história.** Disponível em <<https://www.tecmundo.com.br/celular/59888-conheca-primeiro-smartphone-historia-galerias.htm>>. Acessado em 13 de fevereiro de 2017.