INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

ANDERSON BEZERRA DA SILVA

ÉTICA NA COMPUTAÇÃO: A UTILIZAÇÃO DE SOFTWARE NO SETOR PÚBLICO NAS CIDADES DO ALTO OESTE POTIGUAR

Pau dos Ferros – RN

2019

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

ANDERSON BEZERRA DA SILVA

ÉTICA NA COMPUTAÇÃO: A UTILIZAÇÃO DE SOFTWARE NO SETOR PÚBLICO NAS CIDADES DO ALTO OESTE POTIGUAR

Trabalho de Conclusão de Curso apresentado ao Curso Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de analista de sistemas.

Orientador: Francisco Sergio de Almeida Neto, M.SC.

Pau dos Ferros – RN

2019

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

ANDERSON BEZERRA DA SILVA

ÉTICA NA COMPUTAÇÃO: A UTILIZAÇÃO DE SOFTWARE NO SETOR PÚBLICO NAS CIDADES DO ALTO OESTE POTIGUAR

Trabalho de Conclusão de Curso apresentado ao Curso Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de analista de sistemas.

Trabalho de Conclusão de Curso apresentado e aprovado em ___/___/____, pela seguinte Banca Examinadora:

_____

Francisco Sergio de Almeida Neto - Presidente
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Aluísio Igor Rêgo Fontes, Membro da banca - Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Nome do Prof convidado, Membro da banca - Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Dedico esse trabalho a minha família e amigos que me apoiaram e incentivaram para em toda minha jornada até esse momento em minha vida.

Ao meu professor e amigo Sergio que muito me apoiou, proporcionando toda a ajuda necessária para que fosse possível terminar esse trabalho.

AGRADECIMENTO

A Deus por me proporcionar saúde e energia para poder concluir esse trabalho.

Aos meus professores Francisco Sergio de Almeida Neto e Aluísio Igor Rêgo Fontes, que me apoiaram e me deram todo o suporte para realização desse projeto.

Aos meus pais e amigos pelo o apoio e o incentivo para poder chegar ao final dessa etapa de minha vida.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"*Pois o senhor é quem dá sabedoria; de sua boca procedem o conhecimento e o discernimento.*"

Provérbios 2:6.

RESUMO

Este Trabalho de Conclusão de Curso (TCC) tem por objetivo apresentar o comportamento ético das instituições públicas das cidades do alto oeste potiguar e de seus funcionários na utilização do computador e seus softwares; expondo dados sobre a pirataria de software e seu impacto negativo para a economia; apresentando os tipos de softwares utilizados nessas instituições; evidenciando os problemas de segurança enfrentados nestas instituições pelos funcionários, além de expor as vulnerabilidades de sistemas públicos utilizados por esses funcionários. Assim, o presente estudo tem caráter qualitativo com o método de estudo de caso onde se foi coletado e analisado as informações dos funcionários destas instituições, traçando um perfil sobre o comportamento ético dos mesmos no ambiente de trabalho durante a utilização do computador. O resultado dos dados coletados com 17 funcionários aponta que a maioria desconhece manuais de ética no trabalho e na computação, com comportamentos éticos no trabalho questionáveis em relação a utilização de suas ferramentas de serviço.

Palavras-chave: Ética no trabalho. Pirataria de software. Segurança de dados públicos. Análise de vulnerabilidade.

ABSTRACT

This Term paper aims to present the ethical behavior of public institutions of the *alto oeste potiguar* (region located west of the state of Rio Grande do Norte, Brazil) and of its employees in the use of the computer and its software; exposing data about software piracy and its negative impact on the economy; presenting the types of software used in these institutions; highlighting the issues with security faced in these institutions by the employees, besides exposing the vulnerability of public systems used by these employees. Thus, the present study has a qualitative character with the case study method where the information of the employees of these institutions were collected and analyzed, tracing a profile about the ethical behavior of said employees in the workplace during the use of the computer. The result of the data collected with 17 employees indicates that the majority are unaware of ethics manuals on work and computation, with questionable ethical behavior at work in relation to the use of their service tools.

Keywords: Ethic in the workplace. Software piracy. Security of public data, analysis of vulnerability.

Lista de ilustrações

LISTA DE TABELA

LISTA DE ABREVIATURAS E SIGLAS

TI	Tecnologia da Informação
ABES	Associação Brasileira de Empresas de Software
ENIAC	Eletronic Numeric Integrator Analyser and Computer
ACM	Association for Computing Machinery
BSA	Business Software Alliance
E-GOV	Governo Eletrônico
SSL	Secure Sockets Layer
TLS	Transport Layer Security
ARP	Adrress Resolution Protocol
OSI	Open System Interconnection
CSRF	Cross-Site Request Forgery
MITM	Man In The Middle
DOS	Denial Of Service

Sumário

1 INTRODUÇÃO

A sociedade atual se desenvolveu bastante em relação a tecnologia, com máquinas modernas que facilitam a vida das pessoas, desde simples atividades como lavar a roupa até processos mais complexos como realizar o envio de uma informação através do correio eletrônico. Com esse avanço tecnológico, uma das áreas que mais avançou foi a de Tecnologia da Informação (TI) com um crescimento nos estudos da computação e a modernização dos computadores e seus softwares, que tiveram um progresso no mercado nos últimos anos com ferramentas livres e pagas desenvolvidas para melhorar a vida dos cidadãos. (FILHO, 2007).

Entretanto, com a evolução tecnológica, também surgiram alguns problemas relacionados a sua utilização, em que usuários procuram através da tecnologia obter benefícios para si de maneira ilícita, roubando informações confidenciais, copiando e vendendo produtos que pertencem intelectualmente a outras pessoas e desrespeitando o direito de propriedade do criador do produto.

Essas pessoas desrespeitam o conceito de ética, infringindo a privacidade de outros cidadãos e prejudicando a economia do país por meio dos crimes eletrônicos. A pirataria contribui negativamente para a economia de um país, pois sua realização faz com que o governo perda na arrecadação dos impostos referentes ao produto, como mostra matéria da revista exame no ano de 2018 (KOJIKOVSKI, 2018).

Por mais que esses crimes sejam frequentes em nossa sociedade, existem maneiras de serem prevenidos e combatidos, através de ferramentas e como softwares de antivírus, *firewall* e sistemas de monitoramento de rede. Além disso, o usuário também deve ter um comportamento mais cuidadoso na utilização da internet, evitando entrar em sites de origem duvidosa e adquirir softwares de fornecedores sem credibilidade ou piratas. Estes atos auxiliam na proteção de dados (ARAUJO, 2003).

Devido ao fato desses crimes ocorrerem na sociedade de hoje, instituições públicas devem ter bastante cuidado com seus dados, pois as

mesmas possuem informações de importância pública. Para isso além de investimento alto na segurança dos dados, deve-se ter um treinamento adequado para seus funcionários, que precisam sempre apresentar uma postura ética exemplar, obedecendo aos protocolos e manuais da instituição a qual representam (THOENIG, 2000).

Diante disso, algumas questões importantes são levantadas: como se comportam no que se refere à ética computacional, os funcionários públicos responsáveis pela utilização de softwares para desempenhar seu trabalho? Esses profissionais utilizam somente softwares licenciados ou também utilizam softwares sem licença? Eles conhecem as leis que regem a propriedade intelectual no Brasil? O que os mesmos fazem para proteger os dados que tem armazenados?

Nesse contexto, o objetivo desse estudo é apresentar uma análise sobre o comportamento ético de funcionários de instituições da rede pública na utilização de softwares e sistemas públicos, além de analisar a vulnerabilidade dos mesmos. A unidade de análise serão instituições públicas (escolas, prefeituras e suas secretarias) da região do Alto Oeste potiguar e os sujeitos da pesquisa serão funcionários públicos, como por exemplo digitadores e secretários que trabalham diretamente com o computador e seus softwares nestas respectivas instituições.

1.1 OBJETIVO GERAL

Analisar os sistemas através de um scanner de sistemas web para identificar as vulnerabilidades do mesmo. Analisar o comportamento ético dos funcionários que trabalham diretamente com essas ferramentas em instituições públicas de municípios da região do Alto Oeste potiguar.

1.2 OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral, foram definidos os seguintes objetivos específicos:

- Apresentar as leis vigentes no país em relação a proteção da propriedade intelectual relacionadas ao software;
- Identificar os tipos de softwares utilizados nas instituições públicas;
- Analisar o comportamento ético na computação dos funcionários públicos;
- Realizar uma análise de vulnerabilidade em sistemas do governo.

1.3 JUSTIFICATIVA

A pirataria de software é um problema comum na sociedade. No Brasil este crime é bastante comum. Segundo o Portal MS (2009), o Brasil possuía 58% dos programas pirateados, ficando à frente da Colômbia que tinha 56%. A mesma pesquisa constatou que os produtores de software tiveram um prejuízo de mais de 1,6 bilhões em virtude da pirataria no Brasil. A Associação Brasileira das Empresas de Software (ABES, 2009) afirma que a pirataria é uma questão cultural que se firmou no país.

Por mais que existam alguns estudos sobre a pirataria de software, os estudos sobre a ética relacionada a esse ato de roubo de propriedade intelectual ainda são muito escassos, sendo menor ainda seu estudo em empresas do setor público (MASIERO, 2000).

Os órgãos públicos devem exercer uma conduta ilibada e qualquer tipo de conduta antiética relacionada à tecnologia deve ser analisada e discutida para que estas instituições possam exercer o melhor trabalho possível para seus usuários. A segurança dos dados na rede é algo importante para seus usuários, no entanto esses dados ficam vulneráveis quando os usuários utilizam softwares de origem duvidosa. Estas ferramentas muitas vezes vêm infectadas com algum tipo de vírus que enfraquece a segurança do computador, tornando-o mais fácil de ser invadido por hackers, que podem roubar as informações pessoais do usuário e utiliza-las como bem entender (MASIERO, 2000).

Além disso, o roubo de propriedade intelectual em relação ao software é considerado crime. No Brasil existe uma lei criada no ano de 1998 de número 9609, em que penaliza os infratores desse ato com multa ou pena de reclusão, dependendo da gravidade da infração (Lei Nº 9609/98). Esta lei foi criada como uma maneira do governo proteger juridicamente os direitos dos criadores e das empresas que comercializam esses produtos (ABES, 2018).

Dessa forma, este trabalho se justifica pelo fato de investigar um tema pouco estudado na academia, que é a ética na computação, especialmente de entidades públicas, e pelo fato de poder contribuir com as comunidades envolvidas, uma vez que poderá mostrar possíveis falhas ou problemas que possam estar ocorrendo por parte das entidades públicas e de seus agentes.

2 REFERENCIAL TEÓRICO

O século XX foi marcado com grandes mudanças pelo mundo e com um desenvolvimento tecnológico nunca visto na história. Estas mudanças trouxeram impacto social e econômico em todo o mundo. Neste período teve o surgimento de um dos maiores inventos da história, o computador, ferramenta tecnológica que evoluiu, e hoje em dia é indispensável à sociedade moderna. (FILHO, 2007).

No século XX o cenário de conflitos militares incentivou a realização de pesquisas e a computação foi o foco que mereceu mais atenção. O objetivo do desenvolvimento do computador era quase exclusivamente de uso militar no intermeio entre as duas grandes guerras mundiais (CÔRTES, 2003).

Em decorrência desses conflitos surgiu em 1920 na Alemanha a máquina Enigma, que codificava mensagens. Essas máquinas se aperfeiçoaram, o que levou os rivais da Alemanha criarem em 1943 o Colossos, uma máquina projetada para decifrar os códigos alemães. (CÔRTES, 2003). Com o desenvolvimento dessas máquinas, outras surgiram, como o *Eletronic Numeric Integrator Analyser and Computer* (ENIAC), criado em 1946 para realização dos cálculos balísticos, uma máquina gigante que chegava a consumir energia suficiente para abastecer uma pequena cidade (CÔRTES, 2007).

O computador se desenvolveu, e com seu avanço surgiu a internet. segundo Cantú (2003, p.04), “a Internet é a rede mundial de computadores que interliga milhões de dispositivos computacionais espalhados ao redor do mundo”. Um conceito simples usado para explicar a internet para o povo.

Com esse avanço na computação, o software também se desenvolveu. Roger S. Pressman procurou defini-lo como:

> Software é: (1) instruções que, quando executadas, produzem a função e o desempenho desejado; (2) estruturas de dados que possibilitam que os programas manipulem adequadamente a informação; e (3) documentos que descrevem a operação e o uso dos programas (Pressman, 2007, p. 28).

Pressman apresenta o software de uma maneira mais sucinta, para que o leitor tenha de imediato a ideia do que é um software, apresentando as funções que o mesmo desempenha.

A natureza do software e sua criação é o próximo passo a ser compreendido. Para entender o software Pressman (2007, p.31) define o processo de criação como:

> Os componentes de Software são criados por meio de uma série de conversões que mapeiam as exigências do cliente para código executável em máquina. Um modelo das exigências é convertido em um projeto. O projeto de software é convertido numa forma de linguagem que especifica a estrutura de dados do software, os atributos procedimentais e os requisitos relacionados. A forma de linguagem é processada por um tradutor que a converte em instruções executáveis em máquina.

Em outras palavras, Pressman (2007) tenta dizer que o software é criado a partir de uma série de cálculos e das necessidades dos usuários.

O software sendo uma ferramenta que é desenvolvida para facilitar a vida das pessoas é indispensável para empresas, que utilizam estas ferramentas tecnológicas para acelerar e aumentar a eficiência do trabalho de seus funcionários (ENGHOLM JR, 2010).

Os softwares estão presentes em muitas instituições públicas como escolas, prefeituras, hospitais, entre outras. Estas instituições utilizam dessas ferramentas para melhorar a eficiência de seu trabalho. Em prefeituras, é comum

utilizarem ferramentas como planilhas eletrônicas e editores de texto para digitação de documentos.

Instituições públicas e privadas que utilizam softwares e a internet devem sempre ter uma conduta correta em sua utilização, sempre tendo um comportamento ético para com os outros, pois uma conduta antiética pode trazer problemas para as mesmas, sendo em alguns casos puníveis judicialmente, principalmente em órgãos públicos onde os funcionários devem zelar pelo comportamento correto e ilibado, para não manchar a imagem da instituição a qual representam.

2.1 ÉTICA NA COMPUTAÇÃO E PIRATARIA DE SOFTWARE

Segundo o minidicionário Aurélio (FERREIRA, 2001, p.300), ética pode ser definida como: "**1**. Estudo dos juízos de apreciação referentes à conduta humana, do ponto de vista do bem e do mal. **2**. Conjunto de normas e princípios que norteiam a boa conduta do ser humano". Como mostrado na definição do Aurélio, a ética é o estudo da sociedade e do comportamento humano nela.

De acordo com Masiero (2000), a ética aplicada é aquela que se preocupa com os conceitos éticos do dia-a-dia, e a ética profissional é o mesmo conceito aplicado no exercício da profissão. A ética aplicada tem três teorias muito importantes que são a ética deontológica, o relativismo e o utilitarismo. O utilitarismo será a teoria utilizada para realização da pesquisa neste estudo, que tem por objetivo estudar as consequências de uma ação e assim determinar sua moralidade. Este princípio é resumido como determinar a ação que traga mais benefício para o praticante da mesma.

A ética na computação abrange o comportamento dos profissionais da área e os valores que os guiam durante os seus dias de atividade no trabalho. Segundo Masiero (2000, p.26 apud MOOR, 1985),

> outros autores procuram definir ética na computação como uma ética especial, apontando como razões básicas a recenticidade dos computadores, seu impacto na sociedade e a flexibilidade lógica que permite os computadores serem programados para executar um sem-número de tarefas.

Para o autor, como os computadores são máquinas presentes a pouco tempo na sociedade, a ética aplicada a computação é tida como especial, por ser algo recente, que deve ser mais estudada.

Por mais que a ética na computação seja algo recente, uma organização criou e adotou um código próprio a ser seguido na computação, a ACM (*Association for Computing Machinery*) tem em seu código dedicar-se grande parte de suas regras aos usuários e a sociedade (MASIERO, 2000).

