INSTITUTO FEDERAL GOIANO – CAMPUS CERES
BACHARELADO EM SISTEMAS DE INFORMAÇÃO
GILSON SOARES DE SOUSA

SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS: UMA ANÁLISE COMPORTAMENTAL SOBRE O WHATSAPP E INSTAGRAM

CERES - GO
2021

GILSON SOARES DE SOUSA

SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS: UMA ANÁLISE COMPORTAMENTAL SOBRE O WHATSAPP E INSTAGRAM

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação do Campus Ceres do Instituto Federal Goiano, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação sob orientação do Prof. Me. Roitier Campos Gonçalves.

CERES – GO

2021

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

SSO725s

Sousa, Gilson Soares de
Segurança da Informação em Aplicativos Móveis: Uma análise comportamental sobre o WhatsApp e Instagram / Gilson Soares de Sousa; orientador Roitier Campos Gonçalves. -- Ceres, 2021.
70 p.

TCC (Graduação em Bacharelado em Sistemas de Informação) -- Instituto Federal Goiano, Campus Ceres, 2021.

1. Acessibilidade à Informação. 2. Políticas de Privacidade . 3. Tecnologia da Informação. 4. Segurança da Informação. I. Gonçalves, Roitier Campos , orient. II. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

INSTITUTO FEDERAL
Goiano

Repositório Institucional do IF Goiano - RIIF Goiano
Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese
[ ] Dissertação
[ ] Monografia – Especialização
[X] TCC - Graduação
[ ] Produto Técnico e Educacional - Tipo: _____
[ ] Artigo Científico
[ ] Capítulo de Livro
[ ] Livro
[ ] Trabalho Apresentado em Evento

Nome Completo do Autor: Gilson Soares de Sousa
Matrícula: 2017103202030015
Título do Trabalho: SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS: UMA ANÁLISE COMPORTAMENTAL SOBRE O WHATSAPP E INSTAGRAM

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique: _____
_____
Informe a data que poderá ser disponibilizado no RIIF Goiano: 13/08/2021
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [X] Sim [ ] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O referido autor declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Ceres, 12 de agosto de 2021.

(Assinado Eletronicamente)

Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

(Assinado Eletronicamente)

Assinatura do orientador: Roitier Campos Gonçalves (2891401)

Ceres, 12 de agosto de 2021.

Documento assinado eletronicamente por:

- **Gilson Soares de Sousa**, **2017103202030015 - Discente**, em 12/08/2021 14:11:56.
- **Roitier Campos Goncalves**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 12/08/2021 13:27:15.

Este documento foi emitido pelo SUAP em 12/08/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 298884
Código de Autenticação: 7583fe4407

INSTITUTO FEDERAL GOIANO
Campus Ceres
Rodovia GO-154, Km.03, Zona Rural, None, CERES / GO, CEP 76300-000
(62) 3307-7100

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos 30 dias do mês de julho do ano de dois mil evinte um, realizou-se a defesa de Trabalho de Curso do acadêmico GILSON SOARES DE SOUSA, do Curso de bacharelado em Sistemas de Informação, matrícula 2017103202030015, cujo título é "SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS: UMA ANÁLISE COMPORTAMENTAL SOBRE O WHATSAPP E INSTAGRAM ". A defesa iniciou-se às 20 horas e 07 minutos, finalizando-se às 22 horas e 05 minutos. A banca examinadora considerou o trabalho APROVADO com média 8,5 no trabalho escrito, média 9,0 no trabalho oral, apresentando assim média aritmética final de 8,75 pontos, estando o(a) estudante APTO para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, o(a) estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

(Assinado Eletronicamente)
Roitier Campos Gonçalves
Presidente da Banca

(Assinado Eletronicamente)
Regina Paiva Melo Marin
Membro 1 Banca Examinadora

(Assinado Eletronicamente)
Josimar Viana Silva
Membro 2 Banca Examinadora

Documento assinado eletronicamente por:

- **Josimar Viana Silva**, **Josimar Viana Silva - Outros - Instituto Federal Goiano - Campus Ceres (10651417000410)**, em 02/08/2021 15:02:41.
- **Regina Paiva Melo Marin**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 02/08/2021 12:55:03.
- **Roitier Campos Goncalves**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 02/08/2021 11:10:48.

Este documento foi emitido pelo SUAP em 30/07/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 295401
Código de Autenticação: ac88b6aa08

INSTITUTO FEDERAL GOIANO
Campus Ceres
Rodovia GO-154, Km.03, Zona Rural, None, CERES / GO, CEP 76300-000
(62) 3307-7100

À memória do meu pai que sempre enchia os olhos de lágrimas quando alguém elogiava seus filhos, que eram seu maior orgulho.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e seus inúmeros privilégios, por ter me agraciado com o dom do aprendizado e poder transpor as diversidades que nos vem durante uma graduação, à minha mãe Maria Zita Soares de Souza, ao meu Pai João Gonçalves de Souza (*in memoriam*), os quais sempre me encorajaram e incentivaram-me a buscar pelos valores morais e conhecimentos.

Aos meus irmãos que sempre me apoiaram durante essa longa caminhada acadêmica, por mais que esta não acaba por aqui, em especial à minha irmã Gilsirene Soares de Souza, que por várias vezes me estendia a mão ajudando com várias correções desta pesquisa e instigando copiosamente a seguir por esse infinito caminho da tecnologia.

Imensamente grato à Professora Doutora Jaqueline Alves Ribeiro que conduziu com maestria a primeira coordenação deste curso, entre tantas outras disciplinas, inclusive as de TCI e TCII que por inúmeras vezes me conduzia, até mesmo fora de hora, finais de semanas, feriados e estava sempre disposta a sanar as dúvidas, não medindo esforços para que esse trabalho fosse realizado.

Ao meu orientador Professor Mestre Roitier Campos Gonçalves, que como um ser iluminado foi me norteando durante toda a escrita e preparação desde trabalho, sempre atentos aos e-mails e mensagens que por mim lhe eram enviados constantemente e de toda a atenção, a resposta era instantânea. Infelizmente não pudemos ter contato presencial por causa do crítico momento de pandemia do COVID-19, porém, aceitou o convite para me orientar nesse trabalho e suas orientações foram de valia imensurável. Além de orientador, criamos um vínculo de amizade que por mim será lembrada com imensa gratidão por toda a existência.

Não poderia deixar de agradecer ao Professor Mestre Rangel Rigo, que foi um dos grandes responsáveis pela ajuda na escolha deste tema, foi a primeira pessoa com quem comentei sobre a escolha desta linha de pesquisa e também, através de uma de suas disciplinas, neste cenário, a de Segurança e Auditoria da Informação, que foi de onde despertou o interesse pelo âmbito da Segurança da Informação e assim, depois de muito afunilamento, surgiu a escolha do tema deste trabalho.

À minha esposa Marlene Graciana Soares, que sempre me deu apoio durante a caminhada acadêmica e com muita sabedoria, nunca impôs condições para que pudesse trilhar o caminho do conhecimento, sempre compreendendo o porquê ia dormir às madrugadas, estudando durante toda essa graduação.

Aos meus colegas da segunda turma do curso de Bacharelado em Sistemas de Informação do Instituto Federal Goiano – Campus Ceres, pela união, pelos momentos de descontração, entre tantos outros que ficarão para sempre guardados na memória, aos que por algum motivo pararam durante o caminho e também aos que seguimos juntos desde o princípio do curso, até o final, os quais não os vejo como concorrentes de mercado e sim colegas de profissão.

Sinto-me honrado e imensamente grato aos Professores Prof.ª PhD Regina Paiva Melo Marin e Prof. Me. Josimar Viana Silva que carinhosamente aceitaram o convite para comporem a banca examinadora deste Trabalho de Conclusão de Curso, e sou absolutamente certo que seus conhecimentos trarão uma riqueza imensurável ao conteúdo deste trabalho.

“Aprender é, de longe, a maior recompensa”.

William Hazlitt

RESUMO

A realização deste trabalho adveio com a primordialidade de resguardar a segurança da informação dos usuários de aplicativos em dispositivos móveis. Entende-se que no transcorrer do tempo, são recorrentes os casos de vazamentos de informações que têm ocorrido por meios de softwares que na maioria são agregados, de certa maneira, à rede social. E por excessivas vezes, os possuidores da informação não têm conhecimentos de tal situação. No decurso deste trabalho foi realizada uma pesquisa exploratória, entre usuários, feita por meio de um formulário online, fazendo uso do Google Forms e compartilhado com um público específico de pessoas ligadas à informática e tecnologia de modo geral. O compartilhamento foi feito através de grupos de WhatsApp e Telegram e envios avulsos, para coletar informações de comportamentos de usuários diante do uso dos aplicativos WhatsApp e Instagram, bem como nas redes sociais de modo geral. Foram abordadas questões referentes à exposição de dados pessoais, informações comerciais, localização nos perfis dos aplicativos, armazenamento de senhas em navegadores de internet, envio de dados bancários por mensagens de texto ou imagens através destes aplicativos e demais informações que possam comprometer a confidencialidade dos dados. A seleção destes aplicativos foi realizada com base nas buscas de dados nas lojas Apple Store e Play Store, fazendo uso de termos e palavras chaves que reportassem aplicativos com a funcionalidade de emissão e recebimento de mensagens de modo geral. Foram analisadas as políticas de privacidade de cada aplicativo comparando com as normas da NBR ISO/IEC 27001. Seguidamente, os dados coletados passaram por análise e demonstrados no decorrer do trabalho. Logo após foi feito uma análise descritiva e detalhada dos dados coletados baseados nas respostas do formulário de pesquisa. Em seguida foram feitos cruzamento desses dados para inferir os resultados demonstrados em gráficos e concluímos que 33% dos respondentes da pesquisa são solteiros(as), do sexo masculino, moram na cidade, salvam as senhas nos navegadores de internet e são os que mais acessam as redes sociais usando internet pública.

Palavras-chave: Acessibilidade à Informação. Políticas de Privacidade Segurança da Informação. Tecnologia da Informação.

ABSTRACT

The accomplishment of this work came with the primordiality of safeguarding the information security of the users of applications on mobile devices. It is understood that over time, cases of information leaks that occur through software that are mostly added, in a way, to the social network are recurrent. And all too often, the information holders are not aware of such a situation. In the course of this work, an exploratory research was carried out among users, made through an online form, using Google Forms and complete with a specific audience of people connected to information technology and technology in general. The sharing was done through the WhatsApp and Telegram groups and separate environments, to collect information on the behavior of users when using WhatsApp and Instagram applications, as well as on general social networks. Issues related to the exposure of personal data, business information, location in application profiles, password storage in internet browsers, sending bank data via text messages or images through these applications and other information that compromise data confidentiality were addressed. The selection of these applications was carried out based on data searches in the Apple Store and Play Store stores, using terms and keywords that report applications with functionality for sending and receiving messages in general. The privacy policies of each application were analyzed in comparison with the standards of NBR ISO / IEC 27002. Then, the collected data underwent analysis and demonstrated during the work. Afterwards, a descriptive and detailed analysis of the collected data based on the answers of the survey form was carried out. Then, data were cross-checked to infer the results shown in graphs and we concluded that 33% of the survey respondents are single, male, live in the city, save passwords in internet browsers and are the ones who access the most like social networks using public internet.

Keywords: Accessibility to Information. Privacy Policies Information Security. Information Technology.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SÍMBOLOS

ABNT - Associação Brasileira de Normas Técnicas

EMBRATEL - Empresa Brasileira de Telecomunicações

ENIAC - Electronic Numerical Integrator And Computer

FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo

IEC - Comissão Eletrotécnica Internacional

ISO - Organização Internacional de Normalização

LNCC - Laboratório Nacional de Computação Científica

RENPAC - Rede Nacional de Comunicação de Dados por Comutação de Pacotes

SMS - Short Message Service (Serviço de Mensagem Curta)

UFRJ - Universidade Federal do Rio de Janeiro

SÚMARIO

1. INTRODUÇÃO

Com o avanço da tecnologia, os dispositivos e instrumentos como máquinas computadoras, anteriormente, eram utilizados apenas por matemáticos e profissionais das ciências exatas, e graças a esse avanço, a cada dia os equipamentos mostram maior acessibilidade por se tornarem disponíveis, visto que, a portabilidade vem sofrendo avanços no decorrer dos anos.

Como é o caso dos hardwares que outrora em sua forma física contavam com objetos que ocupavam maiores dimensões como o primeiro computador a ser construído chamado de ENIAC *(Electronic Numerical Integrator And Computer)* que segundo o site Tecnoblog (2021), tinha medidas de 30 toneladas e ocupava uma dimensão de 180 m² de área construída.

Em se tratando de hardwares, o custo benefício vem sendo objeto de atração, ganhando destaques a cada tempo que se modernizam, com isso, os valores se tornam mais alcançáveis. Com a valorização das moedas correntes, esses valores sofrem constantes alterações e não têm deixado de ser objeto de consumo e necessidade entre os entusiastas e dependentes da tecnologia. Assim como os softwares que vêm conquistando o mercado em alta escala de desenvolvimento, sendo cada vez mais independentes de plataforma ou sistemas operacionais.

Diante disto, pela logicidade, quanto mais acesso à informação se tem, mais vulnerabilidade tem a oferecer. Portanto, a permanente busca pela segurança dessas informações só tende a crescer a cada dia. Dessa maneira graças ao progresso do acesso à informação, surge a possibilidade da computação em nuvem, que tem aumentado notadamente o uso de novas ferramentas de trabalho, que transformou uma tendência em realidade.

A computação em nuvem abriu uma gama de possibilidades quanto aos variados serviços que dela dependem. Para que haja segurança da informação durante o acesso às aplicações, faz-se necessário a política de privacidade, que tem como principal função assegurar ao usuário que seus dados serão preservados impossibilitando o acesso indevido.

Segundo Beal (2005), “a definição de segurança da informação está relacionada a práticas de proteger a informação de ameaças que possam comprometer sua integridade, disponibilidade e confiabilidade”.

De acordo com Oliveira et al. (2012), O conceito de segurança da informação está diretamente ligado com à proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização, visto o que remete a ser proteção da informação contra ataques que possam comprometer a integridade dos dados, tanto quanto sua confiabilidade e disponibilidade que são parte dos pilares da segurança da informação. Assim como dispõe a norma NBR ISO 27002:2013, que pressupõe o conteúdo e questionamentos importantes que deverão conter nos termos de política de privacidade.

Deste modo, o tema aqui explanado é baseado no comportamento proveniente de aplicativos móveis que exigem o acesso à galeria de fotos, permissão para acessar a localização do dispositivo e acesso ao microfone para que possa prosseguir com a sua instalação.

Não tendo ciência, o usuário pode estar cedendo os dados para o compartilhamento em massa ou até mesmo a comercialização de informações. Segundo notícia do Jornal Nacional (2021), em seu portal oficial de notícias g1.com, em 10 de fev. 2021, a empresa de segurança cibernética Psafe relata que mais de 100 milhões de brasileiros tiveram os dados expostos por meio de aplicativos de celulares. Entre os dados vazados estão CPF, número de celular, tipo de conta telefônica, minutos gastos em ligação e outros dados pessoais. “As primeiras suspeitas são de que os dados seriam de duas operadoras de telefonia”. Ao todo, foram 102.828.814[1] números vazados, segundo a empresa.

Por fim, como este, são notórios constantes vazamentos de dados percorrendo pela internet em todo o mundo e diversos dados podem ser oriundos de aplicativos de comunicação ou entretenimento, a modo que várias empresas desenvolvedoras de aplicativos atraem o usuário a fazer o download, oferecendo diversão coletiva. Porém, por trás, está a coleta de dados em massa, com pedido de permissão para acessar a câmera e microfone do smartphone, acesso à biblioteca de fotos entre tantos outros meios de acesso como é o caso do Aplicativo *FaceApp* que de acordo com a revista eletrônica Veja (2020), o app lançado em julho daquele ano “a princípio, o temor se dá pelo fato da tecnologia de reconhecimento facial que

[1] G1.com. Jornal Nacional. Empresa diz que mais de 100 milhões de brasileiros tiveram dados de celulares expostos, 2021.

permite as edições na face ser uma ferramenta usada principalmente para a autenticação de senhas, e ser, sem dúvidas, um registro biométrico”[2].

Ainda segundo a Revista Veja (2020), trata-se de uma das maneiras mais comuns para que, um aplicativo possa coletar dados e esses dados possam ser cedidos para terceiros, pois ao instalar o aplicativo, uma lista de permissões necessárias é sugerida ao usuário para que haja o funcionamento adequado do mesmo. Dado as permissões exigidas, abre-se uma porta de comunicação entre o smartphone e os servidores das empresas, que uma vez em posse disso, conseguem traçar um perfil virtual dos usuários.

Com base nisso, o principal objetivo no decorrer deste trabalho, será analisar as políticas de privacidade dos aplicativos de comunicação, bem como se encontram em concordância com as normas de segurança da informação estabelecidas na NBR ISO 27001. A escolha do tema originou-se nas constantes ocorrências em que percebe vazamentos de dados na internet, que podem ser resultado de ciberataques em diversas regiões do mundo.

Segundo BELIC (2021), desenvolvedores de aplicações maliciosas que objetivam a captura de informações por diversos meios de invasões, sendo uma das mais comuns a engenharia social conhecida como *phishing*[3], vista normalmente em recebimentos de e-mails.

E fundamentado nisso, buscamos entender se os motivos desses vazamentos são oriundos do comportamento dos usuários diante do uso de aplicativos de comunicação e/ou da exposição de dados nos perfis das redes sociais.

Os ataques cibernéticos se dão por ser uma tática semelhante a uma pescaria, onde o hacker lança a isca, muitas vezes usando um anúncio falso, oferta de produtos famosos pertencentes às grandes marcas, para assim, tentar ganhar credibilidade do usuário. Uma vez atraído, ao clicar no anúncio, é redirecionado a uma página falsa, como exemplo uma loja virtual com preços atrativos aos internautas que despertam interesse em comprar (BELIC, 2021).

---

[2] LOPES, ANDRE. Como se proteger de aplicativos que exageram na coleta de dados pessoais Leia mais em: https://veja.abril.com.br/tecnologia/como-se-proteger-de-aplicativos-que-exageram-na-coleta-de-dados-pessoais/.

[3] PHISHING é um golpe proveniente de e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos (KASPERSKY, 2021).

A partir deste ponto começam a coletar informações confidenciais, por exemplo, *login* e senha da loja, dados bancários, números do cartão de crédito que são inseridos na tentativa da compra daquele produto. E na maior parte das vezes, esses dados são comercializados ou usados para fins criminosos de modo que são feitas compras usando tais informações[4].

Nesta feita, embasamos nossa pesquisa nas políticas de privacidade e na segurança dos dados inseridos nos aplicativos mobile. Os quais têm abrangente relevância quando se tratam de agilidade e praticidade que atendem as requisições dos usuários, oferecem entretenimentos, serviços de comércio eletrônico, oferta e procura de empregos e uma infinita possibilidade de acesso à informação, comunicação simultânea, portais de notícias, entre outros.

No entanto*,* atentaremos ao que diz as políticas de privacidade quanto às garantias da segurança da informação dos aplicativos WhatsApp e Instagram. No explanar, será abordado sobre a criptografia estendida pelos aplicativos, explorar as funcionalidades da criptografia ponta-a-ponta e como se comporta a segurança de redes e exploração das técnicas usadas para proteção do tráfego de dados.

2. JUSTIFICATIVA

Atualmente, a busca pela informação vem se tornando uma propriedade de alta pertinência. Visto que é com base na informação que são geradas as tomadas de decisões e novos objetivos de negócios assomam a cada dia.

Sendo assim, com o avanço da tecnologia, o acesso à informação vem se tornando cada dia mais expansível, a começar por receber uma notificação na tela de um smartphone por meio de aplicativos de conversas simultâneas. E isso faz com que a expansão da informação venha a tomar grandes proporções e pareado a esse crescimento, surge também a necessidade de as proteger contra acessos indevidos a essas informações.

Deste modo, Sêmola (2014, p. 43) classifica a informação como um "conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou

[4] ROCHA, Douglas. ENGENHARIA SOCIAL: COMPREENDENDO ATAQUES E A IMPORTÂNCIA DA CONSCIENTIZAÇÃO, 2021.

máquinas". Deste modo, ratifica-se, então, que esse processo de envio e recebimento de dados pode ser caracterizado como uma troca de informações de modo a gerar comunicação entre as partes, de outra maneira, informações de relevante importância dentro da empresa e em razão disso, é necessário a proteção dos dados.

Cada pessoa sabe a importância que tem a informação que ela detém, tal como um entregador de correspondência entrega um envelope que a seus olhos não passa de um envelope qualquer, contudo, para alguém que tenha conhecimento prévio do que se refere o conteúdo daquele envelope, alguém que esteja esperando por ele, o seu conteúdo pode ser de tamanha importância, como menciona Mitnick e Simon (2003, p 21), “Assim como as peças de um quebra-cabeça, cada informação parece irrelevante sozinha. Porém, quando as peças são juntadas, uma figura aparece”.

Já, segundo Rosa (2014), a informação sigilosa é aquela sujeita, em caráter temporário, à restrição de seu acesso ao público em geral por conta de sua natureza para o interesse da segurança do Estado ou da sociedade. Em tal caso, se torna fundamental que as informações de cunho sigiloso sejam utilizadas por pessoas com conhecimento e habilidade.

Diante desta situação, a segurança torna-se um dos principais impasses quando se refere à informação, tornando primordial para se ter um gerenciamento proveitoso em diversos nichos e esferas.

3. OBJETIVOS

3.1 Objetivo Geral

Analisar o percurso da segurança da informação oferecida pelos aplicativos de comunicação, bem como os conceitos substanciais que abrangem as abstrações e normas de segurança, de forma que haja garantia de segurança dos dados, no seu compartilhamento em variados ambientes computacionais para se chegar ao objetivo que destina esse trabalho.

3.2 Objetivos Específicos

Analisar o comportamento dos usuários nas redes sociais;

Verificar se vazamentos de dados na internet são provenientes de atitudes de usuários;

Analisar os termos de segurança dos aplicativos com a NBR ISO 27001.

4. METODOLOGIA DE PESQUISA

Para a evolução desta dissertação foi realizada pesquisa de exploração de dados, para respaldar os conceitos e temas que serão discutidos no decorrer deste trabalho, como segurança da informação, tecnologia da informação e virtualização de dados.

Segundo Gil (2009), a pesquisa é desenvolvida através dos conhecimentos disponíveis, com a utilização de técnicas, métodos e procedimentos científicos de forma cautelosa. Trata-se de um processo racional e sistemático buscando responder os questionamentos levantados.

Sendo assim, Gil (2009) presume que a pesquisa bibliográfica é conduzida com base no conteúdo uma vez desenvolvido, embasado em livros e artigos científicos, sendo a parte mais importante deste tipo de pesquisa o poder de obtenção de informação vindo de variadas fontes de conhecimentos. O qual permite que o pesquisador explore conteúdos de forma não superficial que são pertinentes ao objeto em estudo.

A seleção dos aplicativos de dispositivos móveis foi realizada com base nas buscas de dados dos aplicativos da Apple Store e Play Store, fazendo uso de termos e palavras chaves que reportassem aplicativos com a funcionalidade de emissão e recebimento de mensagens e informações como um todo. Foram analisadas as políticas de privacidade de cada aplicativo em comparação com as normas da ABNT ISO/IEC 27002.