Dentre as normas instituídas pela ACM em 1992 e reformuladas em 2018 que devem ser seguidas por seus membros, destaca-se:

Tabela 1 - Normas da ACM

Imperativos de moral geral.	• Contribuir para a sociedade e bem-estar humano. • Evitar prejudicar os outros. • Ser honesto e confiável. • Ser justo e tomar ações para não discriminar. • Honrar direitos de propriedade incluindo copyrights e patentes. • Dar o devido credito por propriedade intelectual. • Respeitar a privacidade alheia
Responsabilidades Profissionais Mais Específicas.	• Esforce-se para alcançar a mais alta qualidade, eficácia e dignidade, tanto no processo e produtos do trabalho profissional. • Adquirir e manter competência profissional. • Conhecer e respeitar as leis existentes relativos ao trabalho profissional. • Aceitar e fornecer avaliação profissional adequada. • Dê avaliação abrangente e completas de sistemas de computadores e seus impactos, incluindo a análise de possíveis riscos. • Honrar acordos e responsabilidade atribuídos (Contratos). • Melhorar a compreensão pública da computação e suas consequências. • Usar recursos de computação de acesso e de comunicação somente quando autorizado a fazê-lo.

Imperativos da Liderança Organizacional	• Imperativos da liderança organizacional. Articular responsabilidades sociais dos membros de uma unidade organizacional e incentivar a plena aceitação dessas responsabilidades. • Gerenciar pessoas e recursos para projetar e construir sistemas de informação que melhorem a qualidade de vida no trabalho. • Reconhecer e apoiar os usos apropriados e autorizados de recursos de computação e comunicação de uma organização. • Certifique-se de que os usuários e aqueles que serão afetados por um sistema, tenham suas necessidades claramente articuladas durante a avaliação e design de requisitos; mais tarde, o sistema deve ser validado para satisfazer as exigências. • Articular e apoiar políticas, que protegem a dignidade de usuários e outras pessoas afetadas por um sistema de computação. • Criar oportunidades para membros da organização para aprender os princípios e limitações dos sistemas de computador.
Obediência ao Código	• Respeitar e promover os princípios deste código. • Tratar qualquer violação a este código como incoerentes com a afiliação à ACM.

Fonte: ACM, 2018.

No mundo em que vivemos hoje, as empresas e os seus profissionais da computação devem ter condutas éticas com seus clientes, podendo se dizer que esse é o diferencial entre o sucesso e o fracasso. O comportamento ético duvidoso mancha a imagem da empresa e a leva a perder clientes e fornecedores, fazendo com que a mesma tenha cada vez menos relevância no mercado (PALETTA, 2004).

Segundo Schwartz (2002), a ética deve ser regida por seis princípios básicos: confiabilidade, respeito, responsabilidade, justiça, cuidado e exercício da cidadania obedecendo à lei vigente.

Uma empresa deve procurar obedecer a estes princípios básicos, pois o não cumprimento dessas funções mancha a imagem da instituição. Muitos atos

feitos na rede podem ser considerados como uma conduta antiética, como é o caso dos *hackers*, que realizam invasões em sistemas com objetivos criminosos como roubo de dados e da propriedade intelectual de outras pessoas, entre outros casos, ou simplesmente por prazer, como um teste de capacidade (MASIERO, 2000).

Com base em MASIERO (2000) para conseguir realizar esses atos os *hackers* utilizam de programas, como vírus que tem a capacidade de auto copiar-se podendo hospedar outros programas. Além dos vírus, existem outros programas que facilitam a invasão por parte de pessoas mal-intencionadas, conforme se observa no quadro abaixo.

Tabela 2 - Programas que facilitam a invasão dos hackers

Vírus	Costumam causar danos ao sistema infectado, como corrupção de arquivos e discos, também podem causar perturbações, diminuindo a velocidade de execução do equipamento. O vírus se espalha de diversas maneiras, por downloads na internet, disquetes e discos infectados que contém jogos e softwares infectados, entre outras maneiras. Para combater esse problema existem antivírus que protegem o computador e costumam remover e restaurar a máquina infectada.
Cavalo de Tróia	Esses programas se escondem mascarados como arquivos ou softwares legítimos. Depois de baixados e instalados, esses programas alteram o computador e realizam atividades maliciosas sem o conhecimento ou consentimento da vítima.
Farejadores ou *Sniffers*	programas responsáveis por monitorar o tráfego na rede, capturam as informações que estão navegando e buscam sequências de identificadores de contas e senhas.

Fonte: (Kaspersky, 2018. Avast, 2018)

Estes programas são ferramentas que diminuem a proteção da máquina do usuário, tornando-a mais vulnerável. Muitas vezes estes programas chegam ao computador quando o usuário de maneira ilícita utilizar de softwares privados, realizando *downloads* de programas duvidosos, burlando o direito da propriedade intelectual que o criador do software tem.

A propriedade intelectual e sua proteção tem como objetivo incentivar o desenvolvimento de novos dispositivos e de novos processos, além da criação de novas obras artísticas, tudo como um meio de melhorar o cotidiano na sociedade. Isso é feito dando ao criador da obra, o poder sobre sua criação, detendo o direito de explorar comercialmente o resultado de sua invenção. Caso qualquer um pudesse copiar e vender o fruto do trabalho de outro, a vontade de investir seria pequena e a sociedade perderia. (MASIERO, 2000).

O roubo de conteúdo intelectual de outra pessoa é um dos atos mais comuns praticados na internet, onde usuários obtêm de maneira ilegal cópias de algo sem prévio pagamento. Um desses exemplos é quando o usuário faz *downloads* de softwares ilegalmente, praticando o crime de piratear software (ORRICO JR, 2004; PALETTA, 2004).

O crime da pirataria é caracterizado pela distribuição, cópia ou venda de qualquer tipo de mercadoria sem que os envolvidos paguem os direitos autorais que abrangem a sua criação, imagem e outras características inerentes a ela, incluindo o próprio direito ao uso de suas funções (ORRICO JR,2004).

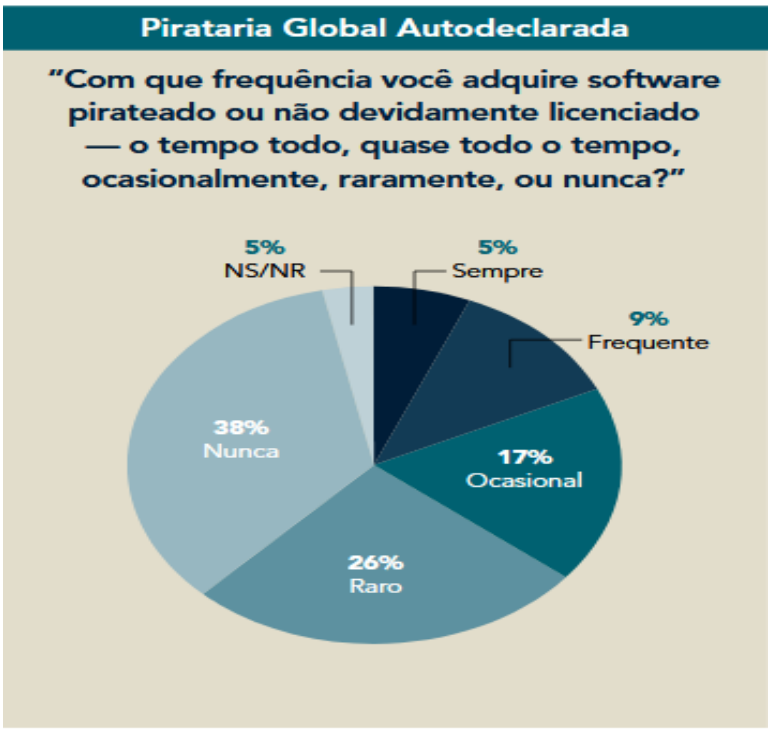
A evolução da tecnologia acarretou uma expansão da internet pelo mundo. A facilidade de se obter informação contribuiu para que o número de produtos digitais copiados sem autorização do proprietário dos direitos autorais aumentasse. Entre esses produtos estão softwares, livros, arquivos, músicas e filmes, o que tem sido denominado de pirataria digital (PEITZ; WAELBROECK, 2006).

Esta comercialização de softwares piratas traz inúmeros prejuízos para a indústria de criação dos mesmos, que tendem a dedicar menos recursos à pesquisa ao desenvolvimento de novos produtos (PHAU; NG; 2009). Esta prática também aumenta o preço dos softwares originais, forçando os consumidores que compram os produtos legalizados a pagarem mais caro. Isto ocorre para que os produtores possam cobrir o prejuízo daqueles que pirateiam (PHAU; NG, 2009; HINDUJA, 2003). A pirataria de software também traz prejuízo ao governo que perde na arrecadação de impostos, além de contribui com o crime organizado,

que inclui tráfico de drogas, armas, pessoas e lavagem de dinheiro (RUTTER; BRYCE, 2008).

Segundo um estudo global realizado sobre a pirataria de software pela BSA (*Business Software Alliance*) em 2011, 57% dos usuários de computador admitem piratear software. Nessa pesquisa se incluem 31% que sempre pirateia ou que ocasionalmente cometem esse crime, e por fim 26% admitem que raramente cometem esse ato.

Figura 1 - Gráficos de frequência de pirataria de software



Fonte: BSA (2012)

Seguindo os dados apresentados no gráfico acima, pode-se notar que o número de pessoas que admitem piratear software é muito superior (57% dos pesquisados) aos que relatam nunca ter pirateado, (38% dos entrevistados) (BSA, 2012).

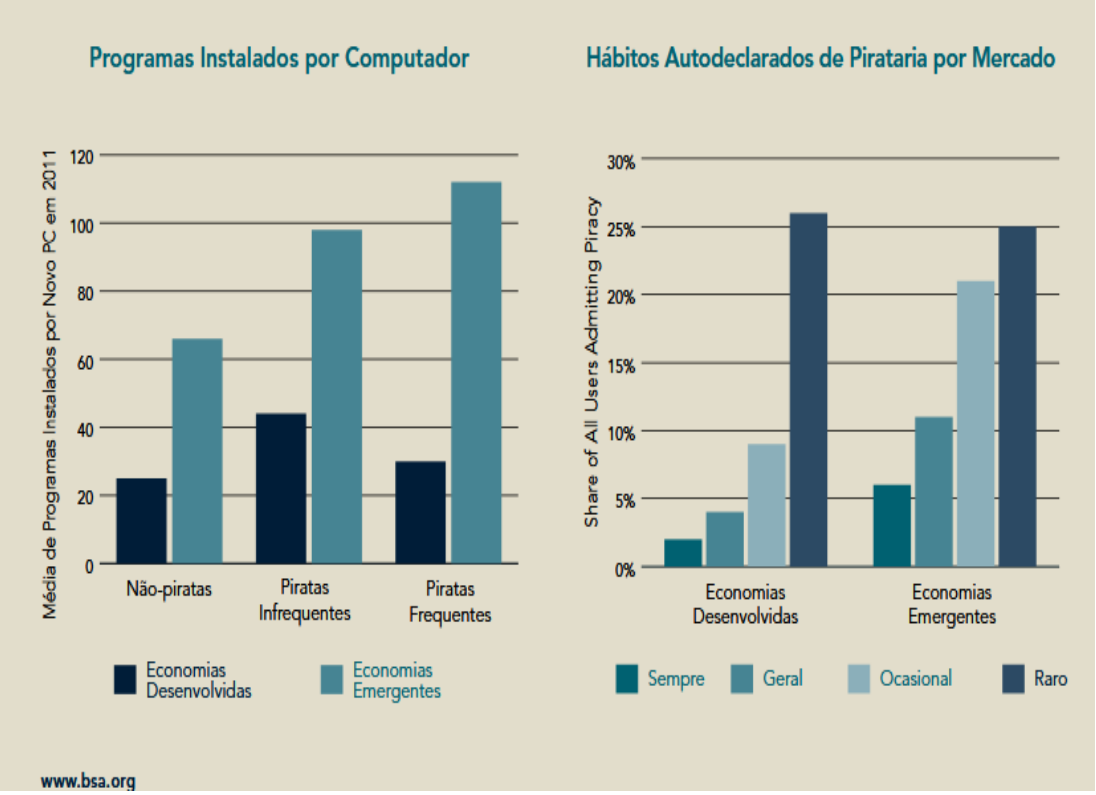
A mesma pesquisa constatou que o valor comercial de software pirateado saltou de US$ 58,8 bilhões em 2010 para US$ 63,4 bilhões em 2011, um recorde

que foi ocasionado pelo aumento na venda de computadores em economias emergentes, onde se encontram as maiores taxas de pirataria.

Essas economias tomaram 56% das vendas de computadores em 2011, isso representa mais da metade da massa de computadores em utilização pelo mundo (BSA, 2012).

Como apresentado no estudo realizado pela BSA em 2011, o número de softwares pirateados em economias emergentes é muito superior aos de economias desenvolvidas, conforme o gráfico abaixo.

Figura 2 - Gráfico de frequência de pirataria nos países



Fonte: BSA (2012)

Podem-se observar na figura que economias emergentes possuem produtos piratas com mais frequência que economias já desenvolvidas, o que demostrar que a pirataria é um reflexo da condição do país e de seu povo, que nações mais ricas com uma população mais bem estruturada procuram com

mais frequência produtos de maneira legal, do que países onde a população é mais pobre.

Segundo a mesma pesquisa realizada pela BSA, as 20 principais economias em valor de software pirateado no ano de 2011, constatou que a maior taxa de pirataria está em economias emergentes, como: Indonésia, Venezuela e China e os que apresentaram a menor taxa de pirataria são EUA, Japão e Austrália, as três últimas todas economias desenvolvidas. Estes dados confirmam as afirmações apresentadas pela pesquisa.

O Brasil como uma economia emergente apresenta uma taxa de 53% em valor de softwares de computador pirateados. Uma taxa considerada alta se comparada com os EUA que tem apenas 19%, a menor taxa em todo o mundo.

Com um número tão elevado, parece que no Brasil não existe leis que protejam a propriedade intelectual do criador do software. No entanto, no Brasil a pirataria de software é considerada crime e possui uma legislação com leis sérias para combater este problema.

2.2 LEGISLAÇÃO BRASILEIRA - LEI Nº 9609/98

Em 19 de fevereiro de 1998, a lei de número 9609 foi criada com o objetivo de combater a pirataria digital. A lei tem o objetivo de preservar os direitos autorais dos autores, assegurando a tutela dos direitos do programa por um prazo de 50 anos.

A pena em caso de uso sem fins comerciais, para esse tipo de crime é a detenção de seis meses a dois anos ou multa (Lei Nº 9609/98). Já se o infrator usar a pirataria para fins comerciais, a pena é a descrita no Art. 12 parágrafo 1º, apresentado a seguir:

> § 1º se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente, o infrator terá pena de reclusão de um a quatro anos e multa (Lei Nº 9609/98).

Portanto, a lei em questão diferencia o crime cometido sem fins lucrativos daquele cometido para benefício comercial do infrator, sendo este tipo o que apresenta uma pena mais grave.

Vale ressaltar que os crimes previstos na legislação somente se procedem mediante queixa, exceto em alguns casos:

> § 3º I - Quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público. II - Quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. (Lei Nº 9609/98).

Com base na lei, o infrator desse crime pode ser punido sem a queixa se trouxer prejuízo para a rede pública.

2.3 O SOFTWARE NO SETOR PÚBLICO

O software está presente no setor público, em instituições governamentais, oferecendo um meio tecnológico para aumentar a eficiência dos serviços que são prestados para a sociedade. O governo procura utilizar de softwares livres para o serviço público.

Segundo Richard Stallman software livre é aquele que permite ao usuário executar, copiar, distribuir e aperfeiçoar um programa de computador (Secretaria de informática, 2007).

Segundo o guia livre (2007), as principais razões para que as instituições públicas estabelecessem programas de migração para o software livre foram: a necessidade de adoção de padrões abertos para o Governo Eletrônico (e-Gov); o nível de segurança proporcionado pelo software livre; independência tecnológica; e independência de fornecedor único. Esse e outros motivos foram importantes para que o governo começasse a aderir ao software livre.

Segundo Borges (2014) as principais razões que levaram ao governo instituir estes softwares como padrão em suas instalações:

> Proteção contra coerção ou ameaças por parte de entidades corporativas que desenvolvem e controlam softwares do qual os

> governos dependem; maior controle de um software do qual depende a segurança nacional; maior potencial econômico para companhias internas propiciando o desenvolvimento nacional, melhoria e suporte ao software sem dependência de sociedades com corporações fora do país; redução de litígios e pressões internacionais acerca de questões relacionadas a “pirataria”; redução de custos que facilita a obtenção de financiamento, além do fato de que estes podem ser distribuídos (BORGES, 2014, p.11).

O governo procura definir o software livre como um direcionamento estratégico para as políticas públicas, visando garantir o desenvolvimento nacional.

2.4 GOVERNO ELETRÔNICO

Governo eletrônico ou e-gov, representa a gestão estatal informatizada pela tecnologia da informação, com o objetivo de disponibilizar um melhor desempenho das organizações estatais e integrar o cidadão no destino das coisas públicas. (PRADO; SOUZA, 2014).

Cunha (2010) procurou definir o governo eletrônico como algo maior que um governo informatizado:

> “trata-se do uso da tecnologia da informação e comunicação para se construir um governo aberto e ágil, ampliar a cidadania, aumentar a transparência da gestão e a participação dos cidadãos na fiscalização do poder público, democratizar o acesso aos serviços de informações na internet e aumentar a eficiência dos serviços públicos” (p.74).

Como defendido pelos autores a tecnologia da informação e comunicação (TIC), são fundamentais para a administração pública, permitindo uma melhoria na eficiência das ações do governo.

No Brasil o Governo eletrônico se comporta conivente com a ideia defendida pelos autores. A política do e-gov brasileiro “segue um conjunto de diretrizes baseado em três ideias fundamentais: participação cidadã; melhoria do gerenciamento interno do Estado; e integração com parceiros e fornecedores” (GOVERNO DIGITAL, 2017).

Quando se utiliza a internet e softwares de computação, o usuário está sujeito a roubo de informações, e óbvio que para empresas no setor público não seria diferente.

Para tentar evitar o roubo de informações no setor público é preciso uma política de tecnologia da informação com profissionais treinados e capacitados para combater invasões de dados (FERNANDES, 2018).

Segundo Fernandes (2018), entre os procedimentos adotados para a segurança da informação é recomendado seguir alguns procedimentos, conforme mostrado no quadro abaixo:

Tabela 3 - Processos para proteção dos dados

Procedimentos	Descrição
Prevenção	Investindo em softwares que dificultem a invasão de *hackers.*
Detecção	Investindo em dispositivos de detecção, adotando recursos de ti como antivírus, *firewall* e sistemas de monitoramento de rede, com o objetivo de neutralizar invasões.
Recuperação	Para que possa recuperar os dados, essa medida minimiza os efeitos da violação do banco de dados, senhas e unidades de armazenamento. Quanto mais rápido reaver as informações, menor é o impacto da invasão.
Controle de Acesso	Limitando o acesso dos funcionários a sistemas e locais onde ficam os equipamentos de TI, para evitar incidentes de segurança da informação.

Fonte: FERNANDES, 2019.

No Brasil existem empresas públicas responsáveis por manter a informação de muitos brasileiros segura. O Serpro é a empresa pública que mantém a segurança dos dados da Receita Federal, Banco do Brasil, Tesouro Nacional, Ministério da Fazenda, entre outros (SERPRO, 2018). Outro órgão responsável pela segurança de dados é a Dataprev, que faz a segurança dos

dados de todos os contemplados no INSS (DATAPREV, 2018; FERNADES, 2018).

Existem muitos dados sob responsabilidade do governo, por isso o investimento em segurança sempre deve ser alto, procurando contar com melhores profissionais, equipamentos e softwares para combater possíveis ataques e roubos de informações.

2.5 ROUBO DE INFORMAÇÕES

Todo usuário que utiliza internet está sujeito à invasão e roubo de informações em que *hacker* utilizam de ferramentas para invadir sistemas web ou a rede do usuário e com isso roubar informações importantes da vítima. Eles podem fazer isso através de um *Sniffer* que são softwares usados para monitorar e analisar o tráfego de rede, para detectar problemas e manter um fluxo eficiente (Avast, 2018), existe um programa bastante usado para isso o *Wireshark*.

O *Wireshark* analisa os protocolos de rede permitindo ao usuário ver o que acontece em sua rede em nível microscópico (*Wireshark*, 2019). Através do mesmo é possível controlar o tráfego da rede e saber tudo que entra e sai da máquina. Podendo ser usada para depurar implementações de protocolos, examinar os problemas de segurança, entre outras funções. No entanto, essa ferramenta tem a desvantagem de ser usada por *hackers* para roubarem informações. É preciso dizer que esta ferramenta não funciona em todos os sites, principalmente os que utilizam o protocolo “https://”.

Os protocolos https que significa protocolo de transferência de hipertexto seguro, visa fornecer uma conexão segura entre o navegador e um serviço na internet. Sendo uma extensão segura do protocolo http, os sites que configuram um certificado SSL/TLS podem utilizar o protocolo https. O *Secure Sockets Layer* (SSL) permite uma comunicação segura entre um site e um navegador, já o *Transport Layer Security* (TLS), certifica a proteção de dados de maneira semelhante ao SSL.

Outro método utilizado por hackers para detectar falhas em sistemas web e com isso poder invadir esses sistemas é tirar vantagens deles para si é através

de scanners de sistemas web. O acunetix é um programa bastante usado para isso, este programa realiza um scanner no sistema web, com isso identificando suas vulnerabilidades e como elas podem ser resolvidas.

3 METODOLOGIA

Metodologia científica é um conjunto de técnicas e processos utilizados para resolver problemas de uma maneira sistemática (RODRIGUES, 2007). Sendo assim este estudo teve como objetivo analisar o comportamento ético dos funcionários públicos quando fazem uso do computador e se utilizam dessas ferramentas para práticas ilegais, além de analisar as vulnerabilidades encontradas em sistemas web que os mesmos utilizam. Para isso foi realizada uma pesquisa de caráter qualitativo, para se ter uma ideia de como esses funcionários se comportam no ambiente de trabalho e se procuram ter uma atitude ética no desempenho de suas funções. No caso desta pesquisa, os sujeitos foram funcionários de instituições públicas municipais do Alto Oeste Potiguar que trabalham diretamente com o computador e os sistemas analisados foram sistemas do governo eletrônico que os mesmos costumam utilizar no trabalho. Do ponto de vista de seus objetivos, a pesquisa se caracteriza como descritiva, propondo-se a levantar os dados, analisá-los e interpretá-los. (BARROS; LEHFELD, 2017).

Referente ao procedimento técnico, foi utilizado o método de estudo de caso que “consiste em coletar e analisar informações sobre determinado indivíduo, uma família, um grupo ou uma comunidade, a fim de estudar aspectos variados de sua vida de acordo com o assunto da pesquisa” (PRODANOV; FREITAS, 2013, p.60). Segundo YIN (2001) para realização de um estudo de caso pode ser utilizado levantamento, análise de informações de um arquivo, experimentos, entre outros.

Este método tem a vantagem de respeitar o estudo individual dos grupos e a vida do grupo em sua unidade, evitando a dissociação prematura de seus elementos (ANDRADE, 2010).

Para coleta dos dados foi utilizado um questionário com perguntas objetivas e subjetivas para ser ter um maior entendimento do comportamento dos entrevistados no ambiente de trabalho. Segundo GIL (1999, p.129) os questionários tem a vantagem de atingir um grande número de pessoas, possibilita menores gastos com pessoal, garante o anonimato das respostas e não permite que o entrevistador influencie o entrevistado.

3.1 SUJEITOS DA PESQUISA

Os participantes desta pesquisa deveriam atender a dois requisitos importantes para poder responder os questionários: i) estar trabalhando em uma instituição pública e ii) trabalhar diretamente utilizando-se do computador em suas atividades. Os entrevistados devem estar enquadrados nesses requisitos para que se possa limitar o grupo de entrevistados e entender o comportamento ético destes funcionários no trabalho.

Não foram coletados o nome do entrevistado e o município a qual trabalha, com o objetivo de manter o anonimato dos mesmos. O intuito da pesquisa foi medir o comportamento ético dos funcionários na utilização dos softwares, identificar quais softwares são usados no trabalho e saber sua opinião em relação à pirataria de software.

3.2 COLETA DOS DADOS

Os dados foram coletados através de um formulário eletrônico, que na sua elaboração foi dividido em 6 etapas: i) definir o perfil do usuário; ii) entender como é seu comportamento ético no trabalho; iii) compreender que tipo de software prefere e utiliza no trabalho; iv) identificar sua opinião em relação a pirataria de software; v) medir seu conhecimento em relação a lei de proteção à propriedade intelectual do software e; vi) analisar como esses funcionários procuram protegem as informações da instituição ao qual trabalham.

Estes formulários foram enviados via e-mail e aplicativo de mensagens (*WhatsApp*) para funcionários que trabalham em instituições públicas

diretamente com o computador e seus softwares. Ao todo foram 17 questionários respondidos, durante o mês de dezembro de 2018 a abril de 2019. A aplicação do questionário foi feita através de uma rede de contatos dos referidos funcionários com o objetivo de traçar o perfil ético de comportamento desses entrevistados e das instituições ao qual trabalham.

3.3 ANÁLISE DOS DADOS

A análise dos dados teve como objetivo principal analisar o comportamento ético dos usuários de softwares nas organizações públicas, identificar os tipos de softwares utilizados nessas instituições, e apresentar o conhecimento dos funcionários sobre as leis vigentes no país que protegem a propriedade intelectual do criador do software. Em seguida foi feita uma pesquisa e uma apresentação dos dados coletados em forma textual e gráfica, que foram analisados individualmente. É por fim foi realizado uma análise de vulnerabilidade em sistemas do governo usados pelos funcionários no ambiente de trabalho.

4 ANÁLISE E APRESENTAÇÃO DOS RESULTADOS

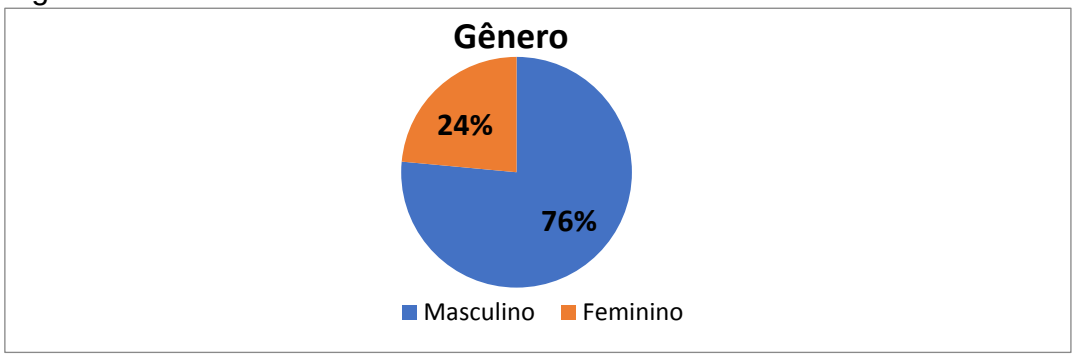
Os dados expostos abaixo são os resultados da pesquisa em torno dos funcionários de instituições públicas e o seu comportamento ético na utilização do computador durante o trabalho. Os dados foram coletados através de um formulário criado no google formulários e compartilhado via *WhatsApp* e *e-mail*.

A princípio, foi realizado um questionário para identificar o perfil do respondente. Logo em seguida, foi aplicado no questionário perguntas para entender o comportamento ético desses funcionários no ambiente de trabalho.

4.1 CARACTERIZAÇÃO DO OBJETO DE PESQUISA

Com base nos dados dos entrevistados constatou-se que o gênero dos entrevistados apresenta uma quantidade de homens superior à de mulheres, 76% são homens e 24% são mulheres.

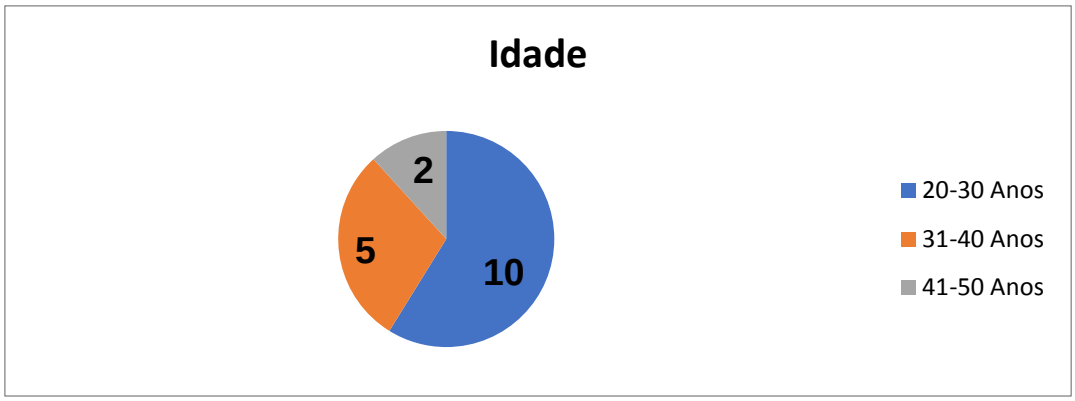
Figura 3 - Gênero



Fonte: Dados da pesquisa, 2019

Em relação à faixa etária, percebe-se que maior parte dos entrevistados estão abaixo dos 40 anos, com uma média de idade de 31 anos.

Figura 4 - Faixa etária de idade dos entrevistados

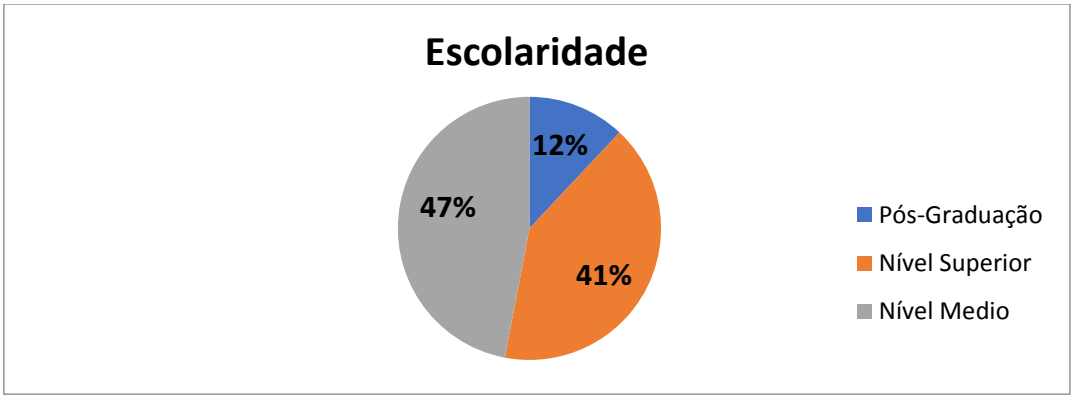


Fonte: Dados da Pesquisa, 2019.

No que se refere à escolaridade dos entrevistados, foram dispostas quatro alternativas, sendo as opções de formação (Ensino Fundamental, Ensino Médio, Ensino Superior e Pós-Graduação).

Identificou-se nessa pergunta que boa parte dos respondentes tem nível superior e pós-graduação, contabilizando os dois como 53% dos questionados.

Figura 5 - Escolaridade



Fonte: Dados da Pesquisa, 2019.

4.2 QUESTÕES DE ÉTICA NO TRABALHO

Foi analisado o comportamento ético dos funcionários da rede pública no seu ambiente de trabalho. Para início foi questionado aos funcionários se a instituição fornece algum manual de ética no trabalho para os mesmos.