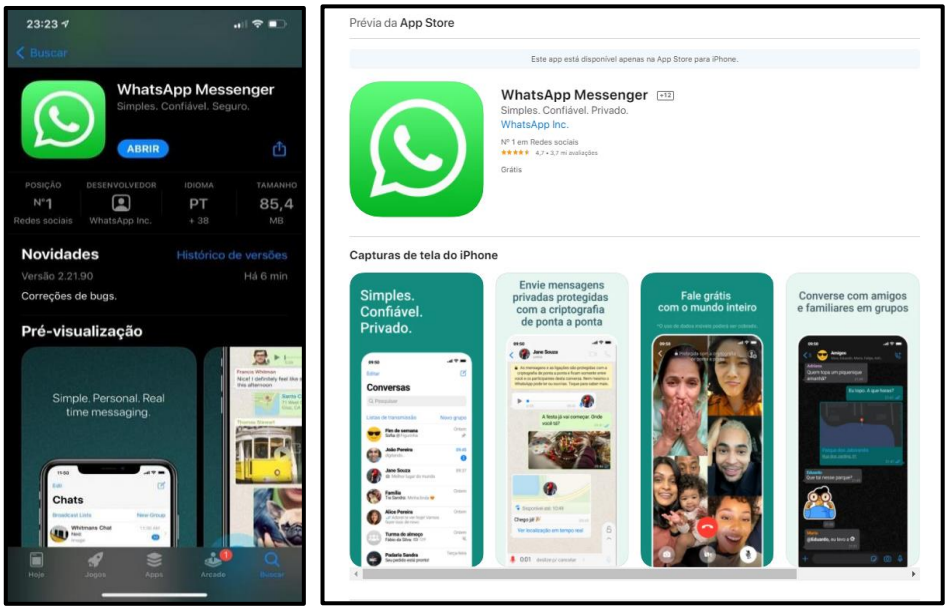
Seguindo as fases da pesquisa, depois da decisão de fazer a busca com os termos que reportassem tais aplicativos em que as principais funcionalidades fossem a mutação de mensagens de texto, imagens, vídeos, videochamadas e o compartilhamento de documentos em diversas extensões em forma de anexo. Foi

possível apontar os dois primeiros resultados de acordo com a relevância dos aplicativos mais procurados nas lojas virtuais Apple Store e Play Store.

Em posse da informação, de acordo com a Apple Store (2021), até a data de 20 de maio de 2021, o aplicativo WhatsApp se encontrava na versão 2.21.90, com tamanho de 85,4MB. O aplicativo gratuito de troca de mensagens e de chamadas de vídeo e de voz é usado por mais de 2 bilhões de pessoas em mais de 180 países, disponível em mais de 38 idiomas, ocupando a posição número 1 na categoria Redes Sociais e com classificação 4,7. Em uma escala de 0 a 5, recomendado para pessoas maiores de 12 anos, somando 3.572.114 (três milhões, quinhentos e setenta e dois mil e cento e quatorze) classificações de usuários.

Neste ínterim, em 20 de maio de 2021, de acordo com a loja de aplicativos Apple Store (2021), o aplicativo Instagram se encontrava na versão 187.0 com tamanho de 155,2MB ocupando a posição número 2 na categoria foto e vídeo e com classificação 4,8. Em uma escala de 0 a 5, recomendado para pessoas maiores de 12 anos, somando 5.616.540 (cinco milhões, seiscentos e dezesseis mil e quinhentos e quarenta) classificações de usuários como mostram as figuras 1 e 2. A Apple Store não disponibiliza a quantidade de download dos aplicativos.

Figura 1: WhatsApp Messenger na Apple Store.



Versão Mobile Versão Desktop

Fonte: Própria (2021)

Figura 2: Instagram na Apple Store.

Versão Mobile Versão Desktop

Fonte: Própria (2021)

Em outra face, embasada na mesma linha de pesquisa, ainda em 20 de maio de 2021, segundo a Google Play (2021), a loja de aplicativos oficial do Google, mantenedora dos aplicativos utilizados no Sistema Operacional Android, o aplicativo WhatsApp se encontrava na versão 2.21.9.15. Lançado em 18 de outubro de 2010, o tamanho em Bytes varia de acordo com o dispositivo[5], ocupando a posição número 1 dos principais aplicativos gratuitos, recebendo classificação 4,0 em uma escala de 0 a 5. Possuindo classificação livre para todas as idades, somando mais de 5 bilhões de downloads e 136 (cento e trinta e seis) milhões de classificações de usuários.

De igual modo, ainda de acordo com a Google Play (2021), o aplicativo Instagram, lançado em 3 de abril de 2012, se encontrava na versão 188.0.0.35.124, o tamanho em Bytes de igual modo ao WhatsApp, varia de acordo com o dispositivo,

[5] A Play Store não define a quantidade de Bytes que contém os aplicativos WhatsApp e Instagram, pois, segundo a loja, varia de acordo com o dispositivo que receberá a instalação. Fonte: https://play.google.com/store/apps/details?id=com.whatsapp&hl=pt_BR&gl=US, https://play.google.com/store/apps/details?id=com.instagram.android&hl=pt_BR.

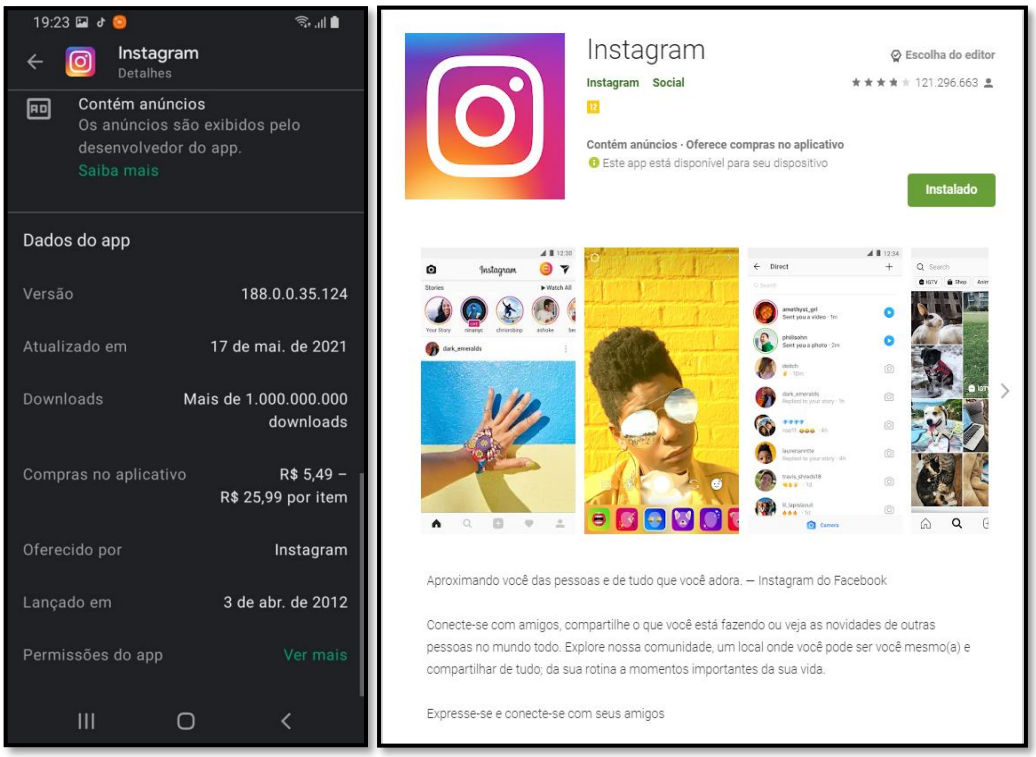
ocupando a posição número 4 dos principais aplicativos gratuitos, recebendo classificação 3,8 em uma escala de 0 a 5. Sendo não recomendado para menores de 13 anos, contendo variados tipos de marketing e oferece compras no aplicativo, somando classificações de mais de 1 bilhão de downloads e 120.005.095 (cento e vinte milhões e cinco mil e noventa e cinco) milhões de classificações de usuários, como mostra as Figuras 3 e 4.

Figura 3: WhatsApp Messenger na Google Play Store.

Versão Mobile Versão Desktop

Fonte: Própria (2021)

Figura 4: Instagram na Google Play Store.



Versão Mobile Versão Desktop

Fonte: Própria (2021)

Nesta senda, para o desenvolvimento desta pesquisa, estes aplicativos os quais apontamos mostraram ser de grande valia para os resultados, sendo que lideram os rankings de maior número de usuários, dando uma vasta percepção no que propomos neste trabalho.

A partir desses aplicativos, a próxima etapa da pesquisa consistiu no ler e avaliar as políticas de privacidade do WhatsApp[6] e Instagram[7], considerando as recomendações descritas nas normas ISO/ABNT 27002, dando maior ênfase às questões que se dizem respeito à segurança da informação.

A partir da pesquisa, para obtermos resultados, foi elaborado um questionário, criado com a ferramenta Google Forms, que consiste em coleta de dados dos

[6] A Política de Privacidade do Aplicativo WhatsApp pode ser conferida em: https://www.whatsapp.com/legal/shops/privacy-policy.

[7] A Política de Privacidade do Aplicativo Instagram pode ser conferida em: https://help.instagram.com/519522125107875

participantes. Após o formulário criado, teve seu link compartilhado de forma individual e em grupos específicos de WhatsApp e Telegram de estudantes de informática e usuários de tecnologias para que o respondessem com a finalidade de elaborar esse trabalho de pesquisa sobre o tema de Segurança da Informação em Aplicativos Móveis. E assim foram coletadas informações durante 15 dias, sendo de 28 de junho a 12 de julho de 2021.

Fundamentado nas informações coletadas foram geradas então as estatísticas, que a partir desta metodologia de criação do formulário online, utilizando da ferramenta Google Forms, o qual foi o recurso desenvolvido para realizar esta coleta de dados. E logo após, analisar os dados, obter estabilidade nas respostas.

Deste modo, o formulário foi composto por 15 questões objetivas e obrigatórias, sendo 11 delas relacionadas exclusivamente à Segurança da Informação em Aplicativos Móveis e 04 questões para coletar a faixa etária, sexo, estado civil e a localidade de residência, bem como saber se o respondente situa em Zona Urbana ou Zona Rural.

Em posse e com base nessas informações, os dados foram filtrados por idade e por sexo de modo que fosse possível explanar qual a faixa etária está menos vulnerável quanto à exposição dos dados durante o uso de aplicativos nas redes sociais. E assim, comprovar se o percentual de vulnerabilidade é maior entre pessoas do sexo masculino ou feminino.

O formulário pôde ser visto e compartilhado através do link: *https://forms.gle/8U79D69MjHeEnkYD8*, e as respostas que obtivemos em relação às perguntas foram de grande importância para colaboração deste trabalho. Deste modo, da Figura 5 até a Figura 10, demonstramos as imagens do formulário de coleta de dados, assim como foi apresentado ao público.