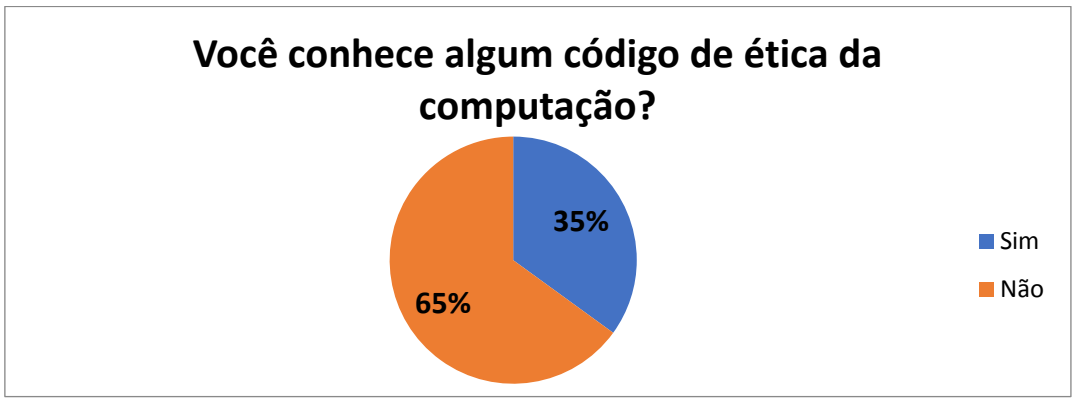
Figura 6 - Manual ético de conduta do trabalho

Fonte: Dados da Pesquisa, 2019.

Com base nos dados coletados constata-se que a maior parte das instituições onde os entrevistados trabalham não oferece um manual ético de conduta no trabalho, que, segundo Masiero (2000) é de extrema importância para o desempenho correto e ético do profissional, no que se refere ao uso das tecnologias.

Em relação à ética foi perguntado aos entrevistados se possuíam conhecimento sobre algum código de ética na computação.

Figura 7 - Conhecimento sobre o código de ética na computação

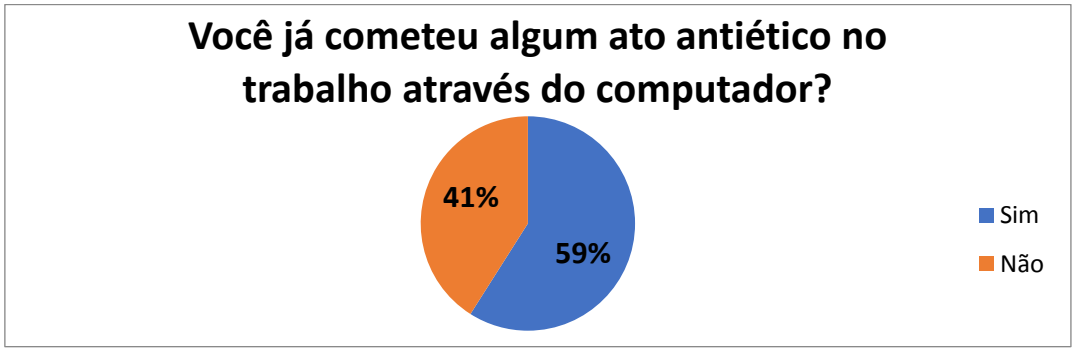


Fonte: Dados da Pesquisa, 2019.

Com base nos dados constatou-se que os funcionários das instituições não conhecem muito sobre a ética na computação, fortalecendo a ideia de Masiero (2000, p.26 apud MOOR, 1985), que classifica esse comportamento ético como algo ainda recente na sociedade, que necessita de mais estudos.

Outro questionamento feito foi se os entrevistados já haviam cometido algum ato antiético no computador durante o trabalho. Através do levantamento dos dados obteve-se que a maioria dos funcionários (59%) já cometeu algum ato antiético no trabalho. Podendo-se observar uma semelhança com o estudo global da BSA (2011), onde se obteve um resultado em que 57% dos usuários admitiram piratear software.

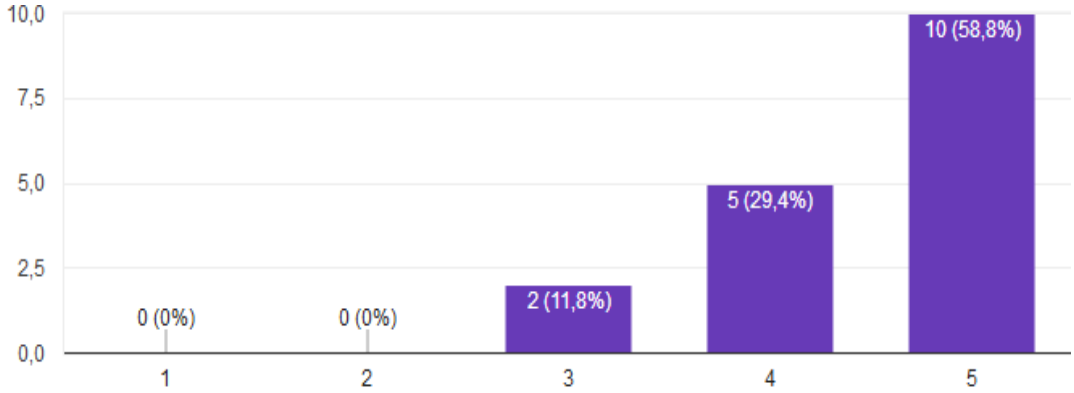
Figura 8 - Comportamento antiético no trabalho com o computador



Fonte: Dados da Pesquisa, 2019.

Ao questionar os funcionários sobre qual a importância em que eles classificam a ética na computação, foram dispostas cinco opções para eles classificarem a mesma. Dos dados coletados constatou-se que todos classificam a ética na computação com uma nota igual ou acima de três, constatando-se que nenhum dos respondentes considera a ética na computação como algo irrelevante.

Figura 9 - Nível de Importância para a ética na computação



Fonte: Dados da Pesquisa, 2019.

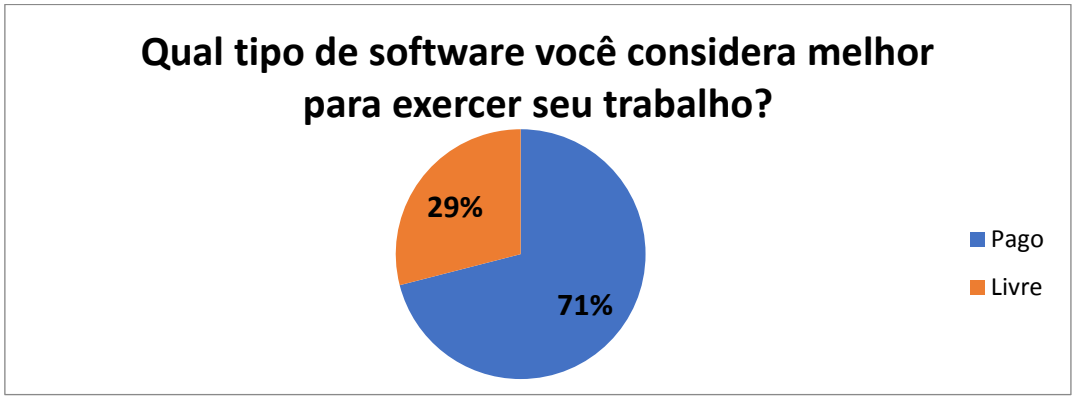
A partir das informações recebidas observa-se que a maior parte dos entrevistados considera ética na computação como algo importante, procurando tratar a mesma como algo importante para o trabalho. Surge assim, uma contradição, uma vez 58,8% consideram a ética extremamente importante e 59% já cometeram algum ato antiético.

4.3 TIPOS DE SOFTWARE

Para poder compreender e se ter uma ideia de quais ferramentas os funcionários públicos utilizam para desempenharem seus trabalhos, foi perguntado aos mesmos com que tipos de softwares trabalham diariamente, sendo fornecidas três opções para a resposta, que são softwares livres, pagos ou ambos. Com base nas respostas obteve-se que 82% dos funcionários utilizam os softwares pagos e livres para se trabalhar e somente 12% utilizam 100% softwares livres.

Com base na pergunta anterior foi indagado quais softwares os funcionários consideram melhor para se trabalhar.

Figura 10 - Software preferido para o trabalho



Fonte: Dados da Pesquisa, 2019.

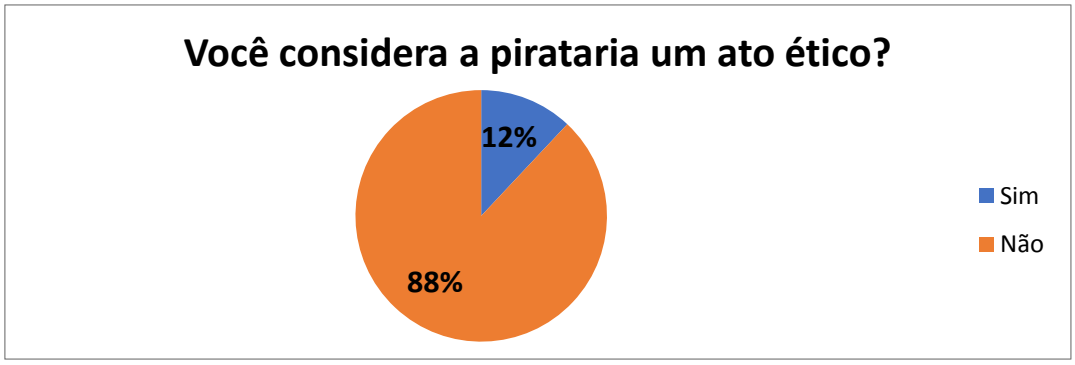
Com Base nas informações recebidas nota-se que a maioria dos funcionários prefere softwares pagos, confirmando o pressuposto de Engholm (2010), em que os funcionários procuram sempre utilizar a ferramenta tecnológica que traga mais facilidade e eficiência para desempenho do seu trabalho.

Visto as respostas anteriores foi questionado para qual função específica utilizam essas ferramentas, alguns responderam que utilizam essas ferramentas para processos administrativos, controle, tratamento e exibição de informações.

4.4 PIRATARIA DE SOFTWARE E SEGURANÇA DAS INFORMAÇÕES NO TRABALHO

Procurando entender um pouco mais sobre a ética desempenhada pelos funcionários no trabalho com o computador, foi questionado qual relação possuem com a pirataria de softwares e qual sua opinião sobre o tema. Para a grande maioria (88%) a pirataria é um ato antiético, enquanto a minoria (12%) considera a pirataria algo ético. Assim, as opiniões dos entrevistados coincidem com o conceito de ética proposto por Schwartz (2002), em que se deve ter responsabilidade e obedecer a lei.

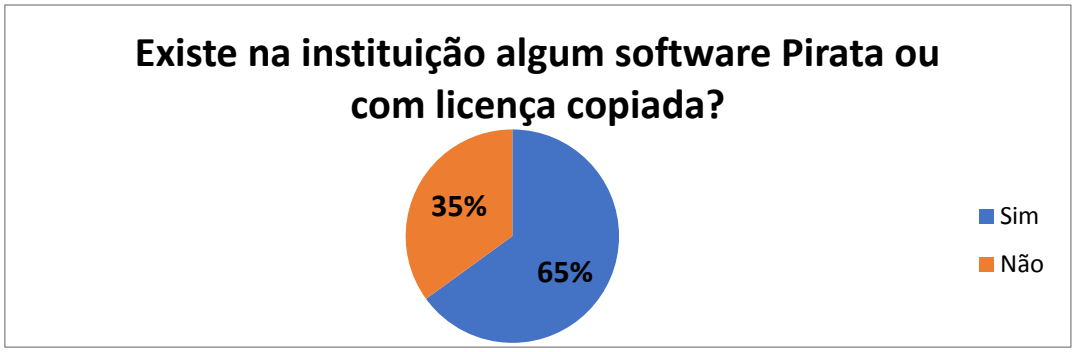
Figura 11 - Pirataria de software é algo ético



Fonte: Dados da Pesquisa, 2019.

Seguindo com o levantamento dos dados foi questionado aos funcionários se na instituição onde trabalham se faz uso de softwares piratas. Por mais que suas opiniões sejam contra a pirataria, foi constatado pela pesquisa que suas instituições que são públicas, praticam estes crimes que são graves. Como apresentado no gráfico abaixo.

Figura 12 - Pirataria no setor público

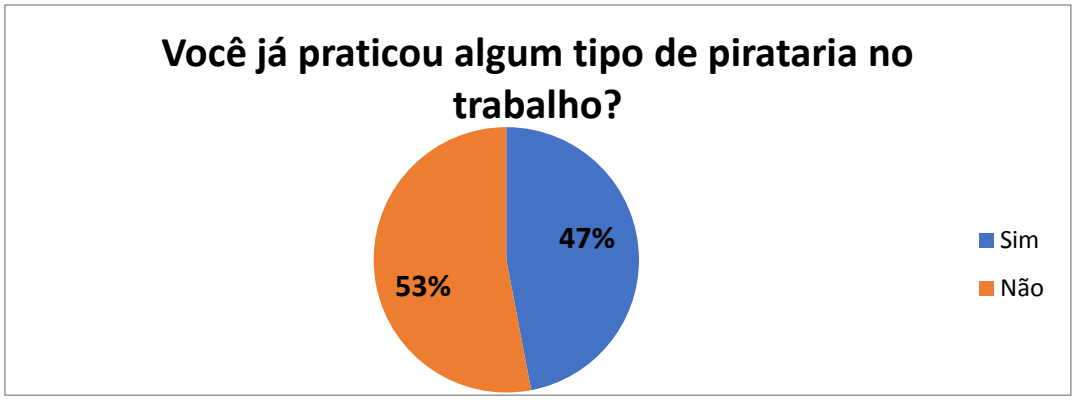


Fonte: Dados da Pesquisa, 2019.

A partir das informações coletadas, constatou-se que 65% das instituições públicas onde os entrevistados trabalham fazem uso de softwares piratas. Com a propagação deste crime acabam contribuindo negativamente para sociedade e para as próprias instituições em si. Segundo RUTTER e BRYCE (2008) estes crimes trazem prejuízos para o governo que perde na arrecadação de impostos e também acaba tendo ligação com o crime organizado.

Procurando saber mais sobre o comportamento dos funcionários no trabalho em relação a pirataria, foi questionado aos mesmos se já haviam praticado algum tipo de pirataria durante o exercício de seu trabalho. Com a coleta das informações notou-se que um número relevante de funcionários, cerca de oito no total, já cometeu esse crime no trabalho.

Figura 13 - Pratica de Pirataria no trabalho



Fonte: Dados da Pesquisa, 2019.

Com base nas informações coletadas observou-se que 47% dos funcionários já cometeu essa infração. Essas informações acabam coincidindo com os dados coletados pela BSA (2012) que mostram que a pirataria é maior em países emergentes, e estes funcionários acabam refletindo e de certa forma, fortalecendo esses dados coletados pela pesquisa da BSA.

Para procurar entender o motivo de funcionários públicos utilizarem ferramentas piratas, foi feita uma pergunta para que os mesmos definissem o motivo de utilizarem essas ferramentas ilegais. Segundo o primeiro entrevistado:

> "Visto as opções oferecidas terem menos qualidade para realização do trabalho, foi necessário utilizar um software mais completo, que neste caso era pirata. (ENTREVISTADO 1, 2019)".