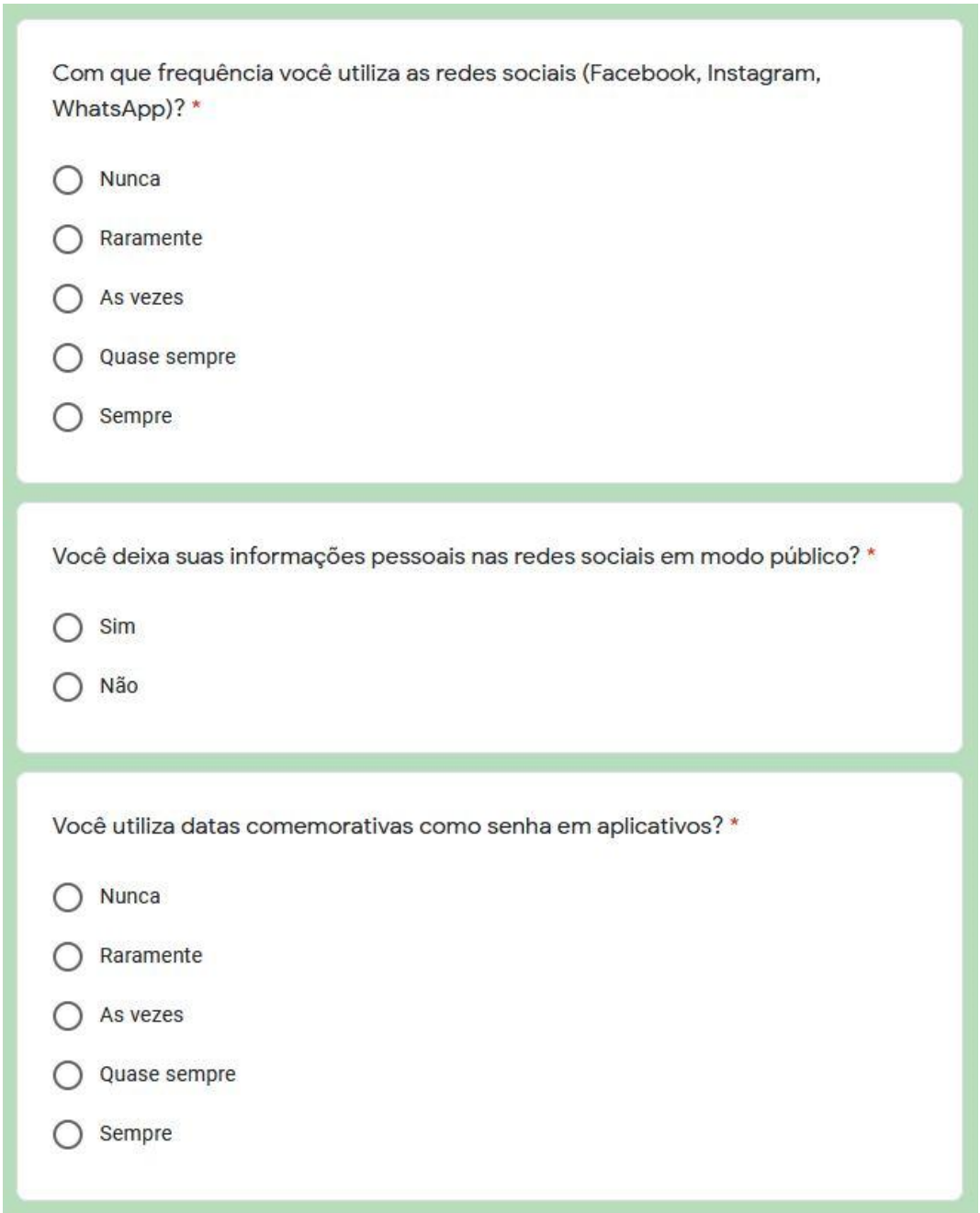
Figura 5: Formulário para coleta da faixa etária dos respondentes.

Fonte: Própria (2021).

Figura 6: Formulário para coleta de estado civil, sexualidade e residência dos respondentes.

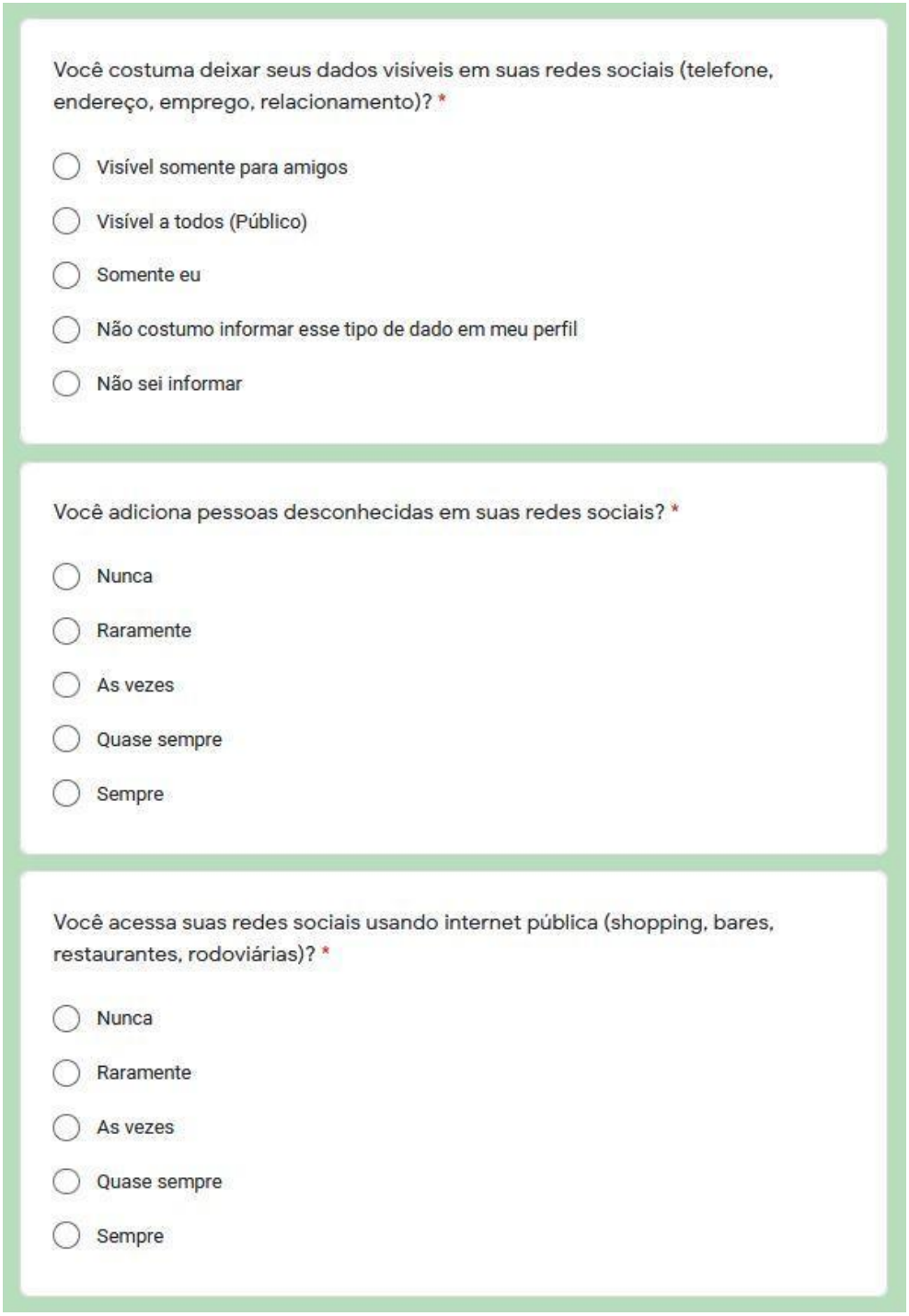
Fonte: Própria (2021).

Figura 7: Formulário de coleta de dados sobre frequência de utilização de redes sociais.



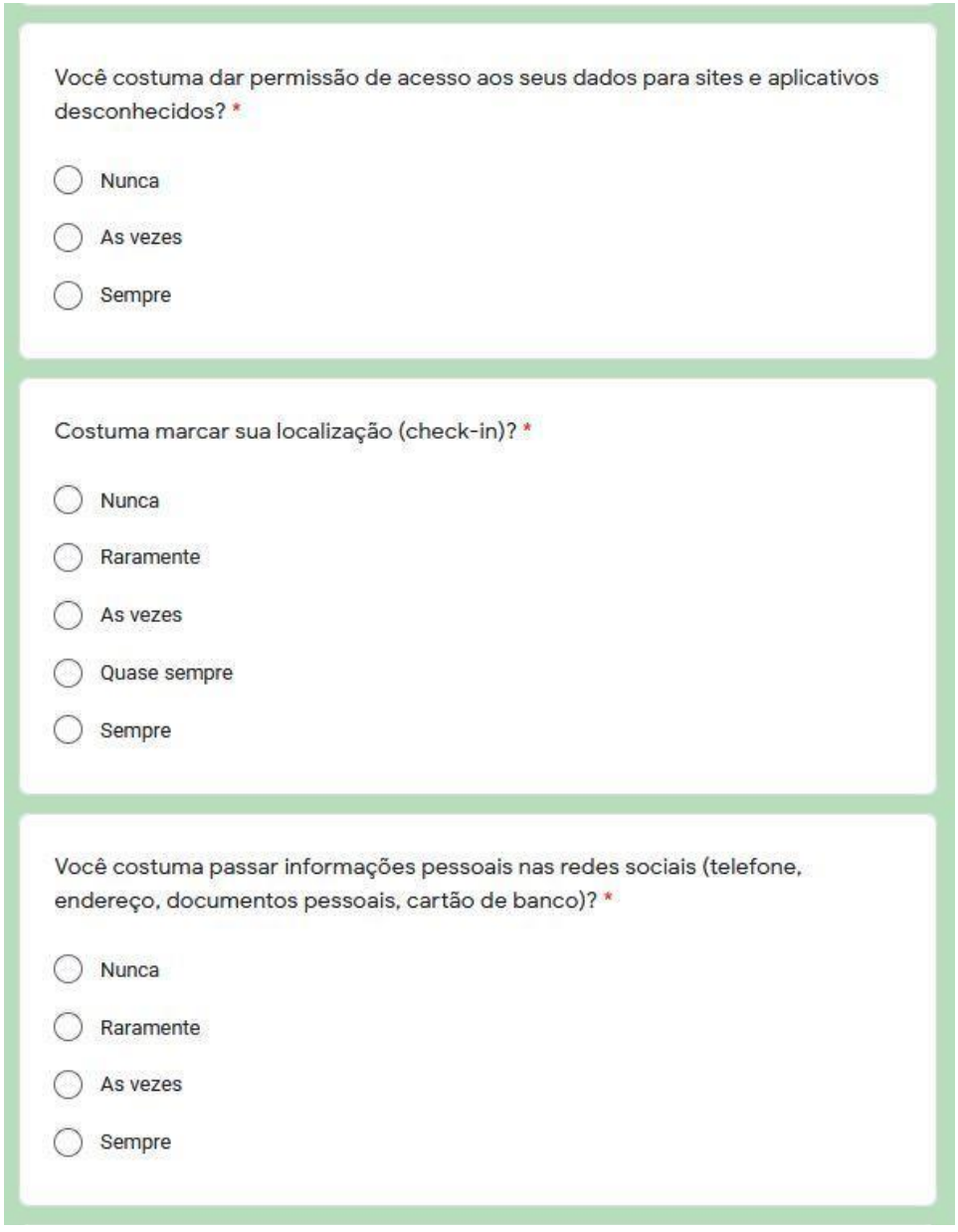
Fonte: Própria (2021).

Figura 8: Formulário de coleta de dados sobre visibilidade de informações, aceitação de perfis desconhecidos e acesso às redes sociais por internet pública.