Sabendo que softwares de origem duvidosa costumam apresentar problemas de segurança, devido a vírus que vem acompanhado do software, justificando sua facilidade, foi questionado aos entrevistados se eles já encontraram algum problema de segurança com a utilização desses softwares. Alguns afirmaram que nunca encontraram problemas, por outro lado a maioria

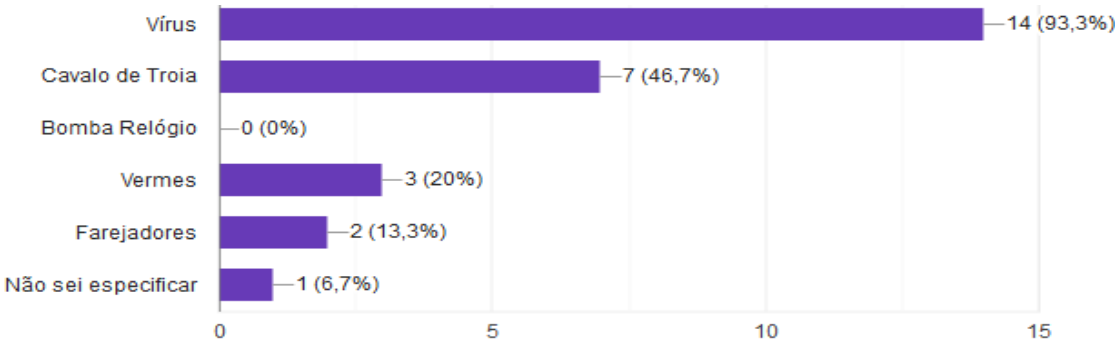
relatou que já teve problemas com isso, apontando que os sistemas vinham acompanhados de crackers que para validar o sistema vem acompanhado de trojans.

> “Muitas vezes, ter de desativar um software de segurança para fazer uso de ferramentas ilícitas traz uma falha de segurança” (ENTREVISTADO 5, 2019).

> “Com cracker usado para validar o sistema, na sua maioria possuem cavalos de troia. (ENTREVISTADO 4, 2019)”.

No gráfico abaixo está demonstrado quais problemas eles mais encontram nesses softwares.

Figura 14 - Programas maliciosos encontrados no trabalho

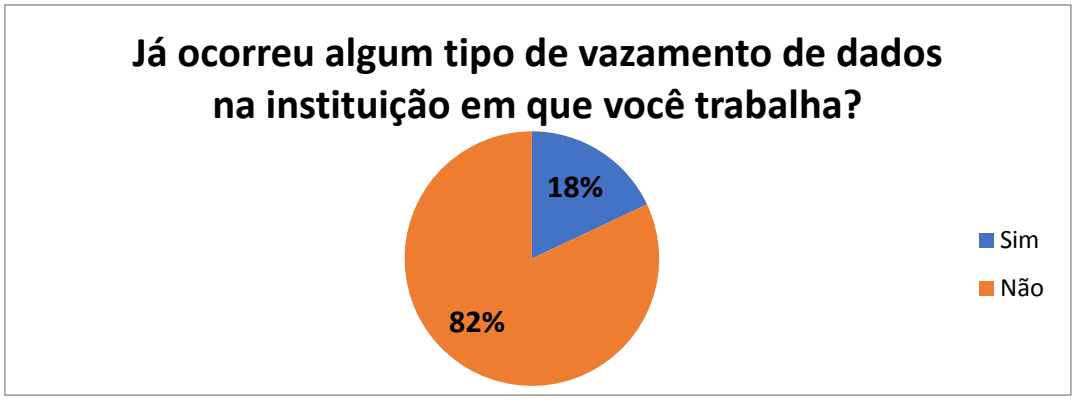


Fonte: Dados da Pesquisa, 2019.

Como apresentado no gráfico acima, os maiores problemas encontrados ao adquirir um software ilegal, são: vírus e cavalo de troia, programas maliciosos que tornam seu computador vulnerável a invasões e roubo de informações. Isto comprova a informação de MASIERO (2000), que apontou que hackers utilizam dessas informações para transmitir vírus e outros programas maliciosos.

Sabendo dos problemas que esses softwares trazem para a segurança dos dados da instituição foi perguntado se já ocorreu algum tipo de vazamento de informação na instituição pela qual trabalham. A maioria afirmou que isso nunca ocorreu, de certa forma desconhecendo se a ou não vazamento de informações. No entanto, três dos entrevistados (18%) afirmam que já se depararam com esse problema, demonstrando os problemas que estas ferramentas ilegais trazem para a segurança das informações da instituição.

Figura 15 - Vazamento de informações



Fonte: Dados da Pesquisa, 2019.

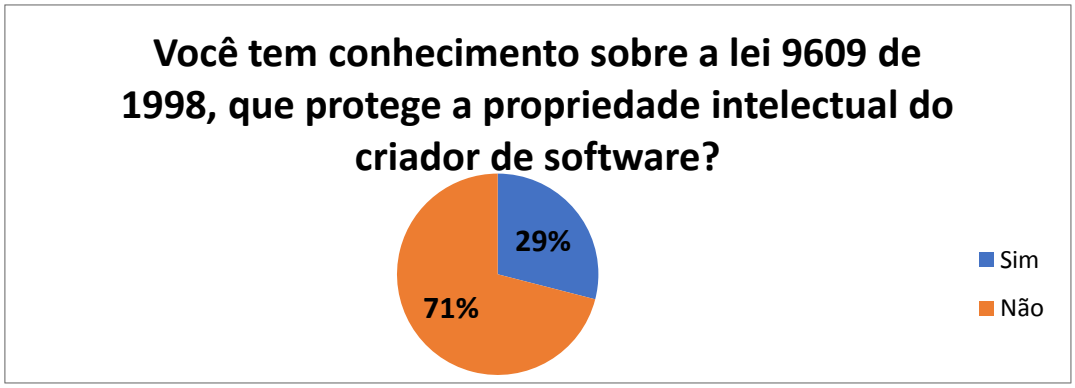
Procurando entender como a instituição a qual os funcionários trabalham procuram se defender de invasões, foi perguntado aos mesmos quais ferramentas são utilizadas para proteção dos dados. Deixando a resposta em aberta para que os mesmos informassem como procuram se defender de possíveis invasões, eles informaram que:

> ”Existe firewall registrando toda atividade da rede, antivírus, hierarquia de usuários, boas práticas”. (ENTREVISTADO 5, 2019).
>
> “Os dados são criptografados, usamos banco de dados nas nuvens.” (ENTREVISTADO 8, 2019).
>
> “Os sistemas são acessados somente por pessoas autorizadas.” (ENTREVISTADO 6, 2019).

4.5 ENTENDIMENTOS SOBRE A LEGISLAÇÃO

Abordando o assunto sobre a legislação, para procurar entender se os funcionários têm algum conhecimento referente a lei e as punições por infringir crimes de pirataria de software e roubo de propriedade intelectual, foi questionado se eles tinham conhecimento sobre a lei 9609 de 1998, que protege a propriedade intelectual do criador do software. Conforme se observa na figura abaixo, a maioria desconhece tal lei.

Figura 16 - Conhecimento sobre a lei 9609

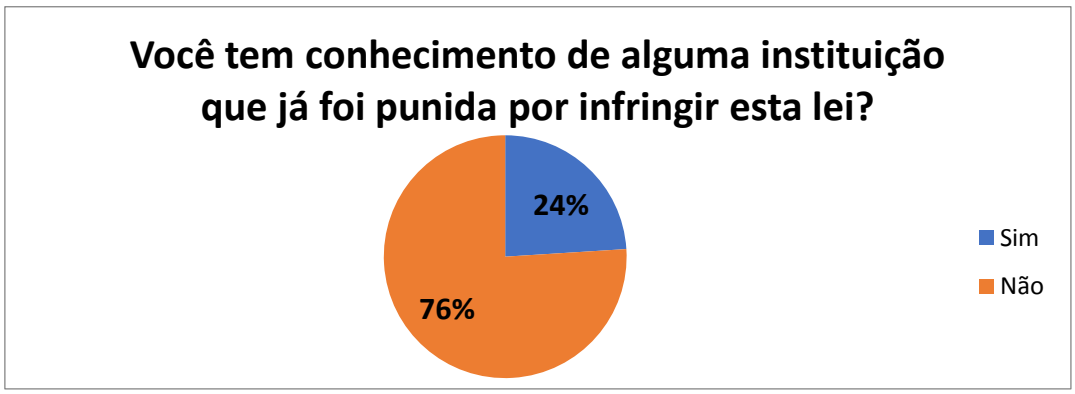


Fonte: Dados da Pesquisa, 2019.

Com base na pesquisa constatou que 71% dos entrevistados desconhece a lei de propriedade intelectual. Esses dados confirmam um elevado desconhecimento dos funcionários públicos em relação à lei em questão, chegando a ser um dos motivos para cometerem o crime de pirataria de software, o que acaba manchando a imagem da instituição, como aponta Paletta (2004).

Além de procurar saber sobre seu conhecimento em relação à lei em questão, procurou saber dos funcionários se eles conheciam quais as punições para aqueles que desobedecem a essa lei e se conheciam alguma instituição que já foi punida por cometer esse crime. Abaixo o gráfico dos funcionários que conhecem algum município que já foi punido.

Figura 17 - Conhecimento sobre alguma instituição pública punida por desobedecer à lei 9609 de 1998



Fonte: Dados da Pesquisa, 2019.

A pesquisa apontou que a maioria dos entrevistados desconheciam casos onde instituições foram punidas por cometer esse crime, no entanto 24% das pessoas mostrou conhecer casos onde ocorreu punição.

> “A Universidade Cândido Mendes teve sua sede leiloada pela Justiça para quitar a dívida feita com a Microsoft após ter perdido um processo pelo uso de versões piratas do sistema operacional Windows.” (ENTREVISTADO, 2019).

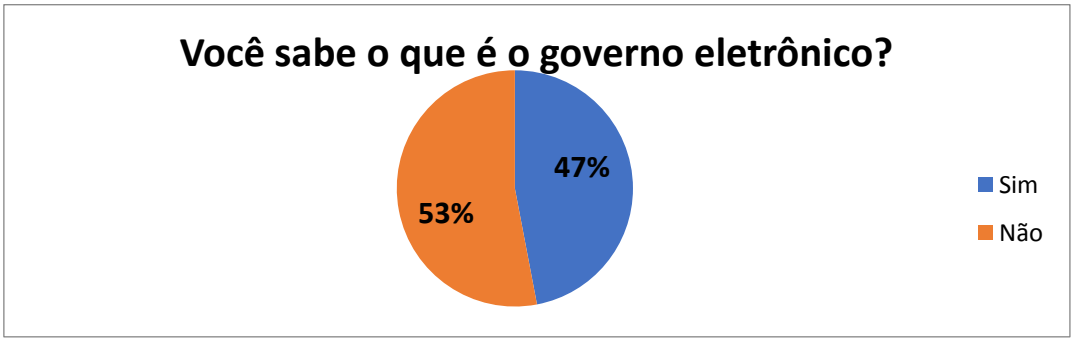
Com base nos dados constatou-se que nem todos os entrevistados consideram a pirataria um ato antiético e que a maioria faz uso destas ferramentas ilegais no ambiente de trabalho, além de poucos conhecerem sobre a lei 9609 de proteção à propriedade intelectual, refletindo claramente a falta de conhecimento sobre o comportamento ético na computação, algo que as instituições deveriam apresentar aos seus funcionários.

4.6 GOVERNO ELETRÔNICO E A UTILIZAÇÃO DE SOFTWARES LIVRES.

Por fim, procurando saber se os entrevistados conhecem e se utilizam ferramentas livres, foi perguntado se sabiam o que era governo eletrônico, se já utilizaram seus sistemas e se já procuraram utilizar softwares livres para melhor desempenhar seu trabalho.

Primeiro foram questionados se conheciam o termo governo eletrônico. Pouco menos da metade afirmou conhecer o que é governo eletrônico.

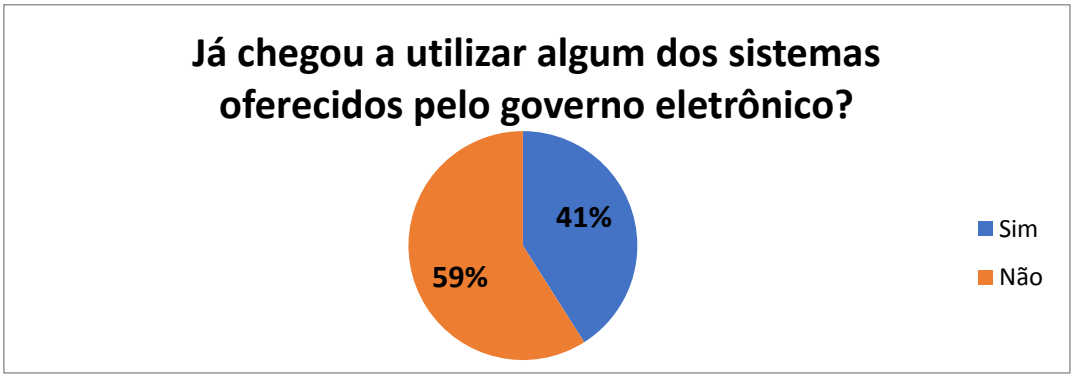
Figura 18 - Conhecimento sobre governo eletrônico



Fonte: Dados da Pesquisa, 2019.

Com base nos dados constata-se que 53% dos funcionários não sabe o que é governo eletrônico, desconhecendo está iniciativa do governo, que visa melhorar o desempenho das instituições, como explicado por Prado e Souza (2014) e Cunha (2010).

Figura 19 - Utiliza algum software do governo



Fonte: Dados da Pesquisa, 2019.

Como demonstrado nos dados apresentados acima, 59% dos servidores entrevistados não utiliza nenhuma das ferramentas oferecidas pelo governo eletrônico, contrariando as ideias de Cunha (2010), defendendo que o uso desses sistemas são importantes para se construir um governo aberto e ágil aumentando a eficiência dos serviços públicos.

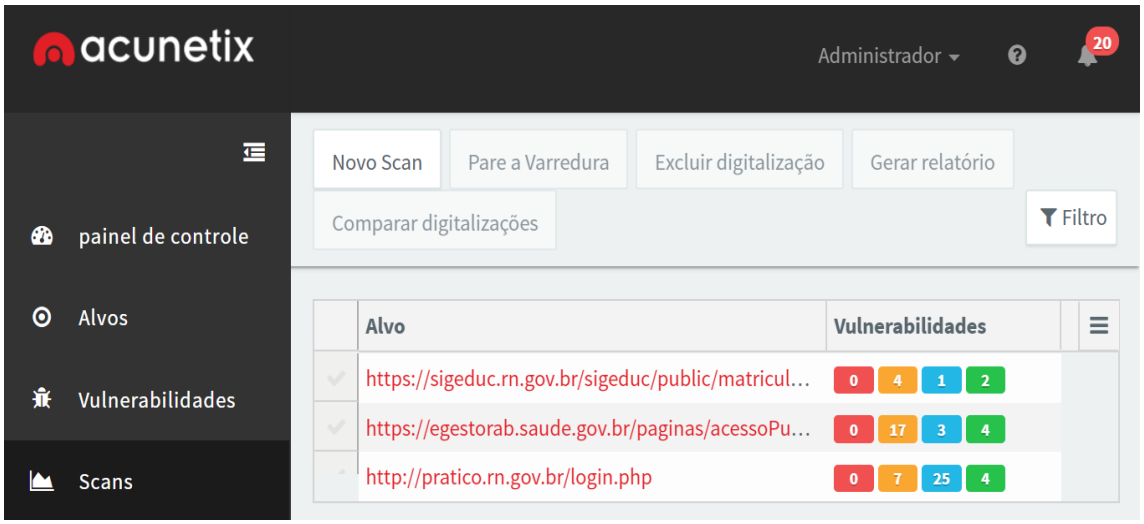
Por fim apresentou-se aos funcionários questões relacionadas ao uso de ferramentas de softwares livre, para procurar saber quantos deles buscam utilizar essas ferramentas no trabalho e qual razão eles consideram elas importantes. A maioria informou que a adoção de padrões abertos para o Governo Eletrônico (e-Gov), a segurança e a independência que o software livre proporciona são importantes fatores para utilização desses softwares.

5 ANALISE DE VULNERABILIDADE E TESTE DE INVASÃO

Para se analisar a vulnerabilidade de 3 (três) sistemas do governo eletrônico, com o intuito de mostrar falhas de segurança em sistemas do governo. Será utilizando o *Acunetix trial* um *Scan* próprio para verificar as vulnerabilidades de sistemas web. Para se realizar a invasão ao sistema e testar

a segurança da rede do usuário foi realizado um ataque simulado utilizando o *wireshark*. Deve ser ressaltado que todos os testes foram feitos com o intuito acadêmico, não tendo objetivo de causar prejuízo aos sistemas analisados.

Figura 20 - Acunetix



Fonte: Autoria Próprio, 2019.

Os quatro sistemas analisados serão o Prático RN, e-gestor AB, o SIGEDUC e um site processo ágil.

5.1 ANALISE DE VULNERABILIDADE DO PRÁTICO RN.

O Prático RN é um sistema do governo do Rio Grande do Norte que serve para troca de informações entre o governo e suas instituições, como uma plataforma de e-mails do estado.

Figura 21 - Prático RN

Fonte: Prático RN, 2019.

Ao todo foram encontrados 36 alertas, sendo 7 de vulnerabilidade de risco médio e 29 de nível baixo, neste caso serão destacadas 3 (três) vulnerabilidades. Entre as principais vulnerabilidades encontradas no sistema estão um arquivo de configuração de desenvolvimento. Foi encontrado um arquivo que pode expor informações confidenciais auxiliando um usuário mal-intencionado a preparar mais ataques avançados. É recomendado remover ou restringir o acesso a todos os arquivos de configuração acessíveis pela Internet. Outra vulnerabilidade encontrada está a *Cross-Site Request Forgery* (CSRF), esta vulnerabilidade permite que um invasor engane a vítima e execute um pedido que a vítima não pretendia fazer. Portanto, com o CSRF o invasor abusa da confiança que o aplicativo da Web tem com o navegador da vítima. É necessário que verifique se este formulário requer proteção anti-CSRF e implementar contramedidas de CSRF se necessário. Por fim, foi encontrado diretórios sensíveis, estes diretórios poderiam ajudar um atacante a saber mais sobre seu alvo. É recomendável restringir o acesso a esse diretório ou removê-lo do site.

Tabela 4 - Detalhes do escaneamento do Pratico RN

Hora de início	27/06/2019, 15:50:16
Inicie a URL	http://pratico.rn.gov.br/login.php

Host	pratico.rn.gov.br
Tempo de varredura	51 minutos e 5 segundos
Informações do servidor	Apache
Servidor OS	Desconhecido
Tecnologias de Servidor	PHP

Fonte: autor próprio, 2019.

Tabela 5 - Alertas

Total de Alertas	36
High	0
Medium	7
Low	25
Informational	4

Fonte: autor próprio, 2019.

Tabela 6 - Vulnerabilidades Destacadas

Vulnerabilidades	**Recomendação**
Cross-Site Request Forgery.	Verifique se este formulário requer proteção anti-CSRF e implemente contramedidas de CSRF se necessário.
A configuration file	Restringir ou remover o acesso a esse tipo de arquivo.
As credenciais do usuário são transmitidas por um canal não criptografado.	Como são informações confidenciais, sempre devem ser transferidas para o servidor através de uma conexão criptografada (HTTPS).

Fonte: autor próprio, 2019.

5.2 ANALISE DE VULNERABILIDADE E-GESTOR AB

Segundo o próprio site do e-gestor (2017), o sistema pode ser definido como:

> Uma plataforma *WEB* para centralização dos acessos e perfis dos sistemas da Atenção Básica - AB, bem como um aglutinador de informações próprias para os gestores estaduais e municipais.

Figura 22 - e-Gestor

Fonte: e-gestor, 2019

Neste sistema ao todo foram encontrados 24 alertas de vulnerabilidade, sendo 17 de risco médio e 7 de nível baixo. Nesta analise serão destacadas duas vulnerabilidades, o sistema utiliza TLS 1.0 uma criptografia fraca para proteger informações confidenciais transferidas para sites da Web, sendo recomendável desabilitar o TLS 1.0 e substituir pelo 1.2 ou superior com um protocolo de criptografia mais seguro. Outra fragilidade no sistema destacada é o cookie não possui o conjunto de sinalizadores HttpOnly, que é recomendável para corrigir essa vulnerabilidade definir o sinalizador HttpOnly para esse cookie.

Tabela 7 - Detalhes do escaneamento do e-Gestor

Hora de início	27/06/2019, 16:48:20
Inicie a URL	https://egestorab.saude.gov.br/paginas/acessoPublico/relatorios/relatoriosPublicos.xhtml
Host	egestorab.saude.gov.br

Tempo de varredura	99 minutos e 4 segundos
Informações do servidor	Apache-Coyote / 1.1
Servidor OS	Desconhecido
Tecnologias de Servidor	Java / J2EE, Java / J2EE

Fonte: Autor próprio, 2019.

Tabela 8 - Alertas e-gestor

Total de Alertas	24
High	0
Medium	17
Low	3
Informational	4

Fonte: Autor próprio, 2019.

Tabela 9 - Vulnerabilidades Destacadas e-gestor

Vulnerabilidades	**Recomendação**
TLS 1.0 não é uma criptografia forte quando usado para proteger informações confidenciais transferidas para sites da Web.	Desabilitar o TLS 1.0 e substituir pelo 1.2 ou superior u protocolo de criptografia mais seguro.
cookie não possui o conjunto de sinalizadores HttpOnly.	Se possível, você deve definir o sinalizador HttpOnly para esse cookie.

Fonte: Autor próprio, 2019.

5.3 ANÁLISE DE VULNERABILIDADE SIGEDUC

O Sistema Integrado de Gestão e Educação (SIGEDUC) é um recurso para modernizar as rotinas de gestão, possibilitando um monitoramento dos indicadores da escola e apoiar o trabalho de seus usuários.

Figura 23 - SIGEDUC

Fonte: SIGEDUC, 2019.

Com base no *Scan* foi encontrado 7 vulnerabilidades no sistema, sendo 4 de risco médio é 3 de baixo risco. Neste caso serão destacados dois riscos encontrados, o RC4 *cipher suites detected*, que permite ataques surgirem de falhas estatísticas no *keystream* gerado pelo algoritmo RC4 que se tornam aparentes no TLS. A contramedida mais eficaz contra este ataque é parar de usar o RC4 no TLS. Outra vulnerabilidade encontrada foi o TLS 1.0 *enabled*, o servidor web suporta criptografia por meio do TLS 1.0 que não é considerado forte. Para isso é recomendável retirar o TLS 1.0 e substituir pelo TLS 1.2 ou superior.

Tabela 10 - Detalhes do escaneamento do SIGEDUC

Hora de início	27/06/2019, 20:51:03
Inicie a URL	https://sigeduc.rn.gov.br/sigeduc/public/matricula/home_sigeduc.jsf;jsessionid=7EEA1173E13354ED3638940598BC4418.srv3inst1
Host	sigeduc.rn.gov.br
Tempo de varredura	3 minutos e 25 segundos

Informações do servidor	SEEC
Servidor OS	Desconhecido
Tecnologias de Servidor	Java/J2EE

Fonte: Autor próprio, 2019.

Tabela 11 - Alertas SIGEDUC

Total de Alertas	7
High	0
Medium	4
Low	1
Informational	2

Fonte: Autor próprio, 2019.

Tabela 12 - Vulnerabilidade destacada SIGEDUC

Vulnerabilidades	**Recomendação**
TLS 1.0 não é uma criptografia forte quando usado para proteger informações confidenciais transferidas para sites da Web.	Desabilitar o TLS 1.0 e substituir pelo 1.2 ou superior u protocolo de criptografia mais seguro.
RC4 cipher suites detected	Procurar para de usar o RC4 no TLS.

Fonte: Autor próprio, 2019.

Tabela 13 - Quadro de Vulnerabilidades

Sistemas	**Alertas**	**Principais Vulnerabilidades**	**Recomendação**
Prático RN	36	1. Arquivo que pode expor informações confidenciais.	1. Remover ou restringir acesso a todos os

		2. *Cross-Site Request Forgery.*	arquivos de configuração acessíveis pela internet. 2. verifique se este formulário requer proteção anti-CSRF e implementar contramedidas de CSRF se necessário.
e-Gestor	24	1. *Cookie(s) without HttpOnly flag set.*	1. Definir o sinalizador *HttpOnly* para esse *cookie*.
SIGEDUC	7	1. RC4 *cipher suites detected.* 2. TLS 1.0 *enabled*.	1. parar de usar o RC4 no TLS. 2. retirar o TLS 1.0 é substituir pelo TLS 1.2 ou superior.

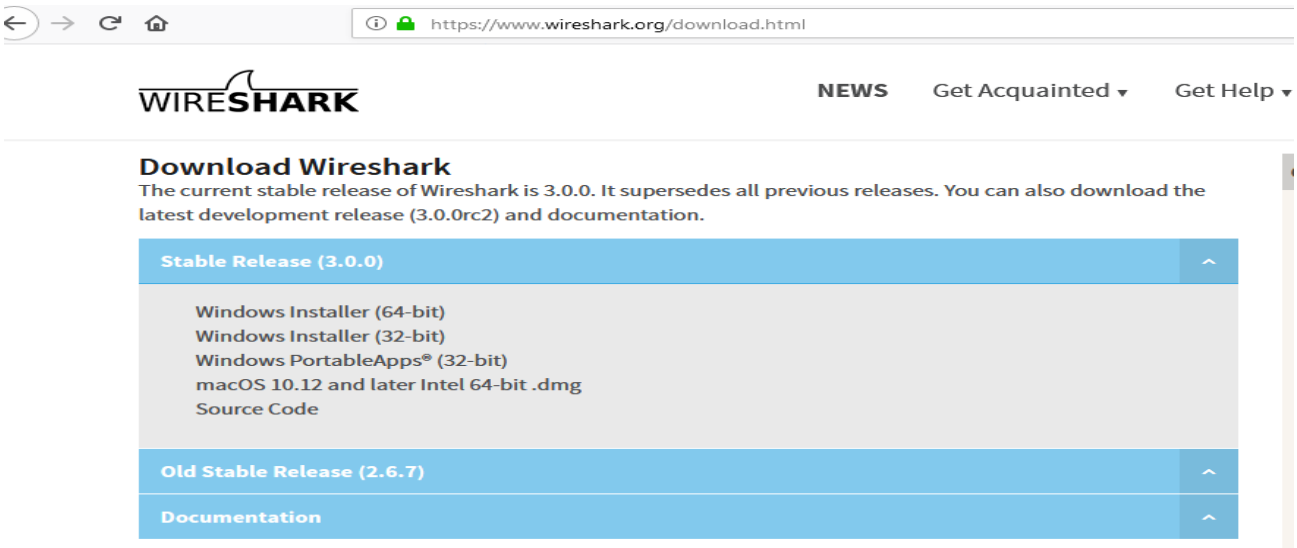
Fonte: Autor próprio, 2019.

5.4 TESTE DE INVASÃO DO SIPNI

Com o intuito de verificar a segurança no sistema é da rede do usuário, foi realizado um teste de invasão utilizando o *wireshark*.

O sistema foi baixado do site www.wereshark.org, onde o usuário vai em downloads e escolhe o sistema de acordo com a máquina que está utilizando.

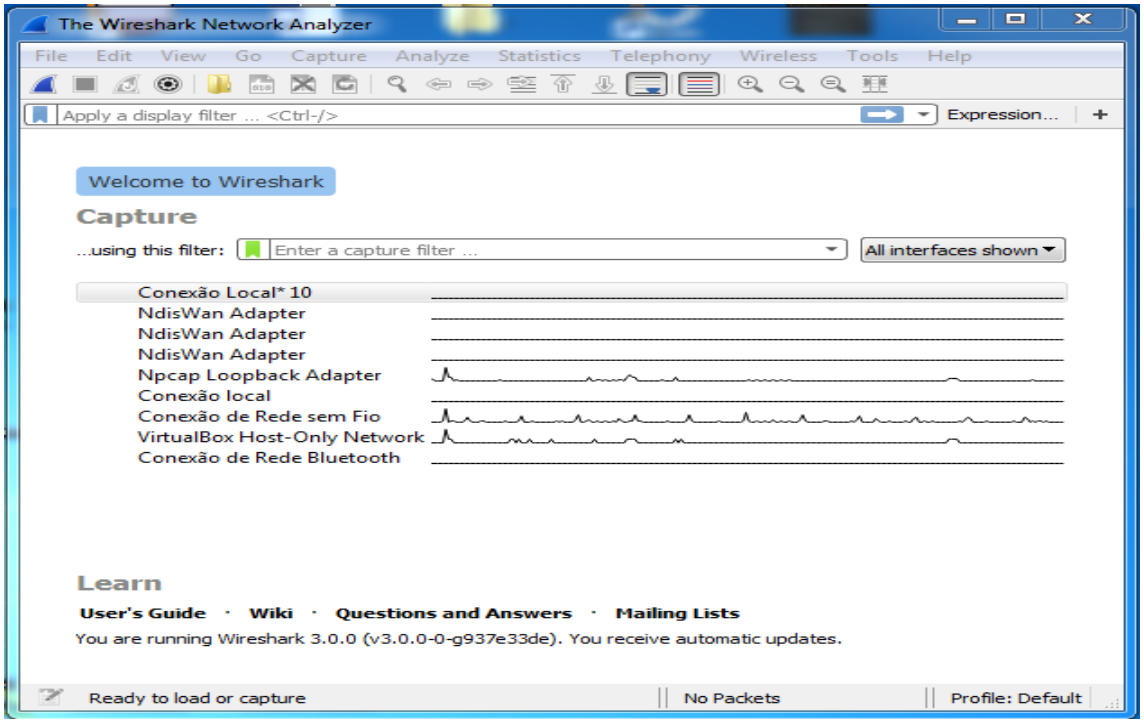
Figura 24 - Download Wireshark



Fonte: Wireshark, 2019.

Depois de instalado, o usuário abre o sistema e no menu inicial escolhe a conexão que deseja monitorar.

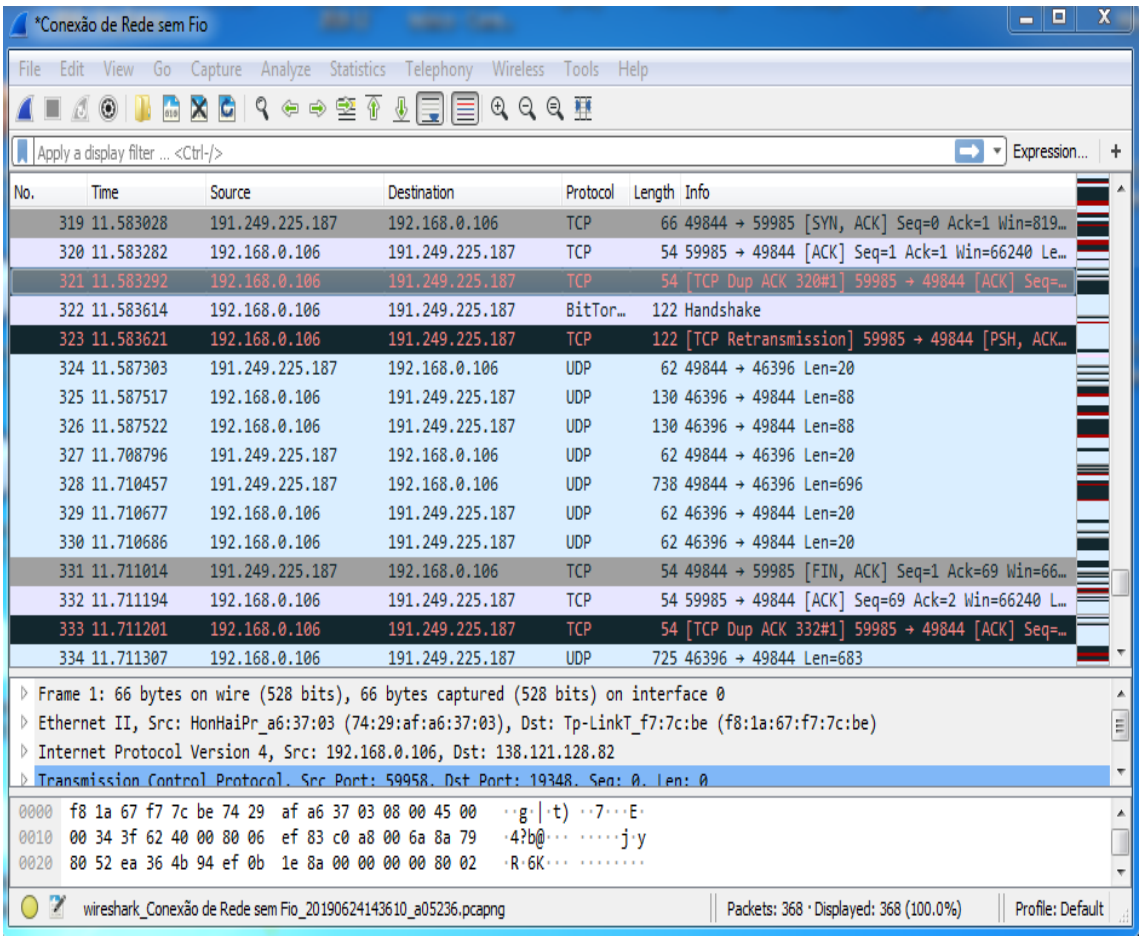
Figura 25 - Menu inicial Wireshark



Fonte: Autoria Próprio, 2019.