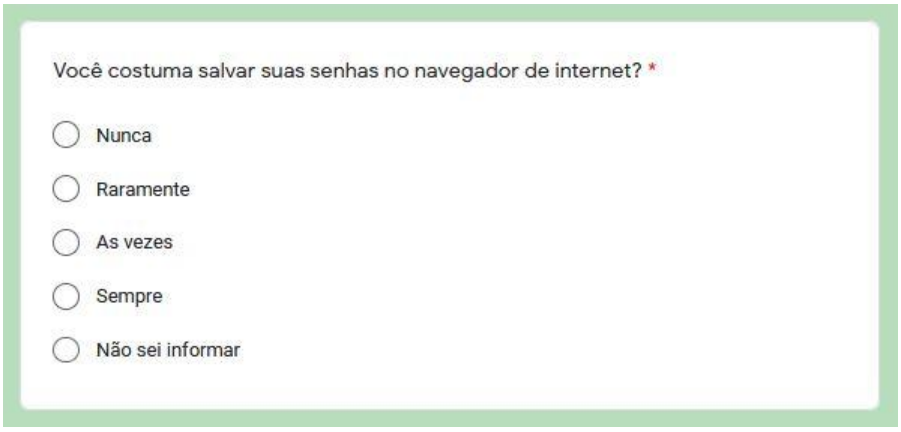
Fonte: Própria (2021).

Figura 9: Formulário de coleta de dados sobre o acesso a sites e aplicativos desconhecidos, disponibilidade de localização e envio de informações pessoais.



Fonte: Própria (2021).

Figura 10: Formulário para coleta de dados sobre o armazenamento de senhas nos navegadores de internet.



Fonte: Própria (2021).

5. FUNDAMENTAÇÃO TEÓRICA

Para que nosso projeto seja solidificado, torna-se indispensável obtermos conhecimentos dos princípios de virtualização de dados e entendermos a maneira que esse processo associa-se à nossa realidade no cotidiano e como percebemos esse desenvolvimento tecnológico e qual a maneira que conduzimos esse processo.

6. SOCIEDADE E A INFORMAÇÃO

De acordo com Pierre Lévy (1996), a definição de virtualização é algo abstrato que simula as características de algo real. Pierre enfatiza ainda que virtual é tudo que não pode ser ou estar presente, apesar de que a virtualização não se deu início com computadores.

Desde que a criação da computação em nuvem, uma imensidão de expectativas tem se criado no âmbito da tecnologia, a virtualização tem se tornado mais habitual e com um alcance mais amplo voltado aos profissionais do setor.

Assim, o doutrinador LÉVY (1996), que a virtualização forma duas esferas nas quais separam o espaço físico e o geográfico, e os relata de seguinte forma:

> Quando uma pessoa, uma coletividade, um ato, uma informação se virtualizam, eles se tornam “não-presentes”, se desterritorializam. Uma espécie de desengate os separa do espaço físico ou geográfico ordinários e da temporalidade do relógio e do calendário. É verdade que não são totalmente independentes do espaço-tempo de referência, uma vez que devem sempre se inserir em suportes físicos e se atualizar aqui ou alhures, agora ou mais tarde. No entanto, a virtualização lhes fez tomar a tangente (LÉVY, 1996, p.21).

Já para Castells (1999), todas as relações, de modo geral, têm seus princípios fundamentados na informação e a capacidade de processar as informações é a principal fonte de conhecimentos. Diante disso, percebe-se a familiarização da sociedade ao fazer uso dessas tecnologias em prol do relacionamento comum, desde a interação pessoal por meio virtual, quanto à exploração dos recursos em prol de si, explorando a tecnologia a seu favor.

Aponta ainda, que um marco na história humana, foi a era da informação de modo geral, pois, a partir desse ponto, se dá início à flexibilidade e a robustez no que se refere a processamento de informação e geração de conhecimento Castells (1999).

No entanto, com o livre acesso a toda essa tecnologia e informação, nota-se a revolução e a frequência com que as pessoas se relacionam e fazem pesquisas acadêmicas. No setor comercial, a modalidade *delivery* vem crescendo constantemente graças aos aplicativos e sites de comércio eletrônico que viabilizam em grande escala a realização desses serviços.

Assim como o acesso às instituições financeiras, bancos que se expandiram migrando grande parte de seus serviços para a plataforma digital fazendo assim, movimentações com agilidade.

Conforme Kunsch (2003) existe uma problemática a ser observada dentro do processo que compreende a informação e a disponibilidade dos dados sendo vista como barreiras que há durante todo esse processo de comunicação tanto pessoal quanto direcionada às máquinas e equipamentos que estabelecem o transporte de informações.

Ainda, Kunsch (2003), enfatiza que o excesso de informação talvez seja a mais atual das barreiras. Grandes volumes de dados, diante à dificuldade da escolha do conteúdo e em diversas vezes está aliado à falta de prioridades, não dando ênfase aos conteúdos de maiores destaques. O que em grande parte causa

confusão com os receptores de informações, complicando a assimilação do que é comunicado e também as informações que virão em sequência.

No entanto, Segundo Kunsch, há também numerosos fatores importantes a serem considerados, principalmente nos dias atuais, entre a imposição de tempo e o consumo nos processos que envolvem a comunicação.

Figueiredo (1987) aponta outra barreira além do excesso de informação e menciona a chamada lei do menor esforço. No que se refere à quando algo pode ser feito de diferentes maneiras, sempre a melhor opção é a que implica o menor gasto de energia, que rege o uso de sistemas de informação. Ou seja, de modo que estes esforços não sejam empregados se não apresentarem facilidade de uso e acesso.

De acordo com Escola (2021), a Internet chegou ao Brasil em 1988*,* por iniciativa da comunidade acadêmica de São Paulo*,* em parceria com a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Universidade Federal do Rio de Janeiro (UFRJ) e Laboratório Nacional de Computação Científica (LNCC). Assim, Escola salienta que somente a partir do final de 1994 houve a expansão comercial, iniciada por um projeto criado pela Empresa Brasileira de Telecomunicações (EMBRATEL).

Partindo daí, foram permitidos os acessos à rede mundial de computadores inicialmente, sendo possível apenas por acesso discado via linha telefônica com o uso de um fax modem. Posteriormente, foi permitido por meio de acesso dedicado via Rede Nacional de Comunicação de Dados por Comutação de Pacotes (RENPAC).

Contudo, só veio ganhar força na década de 1990, quando os primeiros sinais começaram a chegar aos órgãos públicos, escolas, universidades sendo que o acesso era restrito a professores, estudantes e funcionários, e somente aos poucos foi chegando às instituições de pesquisa.

Ainda explanando sobre rede, Castells (2003, p.34-55) diz que a união de quatro concepções, deu à internet uma cultura respectiva, sendo elas a tecnomeritocrática, a hacker, comunitária virtual e a concepção empreendedora.

Conforme Castells, a implantação da rede de internet começou a ter relevância apenas na década de 1990, com o empenho do capital social.

Desde então, começaram a comercializar computadores pessoais com hardwares compatíveis com o ainda pouco acesso à internet, sistemas operacionais até então, de acesso muito restrito a computadores domésticos.

> O ciberespaço (que também chamarei de “rede”) é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo “cibercultura”, especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço (Lévy, 1999, p.22).

Com isso, torna-se notório que o modo de expressão de forma digital vem estimulando a sociedade a obter um amplo entendimento. Usando esse fator, há uma geração de informação, armazenamento, recuperação, processamento e disseminação dos dados tratados, permitindo um maior acesso aos processos[8].

Nesta mesma linha de pensamento, pode se então suscitar que essa gama da informação faz um elo a redes que por um conjunto de módulos e processadores são formadas possuindo as qualidades necessárias para expor o acesso às informações e com isso, podendo distribuir recursos.

Podemos enfatizar que a internet se tornou um amplo sistema de comunicação que estabelece conexão entre redes sociais e corporativas que partilham informações e geram a comunicação entre si formando um *loop* infinito quando se diz respeito à formação de conteúdo acessível a todo instante*,* independente de ambiente físico ou geográfico.

Diante deste cenário, a segurança da informação prioriza a preservação dos pilares Integridade, Disponibilidade e Confidencialidade que pode assegura que a informação seja alcançada somente por quem é autorizado por direito, impedindo assim que seja disseminado de forma desprotegida[9].

6.1 Segurança da informação

Conforme Silva et al (2003), a nomenclatura e o uso do termo Segurança da

[8] OSPINA; PRATES. Tecnologia da informação em pequenas empresas: fatores de êxito, restrições e benefícios. https://www.scielo.br/j/rac/a/vpfnQdJRT5CtbBpN7b7XP9r/?lang=pt. 2004.
[9] Telium Networks. https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao. 2018.

Informação surgiram em meios aos técnicos de informática quando se deu início ao desenvolvimento de sistemas. Daí veio a necessidade de fazer a verificação da segurança dos dados antes de partirem para a distribuição dos sistemas para utilização, mais adiante, com o aumento da produção, os sistemas passaram ser usados em ambientes de rede e com isso, veio o despertar para a certificação quanto a estrutura dos sistemas.

Silva et al (2003) ainda destaca os princípios que se aplica para obter a confiabilidade e alcançar os critérios da segurança da informação como a Relação custo/benefício, Concentração, Proteção em profundidade, Consistência do plano e a Redundância.

6.2 Características da Informação

Para que haja confiabilidade, a informação deve garantir as características essenciais que são chamadas de pilares da segurança informação que, a saber, dentre os mais comuns, são: Confidencialidade, Disponibilidade, Integridade, como já relatamos acima neste trabalho (TELIUM NETWORKS, 2018).

São características que devem ser mantidas porque são os fundamentos que a segurança da informação possui. De acordo com a norma NBR ISO 27002:2005, segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a confirmar a continuidade do negócio, minimizar o risco durante seu ciclo e maximizar o retorno sobre o investimento e as oportunidades de negócio. Deste modo, a norma internacional NBR ISO/IEC 27002:2005, estabelece a segurança da informação como:

> “Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades tais como a autenticidade, responsabilidade, não repúdio e confiabilidade podem estar envolvidos” (ABNT NBR ISO/IEC 27002:2005).

Tratando-se de segurança da informação, é necessário destacar tais pilares, pois todos os feitos que possam envolver qualquer destes será um atentado contra a segurança.

6.3 Integridade

De acordo com Galvão (2015), a integridade garante que as informações são verdadeiras e não são afetadas por nenhum tipo de modificação durante o tempo de seu armazenamento ou percurso caso enviada a um destinatário. Ou seja, a continuação da exatidão, consistência e confiabilidade das informações durante o seu ciclo de vida garantindo que as informações não sofreram alteração no decorrer do percurso, assim sendo, todos os dados precisam ser mantidos como foram produzidos.

Deste modo, nota-se o quanto é fundamental que as informações sejam disseminadas e se mantenham estáveis do mesmo modo ao qual foram produzidas para que não haja alterações em seu conteúdo que possa avariar sua integridade[10].

Deste modo, se tratando da importância da veracidade de informações que são trocadas no interior de uma instituição, manter a integridade é um fator imprescindível. Pois a falta dela, a torna ineficaz e inconfiável podendo ser um fator extremamente agravante diante das tomadas de decisões mais importantes, gerando arruinação patrimonial ou financeira à instituição.

Ainda de acordo com Galvão (2015), é essencial preservar a integridade dos dados para que os sistemas executem suas rotinas corretamente e sem falhas por inconsistência de dados. Além de que as informações trocadas entre dispositivos têm de chegar ao seu destino mantendo com a mesma proporção que foram enviadas para que não haja comprometimento na comunicação no decorrer do seu percurso, o que pode causar graves falhas na execução das ações.

6.4 Disponibilidade

Segundo Galvão (2015), disponibilidade é a garantia de que a informação estará livre quando a pessoa devidamente autorizada a ter acesso fizer requisição para o seu uso. No entanto, a interrupção deste pilar se dá quando a informação não está ao alcance dos destinatários impedindo assim que a informação seja acessada no instante em que for essencial fazer o seu uso.

[10] MELLO, Alessandra. Os três pilares da segurança da informação. 2021. Disponível em: https://ead.catolica.edu.br/blog/pilares-da-seguranca-da-informacao. Acesso em: 24 jul. 2021.

De acordo com a norma NBR ISO/IEC 27002:2005, refere à disponibilidade como a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Todavia, a garantia da disponibilidade é certificar o desfecho em sua leitura, no fluxo e na conservação da informação de forma eficaz quando se faz uso de inserção de processos de preservação de hardware e a subtração de sistemas visando a priorização de softwares compatíveis se tornando essencial a utilização de infraestrutura voltada à tecnologia, manutenção de modo a conservar o acesso aos dados.

6.5 Confidencialidade

A NBR ISSO/IEC 27002 (2005)[11], a confidencialidade tem a ver com a privacidade dos dados da organização. Esse pilar age de modo que a informação seja restringida estando disponível apenas para pessoal autorizado, sendo comum que as informações sejam idôneas de acordo com o estado crítico, sendo assim, a extensão do dano que causaria ficando expostas em razão de diligências de segurança que necessitam de implementações de medidas de acordo com sua característica.

Desde modo, essa concepção tem relacionamento direto com as atitudes tomadas para certificar que as informações que são mantidas privacidade não sejam surrupiadas dos sistemas de informação através de ataques cibernéticos, softwares de espionagem entre outras formas de ataques.

Para que a confidencialidade seja robusta, é ponderoso que haja prevenção como a disposição da informação apenas para pessoas habilitadas, o que pode ser estabelecido com níveis de acesso, onde os cargos de maior importância têm esse acesso a dados de alta relevância.

[11] ABNT NBR ISO/IEC 27002. (2005). Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

7. MEIOS DE SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS DE COMUNICAÇÃO

De acordo com Fontes (2006), a informação é um ativo de grande valor e importância para a empresa. Diante deste cenário, visando à privacidade e a segurança, os principais dados de grandes e pequenas organizações são armazenados em formato digital, de modo que a atenção com a proteção dos dados seja ainda maior.

Contudo, essa pratica não contem a ação os crimina de tentarem violar a segurança e acessar os dados ou até mesmo causarem danos irreversíveis a eles, necessitando que muitas empresas recorram a meios de proteção buscando maior eficiência e proteção[12].

Sendo assim, não basta utilizar qualquer forma de proteção. É extremamente valioso que se tenha domínio das ferramentas mais robustas, atualizadas e com altos índices no que se refere a conceito no mercado para que não haja perda de tempo em testar qual aplicação vai proteger mais. E assim, usar critérios de proteção para os dados como traz as ideias do próprio autor.

7.1 Criptografia

O conceito da palavra criptografia, segundo STALLINGS (2008, p.18) consiste no desenvolvimento de técnicas para garantir o sigilo e/ou a autenticidade de informações. A criptografia, de origem grega, é composta por dois elementos básicos. O primeiro – CRIPTO – significa oculto ou secreto e o segundo – GRAFIA – significa escrita.

A escrita de dados de forma oculta de tal modo que apenas seu possessor tem a capacidade de interpretá-la. Tornando assim uma conversão de texto com caracteres alfanumérico em símbolos, números e letras de forma ininteligível aos olhos humanos que, assim, não possa identificar o que ali contém (BOAVIDA e BERNARDES 2019, p10).

[12] NETTO, Abner. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. 2007.

Deste modo, ainda seguindo a linha de raciocínio do mesmo autor, a criptografia é a forma de proteção de dados onde palavras, números e símbolos são convertidos em caracteres não entendíveis aos olhos humanos. E isso define segurança às informações que são transmitidas por meio de máquinas e equipamentos estabelecendo assim a comunicação entre aplicações, de tal forma que somente sistemas autorizados têm acesso ao conteúdo descrito.

Para SCHNEIER (2001, p. 93 e 118-119), é uma tecnologia básica do ciberespaço, dado que a criptografia é que permite gerir a sua segurança. A internet vê a criptografia como algo relativamente novo, visto que sua necessidade se dá devido à expansão do comercio eletrônico.

A criptografia dos protocolos vistos pela internet se torna algo moderno e as primeiras amostras fazem referência no ano de 2000, assim com a encriptação de e-mails e compras na Internet via cartões de créditos. Posteriormente, sobretudo até meados do século XIX, a criptografia era vista como fonte de estudo sendo alicerçada por uma gradativa base científica[13].

Contudo, hoje, abrange os grandes centros de ensino tendo destaque como uma disciplina das ciências exatas, e sua característica principal vêm ganhado ênfase na ciência da computação, embora a criptografia tenha acentuada abrangência no que diz respeito à essas duas áreas da ciência[14].

7.2 Verificação Em Duas Etapas

Em meio às mais variadas formas de segurança da informação, podemos destacar a verificação em duas etapas ou verificação em dois fatores lançado no início de 2017, usada em diversos aplicativos de comunicação inclusive no WhatsApp. Segundo o WhatsApp[15] meio de verificação é uma medida protetiva, de uso opcional, que é oferecida ao usuário, e essa proteção, atua como uma camada

[13] BOAVIDA e BERNARDES (2019, p.11).
[14] ADIL. Josué. O uso da criptografia na ciência da computação. https://acaditi.com.br/criptografia-ciencia-da-computacao/. 2019.
[15] WHATSAPP. Sobre confirmação de duas etapas. https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=pt_br

extra de proteção aumentando a segurança no acesso. No caso, ao aplicativo de mensagens instantâneas.

Ao ativar esse recurso, todas as vezes que o usuário inserir o número de telefone vinculado ao WhatsApp para fazer a verificação, o aplicativo gera um código de 6 dígitos que lhe é enviado via SMS ao número de celular requerido pelo WhatsApp, para que seja recebido o código. Assim, o usuário tem que fornecer esse código e além do mais, faz necessária a criação de uma senha de acesso ao aplicativo, contudo, pode ser desabilitado a qualquer momento durante o uso[16].

Deste modo, esse meio de autenticação já está em operação em diversas aplicações visando a ampliar complexidade de acesso inadequado, e com isso, aumentar a segurança das aplicações. O WhatsApp ainda possibilita ao usuário associar um e-mail para, caso a senha seja esquecida, o usuário poderá ter acesso a um link de desativação da verificação.

8. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS

Neste segmento, serão demonstrados os conceitos da Segurança da Informação e comunicações, as normas e padrões de segurança evidenciando a Associação Brasileira de Normas Técnicas (ABNT) e também a NBR ISO/IEC 27002, mais à frente, as Políticas de Privacidade bem como os Termos de Segurança.

8.1 Segurança da informação e comunicações

O termo Segurança de acordo com o dicionário Houaiss (2001)[17] é tudo que está seguro e afastado de todo perigo. Com base nisto, a segurança da informação tratar-se de tornarem seguras as informações tanto quanto de pessoa física como pessoa jurídica, dados que uma vez acessados ou vazado de alguma forma, acarretariam transtornos a quem é de direito.

[17] HOUAISS, Antônio. Dicionário Houaiss da Língua Portuguesa. Rio de Janeiro, Ed. Objetiva, 2001.

Conforme Alves (2006, p.15), a Segurança da Informação tem como objetivo proteger a informação de modo que se assegura o seguimento dos negócios, reduzindo as falhas e aumentando o retorno das aplicações e as viabilidades de mercado. Nesta feita, o termo segurança consiste na ação ou efeito de assegurar e garantir alguma coisa, estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais danos.

Campos (2007) enfatiza que, o conceito de informação não apresenta um único sentido, tornando improvável e sofrendo variações em diversas áreas do conhecimento secular, culturais e científicos. Contudo, existe a concordância de que a informação é mesclada de dados e elementos do conhecimento como um todo, transformando dados em informações e essas informações promovem o conhecimento.

Salienta ainda que informação é um grupo de dados exposto de forma ordenada, que com ele, se constrói a mensagem a respeito de uma estabelecida ocorrência ou fato, que por hora, permite solucionar complicações e tem grande importância nas tomadas de decisões.

E sua segurança em conformidade com a NBR ISO/IEC 27002:2008, é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades.

Segundo Beal (2005), a Segurança da Informação é enxergada como o processo de proteger as informações de ameaças e ataques preservando assim a sua integridade, disponibilidade e confidencialidade, que são alguns dos seus pilares. Contudo também não pode ser vista como um ambiente onde se esconde informações valiosas e sim aprimorar a criação ou a existência de política de proteção, garantindo a preservação contra ameaças e vulnerabilidades.

O Art. 154-A da Lei 12.737, de 30 de novembro de 2012, presume crime no Código Penal Brasileiro:

> [...] invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (BRASIL, 2012. p.1).

Este crime pode gerar uma pena de detenção de 3 (três) meses a 1 (um) ano, e multa. Em outras épocas, antes da criação dessa lei, se fazia necessário caracterizar as condutas efetivas as quais eventualmente se tem êxito.

8.2 Normas e padrões de segurança

De acordo com a ABNT (2015), desde 1940, a Associação Brasileira de Normas Técnicas (ABNT) é a intendente por criar as normas e padrões técnicos, sendo também uma das fundadoras da Organização Internacional de Normalização (ISO).

> A normalização é, assim, o processo de formulação e aplicação de regras para a solução ou prevenção de problemas, para o benefício e com a cooperação de todos os interessados, e, em particular, para a promoção da economia global. No estabelecimento dessas regras, recorre-se à tecnologia como o instrumento para estabelecer, de forma objetiva e neutra, as condições que possibilitem que o produto, projeto, processo, sistema, pessoa, bem ou serviço atendam às finalidades a que se destinam, sem se esquecer dos aspectos de segurança (ABNT, 2015).

De acordo com a NBR ISO/IEC 17799, somente a partir de 2007 foi inserido à sua nova edição um novo método de numeração como NBR ISO/IEC 27002, o qual é o código de práticas para o gerenciamento da segurança da informação. Tornando-se um marco referencial à criação de diretrizes e fundamentos gerais quando se trata de metas.

E comumente aceita no controle da segurança da informação que na descrição de controle da norma NBR ISO/IEC 27002, percebe a maneira de coordenar o risco, inserindo políticas, metodologias, diretrizes ou estrutura organizacional e pode ser de origem administrativa, controle ou assegurado.

Segundo Campos (2007), um controle é toda técnica usada para reduzir a vulnerabilidade de um ativo, ora uma tecnologia, ora uma pessoa ou um âmbito.

De acordo com a norma NBR ISO/IEC 27002:20008, há 11 regras de boas práticas de gestão de segurança da informação, os quais são dispostos:

- Políticas de segurança da informação;
- Organização da segurança da informação;

- Gestão de ativos;
- Segurança em recursos humanos;
- Segurança física e do ambiente;
- Gerenciamento das operações e comunicações;
- Controle de acesso;
- Desenvolvimento e manutenção de sistemas de informação;
- Gestão de incidentes de segurança da informação;
- Gestão de continuidade de negócio;
- Conformidade.

Boas práticas de segurança da Informação são importantes para garantirem a proteção contra invasões de arquivos maliciosos que resultam em vazamento de dados, podendo assim manter a integridade das informações.

É ideal que esse método seja partilhado entre as equipes de trabalho e assim assegurar a segurança da informação.

8.3 Política de Privacidade e Termos de segurança

A norma NBR ISO/IEC 270022008[18], presume-se que as políticas de segurança da informação aconteçam por meio da preservação do acesso e da privatividade dos dados, para que ocorra a segurança dos mesmos. Pois tem se tornado cada vez mais comum, se deparar com a mensagem de aceitação dos termos de Políticas de Privacidade ao acessarmos algum site.

Isso se torna necessário por estar incluso ao sistema de políticas de segurança da informação, que são uma forma de garantia de que os dados que o internauta fornece como informações pessoais ou empresariais. Quanto à utilização dos dados por ele fornecidos podem ou não serem usados para alguma finalidade de interesse da empresa mantenedora do site. Em outros termos, uma forma de manter a transparência com os usuários em relação aos dados fornecidos.