Neste teste, foi utilizada a opção de conexão de rede sem fio. Depois de escolhido na tela inicial a rede que será monitorada, será exposto para o usuário um menu de tarefas acompanhado de um filtro de pesquisa, em que o usuário poderá realizar uma pesquisa mais minuciosa, além de expor as máquinas que estão utilizando a rede em questão, mostrando o IP da mesma e os protocolos de rede que estão sendo utilizado no momento.

Figura 26 - Tela de conexão

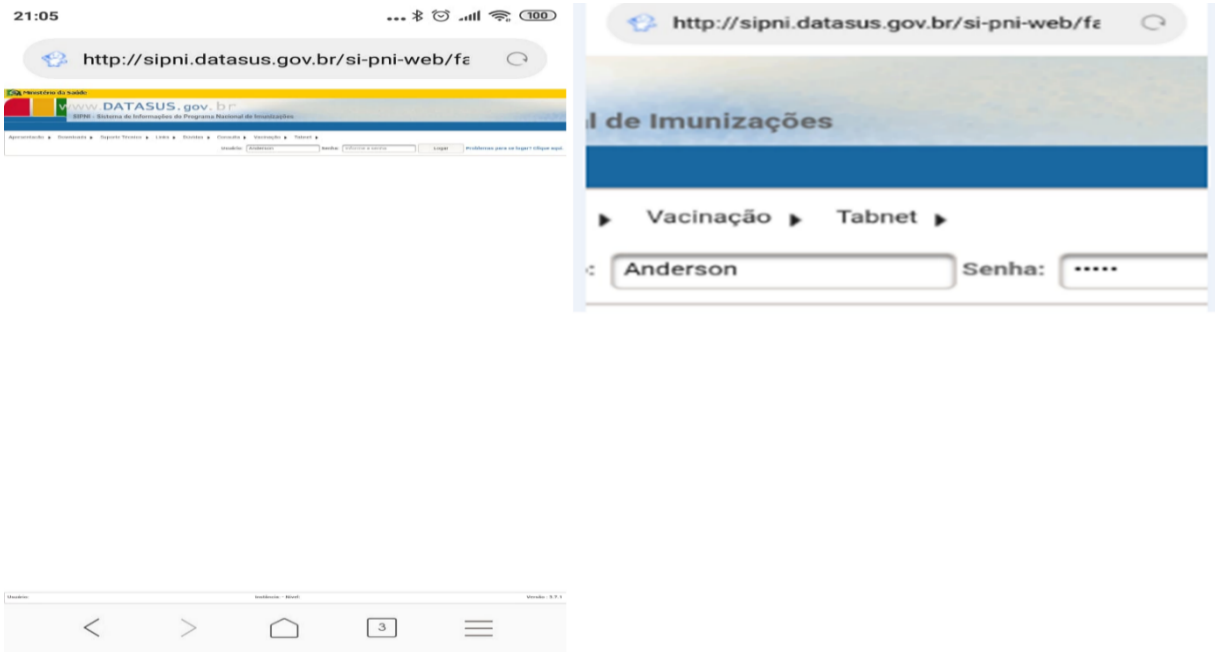


Fonte: Autoria própria, 2019.

Por mais que o *wireshark* capture sozinho os protocolos, ele sozinho não é capaz de capturar informações de outras máquinas em sua rede, para isso será preciso utilizar o *Arpspoof* que serve para redirecionar os pacotes a partir de um host-alvo (ou todos os hosts), uma forma extremamente eficaz de *sniffing* para tráfego em um interruptor. O ARP spoofing é uma técnica usada por cybers criminosos para realizar ataques em MITM (Man in The Middle), DOS (Denial of Service), ou explorar falhas para se ter acesso ao equipamento da vítima. O *Address Resolution Protocol* (ARP) é um protocolo de camada 2 no modelo de comunicação *Open System Interconnection* (OSI) que é responsável pela resolução de endereços IP e MAC.

Neste exemplo utilizou-se para realizar o ataque ao celular Motorola com o endereço de IP 192.168.0.101. Entrarei em um site do governo, que geralmente utiliza um protocolo http, um protocolo pouco seguro, que pode ser invadido. No site do sipni.datasus.gov, site do governo destinado ao sistema de saúde, relativo a vacinas, irei utilizar o nome de usuário como Anderson e a senha igual a 12345, como será demonstrado na figura abaixo.

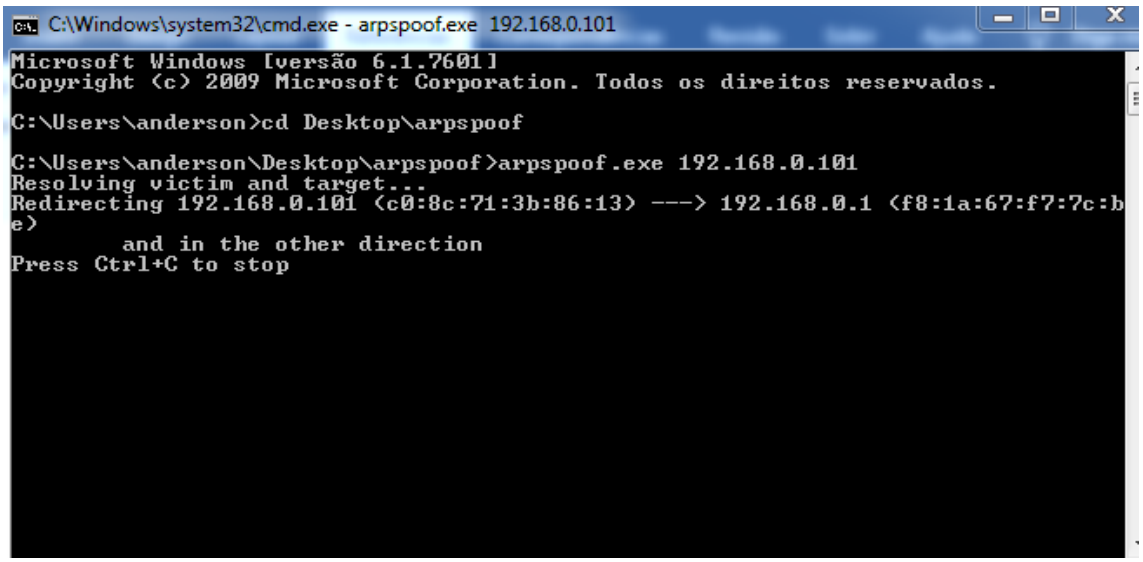
Figura 27 - Site do sipni na tela do celular



Fonte: SIPNI, 2019.

Primeiro deve-se instalar o arpspoof.exe, depois precisa abrir o processador de comando do *Windows* o cmd.exe, em seguida executar o comando arpspoof.exe acompanhado do endereço de IP da máquina que será invadida.

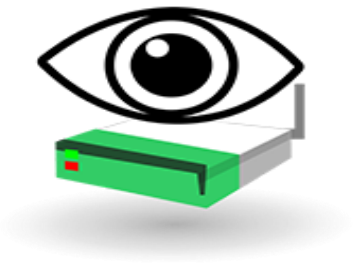
Figura 28 - Ataque do Arpspoof



Fonte: Autoria própria, 2019.

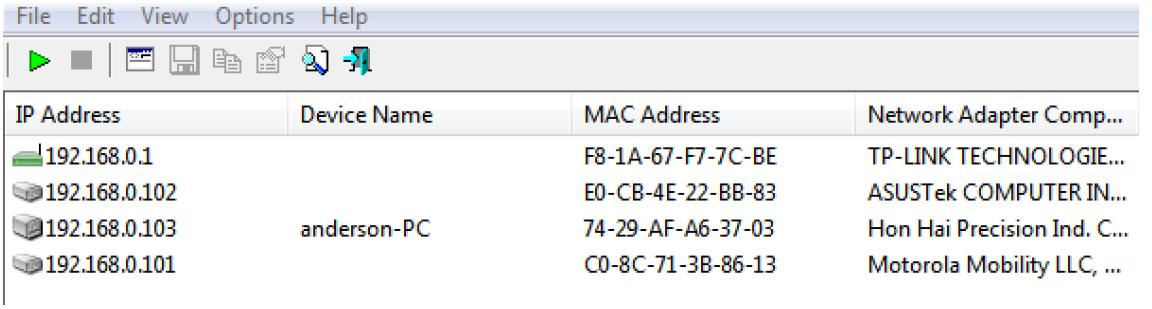
Para se descobrir o IP da vítima, pode-se usar um programa chamado *Wireless Network Watcher* que mostra todos os IPS das máquinas que estão na mesma rede da vítima.

Figura 29 - Wireless Network Watcher



Fonte: http://informatics-club.blogspot.com/2016/07/wireless-network-watcher-v-171.html

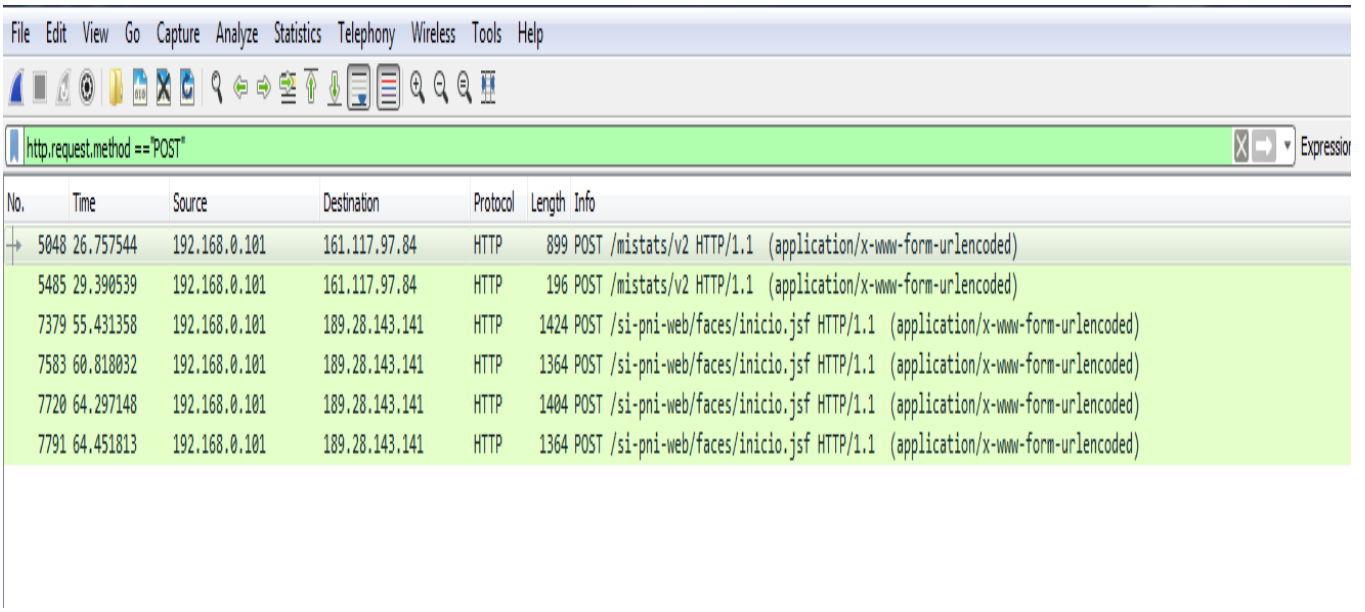
Figura 30 - Wireless Network Watcher em ação



Fonte: autoria própria, 2019.

Depois que se inicia o ataque o *wireshark* irá capturar todos os protocolos da máquina da vítima, como mostrado na figura 8. Para visualizar as informações da vítima, o *hacker* filtra a informação, que pode ser feita de duas maneiras, a primeira usando um caminho como *http.request.method =="POST"* que irá listar todos os métodos post capturados.

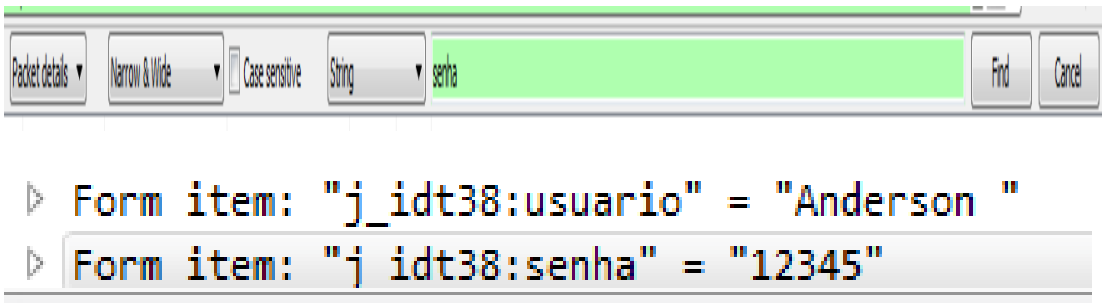
Figura 31 - Filtro com o Método Post



Fonte: Autoria Próprio, 2019.

Outra maneira seria através do atalho ctrl+f e filtrar por senha, que irá lhe mostrar a senha utilizada pelo usuário e o nome do usuário.