Segundo a MICROSOFT (2021), todos os sites devem manter em local visível os termos e políticas no que se refere à segurança dos dados dos usuários. Para

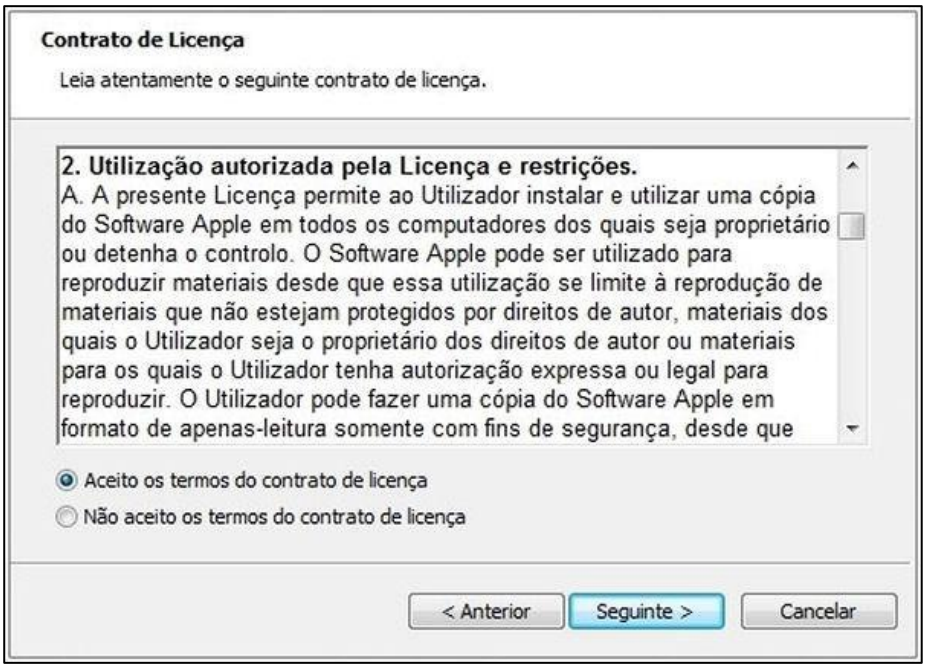
[18] NBR ISSO/IEC 270022008. https://pt.scribd.com/doc/250405384/ISO-27002-2008-pdf

que não haja desconhecimento dos termos por parte dele e nesta pauta de explanação, se faz necessário mencionar, por mais que tenha citado precedentemente, como foram abordados assuntos como o compartilhamento de informações de diversas maneiras, informações que comprovem seu comprometimento com o internauta. Quando se trata dos termos e serviços, que são nada mais, que uma espécie de contrato celebrado entre o usuário e a empresa que fornece o acesso a um determinado site ou serviço.

Quando o internauta ou usuário aceita os termos de serviços de um site ou até mesmo o contrato de licença que é exibido, no caso do uso de um software, quando é iniciada a instalação do mesmo. É exibida a famosa tela de Contrato de Licença que literalmente te obriga a concordar com os termos daquele contrato para uso do sistema, no qual se a opção selecionada for “Não aceito os temos do contrato de licença”.

Assim, o sistema não prosseguirá com a instalação forçando a aceitação dos termos. Uma vez que, antes de selecionar a opção “aceitar”, o botão para prosseguir à próxima tela se apresenta desabilitado, impossibilitando assim, o progresso da instalação do software e, ao aceitar, automaticamente ele fica ciente de que está concordando com cada cláusula daquele termo ali escrito. Porém, é mínima a quantidade de pessoas que leem aquelas pequenas letras que compõe um extenso texto que é o contrato de licença como mostra a figura 11.

Figura 11: Termos do Contrato de Licença.



Fonte: Tecmundo (2011).

Figura 12: Termos de adesão de serviços.

Fonte: Tecmundo (2021).

Segundo a REVISTA SUPERINTERESSANTE (2012)[19], nos remete à uma reportagem por título “Não li e concordo”, a qual aborda um questionamento esclarecedor: “Afinal, quem lê contratos?”. É de grande valia se atentar aos paradigmas do cotidiano aludidos no conteúdo de cunho jornalístico:

[19] ROMERO, LUIZ. NÃO LI E CONCORDO. REVISTA SUPERINTERESSANTE. Edição 307 de agosto de 2012, pág. 80.

> No começo de 2005, Doug Heckman resolveu ler um contrato. No meio das cláusulas, encontrou algo estranho – um prêmio de mil dólares. Entrou em contato com a empresa de softwares *PCPitstop*, responsável pelos termos, e recebeu o prêmio. O problema: foram precisos 5 meses e 3 mil cadastros para que alguém percebesse a brincadeira. Anos depois, em abril de 2010, a loja de jogos *GameStation* foi ainda mais longe: escondeu uma cláusula que fazia o usuário ceder os direitos da própria alma à empresa. Enquanto mil pessoas identificaram a brincadeira, 7 mil concordaram. Assim como a maioria das pessoas nesses dois casos, você, provavelmente, não lê termos de uso e políticas da internet. São 97%, segundo pesquisa da Universidade Stanford, os usuários que pulam direto para o "concordo". Ou seja, de cada 100 cadastrados, apenas 3 sabem o que podem e o que não podem fazer dentro de redes sociais, sistemas de busca e ferramentas de postagem (REVISTA SUPERINTERESSANTE, 2012, pág. 80).

Segundo Doug Heckman (2012), a tendência de o usuário/internauta aceitar os termos sem ao menos ler o contrato de licença é comum. De acordo com a Universidade de Berkley, em uma pesquisa realizada pela própria instituição, dos 81.920 dos usuários que participaram da pesquisa, 50% aceitaram os termos de contrato em menos de 8 segundos.

Segundo a Revista SUPERIENTESSANTE (2012), a empresa *Measuring Usability*, diz que 95% das pessoas nem sequer leem o texto descrito nos termos de contrato antes de aceitarem as condições e esse resultado pode ser visto no Gráfico 1.

Gráfico 1: Gráfico de resultado da pesquisa da Universidade de Berkley

Fonte: Própria (2021).

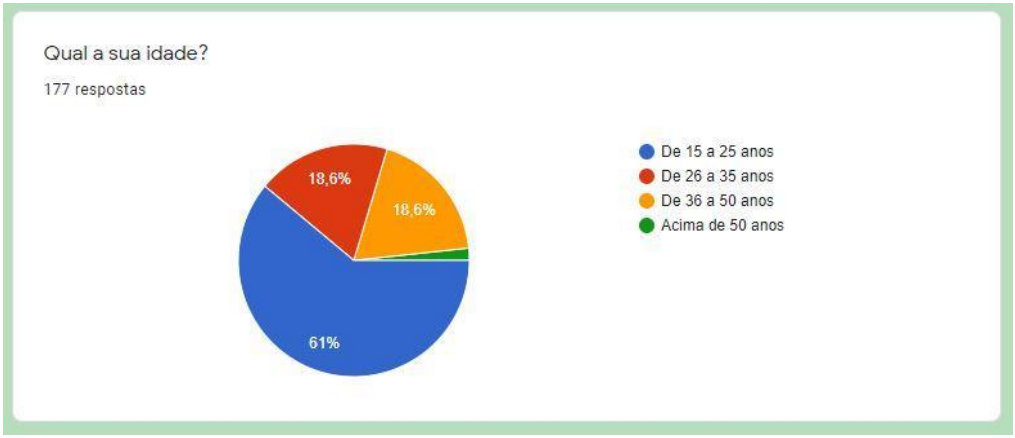
9. ANÁLISE DE RESULTADOS

Este trabalho consiste em entender o grau de conhecimento das pessoas em relação à segurança da informação nas redes sociais em aplicativos como Instagram e WhatsApp e suas vulnerabilidades.

Como mencionado na metodologia deste trabalho, demonstramos a maneira em que o respondente do questionário foi abordado ao solicitar a sua participação na pesquisa. Para se inteirar sobre o assunto, o respondente recebeu o seguinte enunciado:

O questionário é rápido e objetivo, contendo uma questão relacionada à faixa de idade, o sexo dos respondentes, bem como o estado civil, ambiente de residência dos usuários e demais perguntas diretas sobre os métodos de segurança utilizados nos aplicativos de rede social. Assim como nível de conhecimento em relação às suas vulnerabilidades diante do vasto desenvolvimento tecnológico dos dias contemporâneos.

Gráfico 2: Qual a sua idade?



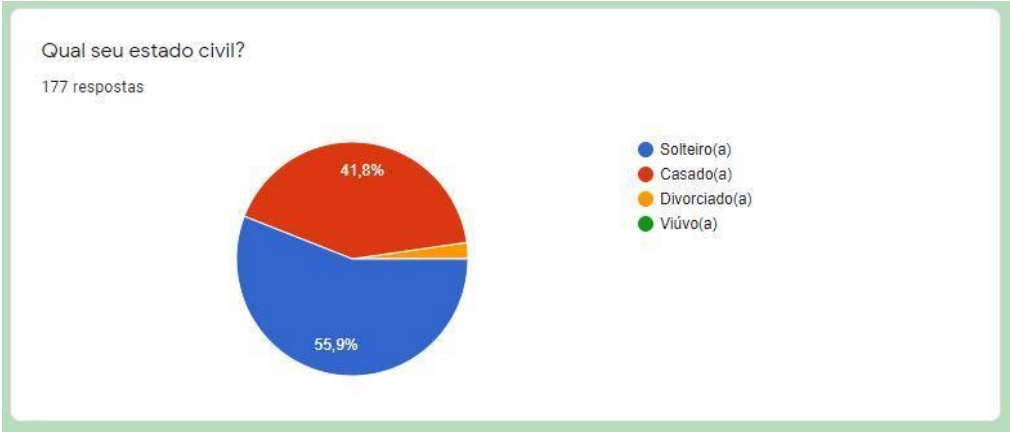
Fonte: Própria (2021).

Diante da análise desta pesquisa podemos certificar que, em um total de 177 respondentes, 108 pessoas, o que corresponde a 61% dos entrevistados, se encontram na faixa etária entre 15 e 25 anos, e 33 pessoas, ou seja, 18,6% estão com idade entre 26 a 35 anos, de igual modo 18,6% estão entre 36 a 50 anos,

ficando apenas 3 pessoas com idade acima de 50 anos, é o que representa 1,7% dos respondentes desta pesquisa.

De acordo com gráfico 2, podemos observar que o maior número de usuários que participaram respondendo ao questionário, está com idade entre 15 e 25 anos.

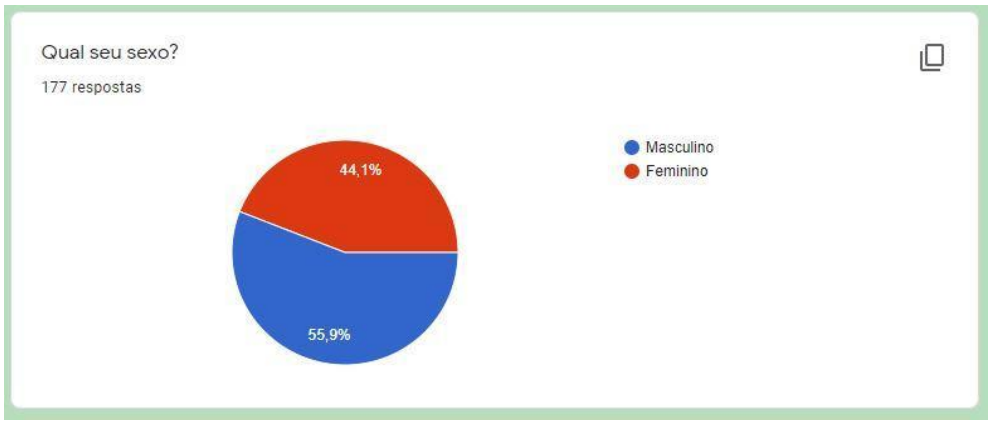
Gráfico 3: Qual seu estado civil?