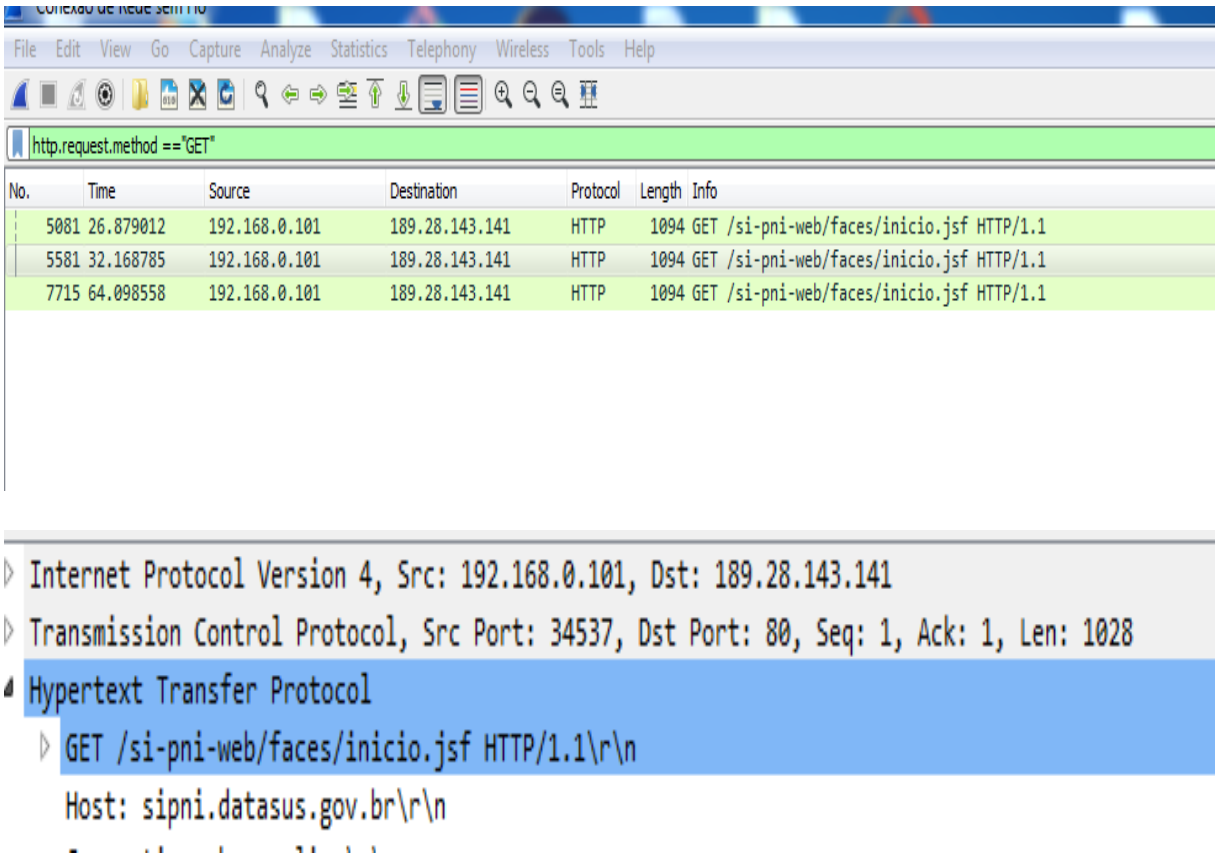
Figura 32 - Filtrar a pesquisa utilizando ctrl + f



Fonte: Autor Próprio, 2019.

Mostrando claramente o usuário e a senha capturados. Para se saber o site que o usuário entrou e inseriu esses dados, basta apenas usar o comando *http.request.method == "GET"* que irá listar todos os métodos *get* capturados.

Figura 33 - Método GET

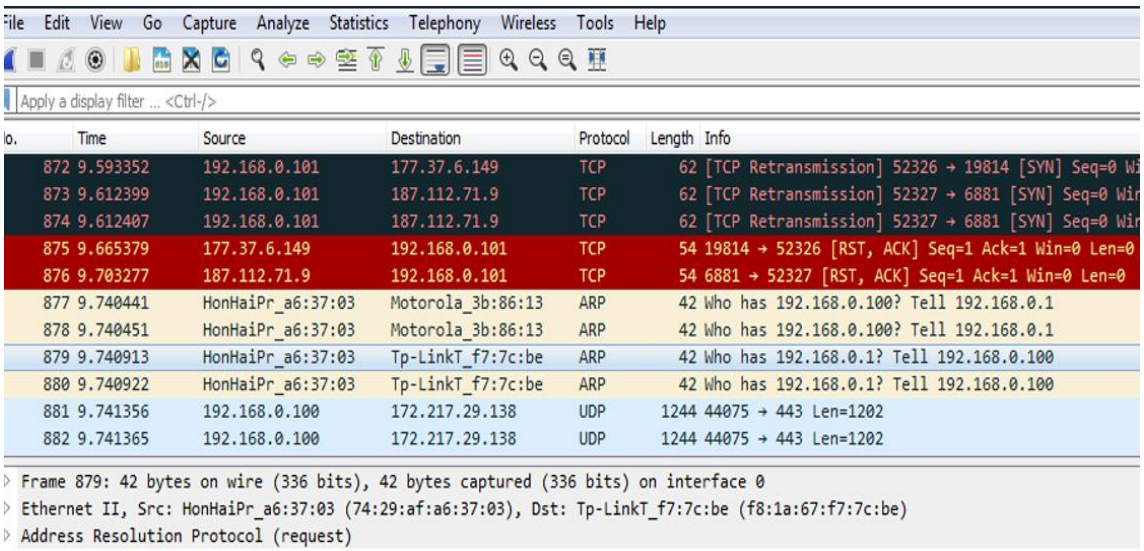


Fonte: Autoria Próprio, 2019.

Nota-se que sistemas governamentais podem ser invadidos e trazem como consequências vazamento de dados que acarretam prejuízos financeiros para o estado. Para se defenderem dessas invasões apresentadas, os usuários comuns e principalmente os que trabalham com sistemas do governo, devem ter bastante disciplina e segurança com suas informações, evitar compartilhar o acesso da rede que utiliza para desconhecidos, procurar criptografar tudo que envia ou recebe na rede, utilizar redes *wi-fi* confiáveis, procurar saber quem está utilizado a rede através do *Wireless Network Watcher* ou através do comando arp –a no Prompt de Comando que irá listar todas as máquinas que estão conectadas a rede e utilizar o próprio *wireshark* para identificar as invasões através dos pacotes mostrados em vermelho, o que pode indicar ataques DOS ou outras atividades de *hackers*.

Os ataques DOS são problemáticos porque inundam servidores a partir de endereços IP falsificados, fazendo com que o desempenho da máquina caia e o servidor eventualmente falhe.

Figura 34 - Identificando invasão



Fonte: Autoria Próprio, 2019.

Para remover um desses *sniffers*, é recomendável excluir os arquivos e pastas associados a ele.

Por outro lado, para se evitar problemas com *sniffers* que estejam clandestinamente em sua rede, é recomendável usar um software de segurança que possua um *scanner* de rede que a vasculhará em busca de problemas e o orientará sobre como resolvê-los (Avast, 2018).

Outra maneira de se proteger é utilizar sistemas que funcionem com o protocolo https que criptografa os dados e impede o farejador de encontrar os dados que desejam roubar das vítimas.

6 CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo analisar o comportamento ético dos funcionários públicos que se utilizam de softwares para desempenhar o seu trabalho, procurando entender mais especificamente qual sua opinião sobre a pirataria, os tipos de sistemas utilizados, procurar saber qual seu conhecimento sobre a lei de segurança da propriedade intelectual do software e, por fim, uma análise de sistemas públicos e privados com o objetivo de apresentar as vulnerabilidades presentes nestes sistemas, apresentando como resolver estes problemas.

Referente aos resultados, constatou-se que a maioria das instituições não oferece manuais de comportamento ético no trabalho para os funcionários. Além disso, no que se refere ao comportamento dos funcionários, observou-se que muitos cometeram crimes de roubo de propriedade intelectual de softwares no trabalho. Assim, vemos que instituições públicas, que deveriam apresentar uma conduta ética acima do comum, falham em não deixar claro para os funcionários a importância de questões éticas na sua conduta no ambiente de trabalho, no que se refere ao uso de computadores e sistemas.

No que se refere à legislação brasileira, que trata sobre a proteção da propriedade intelectual do software, foram identificados que a maioria dos funcionários desconhece essa lei, o que parece ser algo grave, uma vez que são

funcionários públicos atuando em suas funções, ou seja, deveriam, no mínimo, conhecer e obedecer à legislação do país. O que também chama atenção é o fato de a maioria dos entrevistados não conhecerem nenhum caso em que alguma instituição foi punida, o que pode reforçar o seu comportamento e desinteresse em conhecer a legislação.

Se referindo aos sistemas do governo eletrônico, ao se realizar a análise de vulnerabilidade em alguns constatou-se que ainda existem problemas de segurança nestes sistemas.

Uma possível solução para o problema dos crimes de roubo da propriedade intelectual e do comportamento antiético dos funcionários público é a utilização de softwares livres, que foram citados, por aqueles que já usam, como sistemas seguros, assim como os sistemas do governo eletrônico, já que são sistemas próprios para o desempenho do seu trabalho.

Assim, a pesquisa teve grande valia no sentido de conhecer como funcionários públicos se comportam eticamente no trabalho, expondo como eles vêem a ética na computação, mostrando de forma notória que se as instituições não apresentarem um manual de ética para seus funcionários e não começarem a fiscalizá-los, bem como, se os mesmos não buscarem informações sobre as questões relevantes a ética, tanto os funcionários como as instituições podem acabar se prejudicando e trazendo problemas futuros para as mesmas. A pesquisa também contribui expondo falhas encontradas em sistemas do governo e mostrando maneiras de resolver esses problemas.

Para trabalhos futuros, o aprimoramento do questionário e a ampliação do número de participantes da pesquisa são importantes para que se possa obter dados mais sólidos que sirvam para representar de forma mais concreta a realidade das instituições públicas e dos seus funcionários.

REFERENCIAS

ACM. **Código de ética e conduta profissional da ACM.** Disponível em: < http://www.acm.org/code-of-ethics/>. Acesso em: 25 set. 2018.

ANDRADE, M.M. **INTRODUÇÃO À METODOLOGIA DO TRABALHO CIENTÍFICO.** 10.Ed. São Paulo. 2010.

ARAUJO, Regina Borges. **Computação Ubíqua, Princípios, Tecnologia e Desafios** – XXI Simpósio Brasileiro de Redes de Computadores. 2003. Disponível em <http://www.professordiovani.com.br/rw/monografia_araujo.pdf>. Acesso: 20 de out. 2018.

AVAST. **O que é um *Sniffer***. 2018. Disponível em: <www.avast.com/pt-br/c-sniffer>. Acesso em: 19 out. 2018.

BARROS, A. J. P; LEHFELD, N. A. S. **Projeto de Pesquisa: Propostas Metodológicas.** 23. Ed. Petrópolis, RJ. 2014.

BENETT, W.L. ***"Branded Political Communication: lifestyle Politics, Logo Campaigns, and the Rise of Global Citezenship".*** *In:* MICHELETTI, Michele, FOLLESDAL, Andreas, and STOLLE, Dietlind (eds). *Political Consumerism-Global Responsibility in Action. Cambridge: Cambridge University Press*, 2013.

BORGES, Job Diógenes Ribeiro. **Governo Eletrônico e Software Livre: A Tecnologia com a Cidadania a Serviço da Comunidade.** Disponível em: <www.buscalegis.ccj.ufsc.br/>. Acesso em: 03 nov. 2018.

BRASIL. **DataPrev**. Disponível em: <https://portal.dataprev.gov.br/>. Acesso em: 5 out.2018.

BRASIL. **Guia Livre**. Referência de migração para software livre do governo federal. Brasília. 2005. Disponível em: <https://www.governodigital.gov.br/documentos-e-arquivos/GuiaLivrev1-02.pdf/>. Acesso em: 10 out. 2018.

BRASIL. Lei no. 9.609/98, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. **Diário Oficial da União**, Brasília, DF. 19 de fev. 1998. Seção 1. Disponível em: <www.planalto.gov.br/ccivil_03/leis/L9609.htm/>. Acesso em: 10 out. 2018.

BRASIL. **Serpro**. Disponível em: <http://www.serpro.gov.br/>. Acesso em: 5 out. 2018.

BSA. **Mercado das sombras**. Estudo global de pirataria de software BSA 2011. Mai 2012. Disponível em: <www.assoft.org/uploads/docs/2011GlobalPiracyStudy_pt.pdf>. Acesso em: 11 out. 2018.

CANTÚ, E. **Redes de computadores e internet.** São José. Primavera. 2003. Disponível em: <https://docente.ifrn.edu.br/rodrigotertulino/disciplinas/2016.2/arquitetura-de-redes-de-computadores/resumo-livro-do-kurose/> Acesso em: 28 set. 2018.

CORTES, P. L. **Administração de Sistemas da Informação**.1. Ed. São Paulo: Saraiva. 2007.

ENGHOLM JR, H. **A engenharia de software na prática**. 1. Ed. São Paulo. 2010.

FERNANDES, L. **Conheça os principais pilares da segurança da informação**. Jan. 2018. Disponível em: <https://suntech.com.br/artigos/principais-pilares-seguranca-informacao/>. Acesso em: 15 out. 2018.

FERREIRA, A.B.H. **mini Aurélio XXI:** o minidicionário da língua portuguesa. 4. ed. rev. ampl. Rio de Janeiro: Nova Fronteira, 2001.

FONCECA FILHO, C. **História da computação: o caminho do pensamento e da tecnologia**. Porto Alegre. EDIPUCRS. 2007.

FRANÇA, L. C. M. **LETRAMENTO DIGITAL E PARTICIPAÇÃO SOCIAL**: o discurso midiático da Microsoft. In: Wilton James Bernardo-Santos; Fabio Elias Verdiani Tfouni. (Org.). Discurso, mídia e ensino: entre cruzamentos de abordagens. 1.Ed. Aracaju-SE: Editora da UFS, 2015.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

HINDUJA, Sameer. ***Trends and Patterns Among Online Software Pirates***. *Ethics and Information Technology*, v. 5, pp. 49-61, 2003.

KASPERSKY. **Fatos e perguntas frequentes sobre vírus de computador e malware. 2018**. Disponível em: <www.kaspersky.com.br/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>. Acesso em: 19 out. 2018.

ORRICO JR, H.; PALETTA, F. **Pirataria de software**. 2. Ed. São Paulo. 2004.

PEITZ, Martin; WAELBROECK, Patrick. ***Piracy of Digital Products: A Critical Review of the Theorical Literature. Information Economics and Policy***, v.18, p. 449-476, 2009.

PHAU, Ian; NG, James. ***Predictors of Usage Intentions of Pirated Software****. Journal of Business Ethics, published on line,* 22 oct. 2009.

PLANTIER, R. D. **O primeiro software criado na história**. Disponível em: < http://tecnologia.culturamix.com/tecnologias/o-primeiro-software-criado-historia-da-informatica/>. Acesso em: 10 set. 2018. PORTALMS. **Pirataria de software cresce no mundo, mas cai no Brasil**. Disponível em:<http://www.portalms.com.br/noticias/Pirataria- de-software- cresce-no-mundo-mas-cai-no-Brasil/Brasil/Tecnologia/35333.html>

PRESSMAN, R. S. **Engenharia de Software**. 6. Ed. Rio de Janeiro: McGraw-Hill, 2006.

PRESSMAN, Roger S. **Engenharia de Software**.6. Ed. São Paulo: Makron Books, 2007.

PRODANOV, C. C; FREITAS, E. C. **METODOLOGIA DO TRABALHO CIENTÍFICO: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico.** 2 Ed. 2013. Novo Hamburgo, RS. 2013.

RODRIGUES, William Costa. **Metodologia Científica**, 2007. Disponível em:<http://www.academia.edu/download/33851445/metodologia_cientifica.pdf> . Acesso em: 28 mai. 2019.

ROHR, A. **Como a pirataria pode fazer seu computador ser infectado por vírus**. Disponível em:<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-pirataria-pode-fazer-seu-computador-ser-infectado-por-virus.html/>. Acesso em: 16 out. 2018.

RUTTER, Jason; BRYCE, Jo. ***The Consumption of Counterfeit Goods****: 'Here Be Pirates?'. Sociology*, v. 42, pp.1146-1164, 2008.

SCHWARTZ, M. S. ***A code of ethics for corporate code of ethics****. Journal of Business Ethics. Kluwer Academic Publishers*, v.41, p.27-43, 2002.

SHORE, Barry; VENKATACHALAM, A.R.; SOLORZANO, Eleanne; BURN, Janice M.; HASSAN, Syed Zahoor; JANCZEWSKI, Lech J. ***Softlifting and Piracy: Behavior Across Cultures****. Technology in Society*, v. 23, pp. 563-581, 2001.

THOENIG, Jean-Claude. **A avaliação como conhecimento utilizável para reformas de gestão pública**. Revista do Servidor Público. Ano 51, n.2. 2000. Brasília. ENAP.

WIRESHARK. **Sobre o *Wireshark***. 2018. Disponível em:< https://www.wireshark.org/>. Acesso em: 19 out. 2018.

YIN, R. K. **Estudo de caso: Planejamento e métodos.** Tradução Daniel Grassi. 2. Ed. Porto alegre: Bookman, 2001.