Fonte: Própria (2021).

A pesquisa mostrou que quando a pergunta foi referente ao estado civil dos respondentes, 99 pessoas disseram ser solteiras, o que representa a 55,9% e 74 pessoas 41,8%, disseram ser casadas, restando apenas 4 pessoas divorciadas que são 2,3% dos respondentes. Deste modo, a maioria dos respondes a esta questão é pertencente ao Estado Civil solteiro.

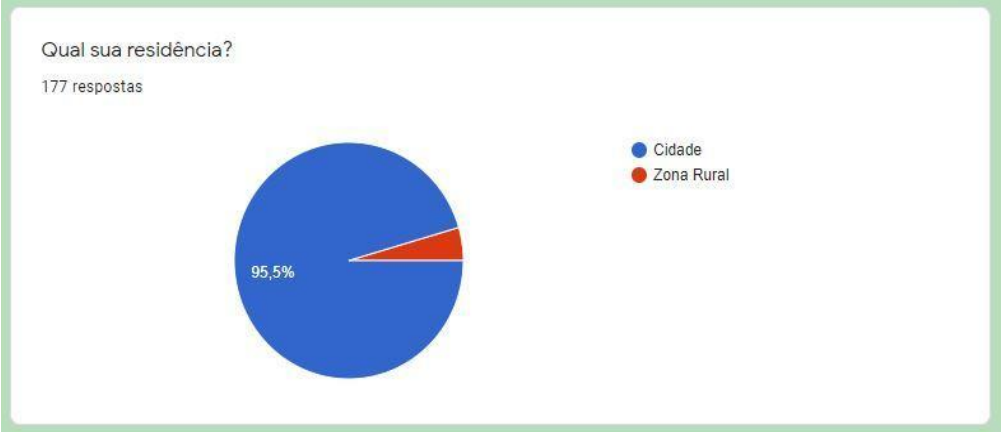
Gráfico 4: Qual seu sexo?



Fonte: Própria (2021).

Diante do levantamento da pesquisa, como mostra o gráfico 4, no que faz referência ao sexo dos respondentes, 99 pessoas disseram ser do sexo masculino, o que representa a 55,9% e 78 pessoas 44,1%, disseram ser do sexo feminino. Portanto, a maioria dos respondes a esta questão são do sexo masculino.

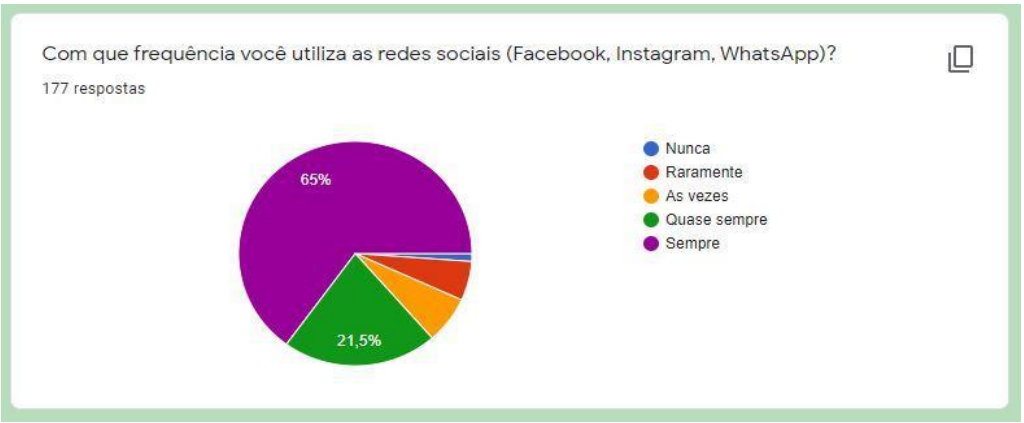
Gráfico 5: Qual sua residência?



Fonte: Própria (2021).

Deste modo, quando perguntado aos respondentes quanto à localização de suas residências, se é centralizada na Cidade ou na Zona Rural, 169 pessoas disseram residir na cidade, o que representa a 55,5% e apenas 8 pessoas 4,5%, disseram morar na Zona Rural. Nota-se que, a maioria dos respondes está centralizado nos perímetros urbanos, como mostra o gráfico 5.

Gráfico 6: Com que frequência você utiliza as redes sociais (Facebook, Instagram, WhatsApp)?

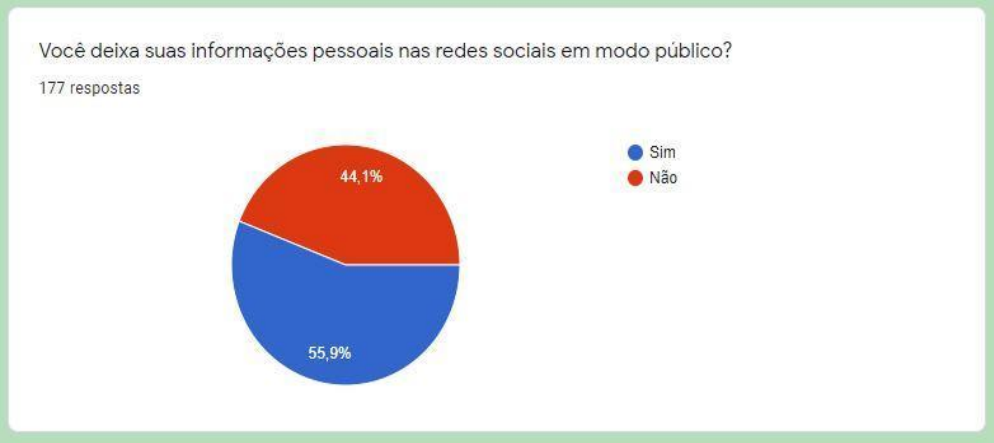


Fonte: Própria (2021).

Analisando o Gráfico 6, que a pergunta é feita em relação à que frequência o respondente utiliza as redes sociais, podemos perceber que das 177 respostas que obtivemos 115 pessoas, ou seja, 65% das pessoas que participaram da pesquisa estão sempre conectados com a internet por meio de um dos aplicativos citados.

Desde modo, 38 pessoas é o equivalente a 21,5% disseram que quase sempre estão conectadas, 6,8% o que representa 12 pessoas, disseram que às vezes usam as redes sociais. 10 pessoas 5,6%, raramente estão conectadas a rede social em busca de algum tipo de informação ou entretenimento e apenas 2 pessoas 1,1% nunca utiliza as redes sociais em busca de entretenimento ou alguma informação confiável.

Gráfico 7: Você deixa suas informações pessoais nas redes sociais em modo público?



Fonte: Própria (2021).

No momento onde a questão é direcionada a deixar os dados pessoais visíveis nos perfis das redes sociais, compreende-se que 55,9% das pessoas participantes da pesquisa, 99 pessoas, não veem problemas em manter os dados pessoais expostos.

Em contrapartida, 78 pessoas 44,1% preferem ocultar suas informações pessoais deixando de modo que apenas o responsável por elas possa visualizar, ou optam até mesmo a não preencher os dados que são solicitados no momento em que estão criando o perfil na rede social, mantendo a privacidade evitando assim

que os dados possam ser usados de forma indevida em outras finalidades não autorizadas pelo titular.

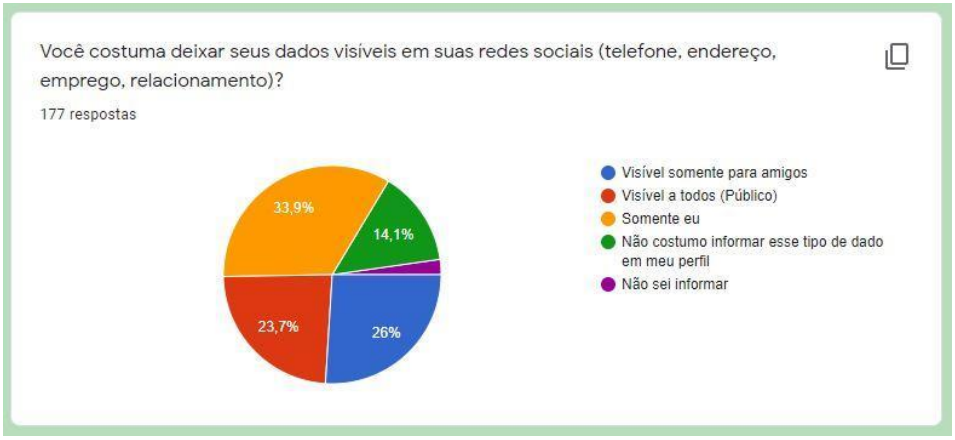
Gráfico 8: Você utiliza datas comemorativas como senha em aplicativos?

Fonte: Própria (2021).

Quando se refere à criação de senhas, em foco para redes sociais o objetivo é assegurar a privacidade e segurança dos dados. Contudo, das 177 pessoas que responderam ao questionário, 52 (29,4%) respondentes disseram que às vezes usam datas comemorativas como senha, já 50 pessoas 28,2% tem um cuidado maior com relação a senhas e raramente usam datas para representá-las.

Porém, 33 respondentes correspondem a 18,6%, disseram que nunca usam datas como senha por ser de fácil descoberta e desse total apenas 17 (9,6%) diz sempre usar datas comemorativas e 25 pessoas (14,1%) disseram que sempre usam esse método.

Gráfico 9: Você costuma deixar seus dados visíveis em suas redes sociais (telefone, endereço, emprego, relacionamento)?



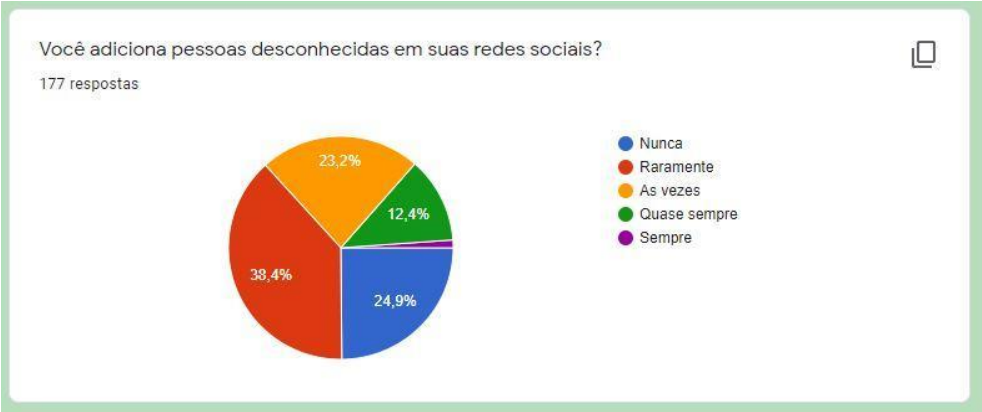
Fonte: Própria (2021).

Bem sabemos que nem todas as informações podem ser exibidas ao público e que dados pessoais precisam ser assegurados com maior sigilo de maneira que não venham ser usados de forma inconveniente.

Partindo desse pressuposto, pesquisamos sobre a possiblidade das pessoas deixarem os dados visíveis em seus perfis de redes sociais e constatamos 33,9% deixam os dados visíveis somente para si, 42 pessoas 23,7% não se importam que os dados pessoais fiquem expostos para o público.

Já para 26% das pessoas que responderam nossa pesquisa, representados por 46 pessoas, mantém seus dados visíveis somente para os amigos em comum nas redes. E 25 pessoas 14,1% costumam preservar seus dados pessoais não informando no momento de preencher os requisitos do perfil das redes sociais e apenas 4 respondentes 2,3% não souberam informar se costumam deixar seus dados de forma visível ou se usufruem algum meio de privacidade nas redes sociais.

Gráfico 10: Você adiciona pessoas desconhecidas em suas redes sociais?



Fonte: Própria (2021).

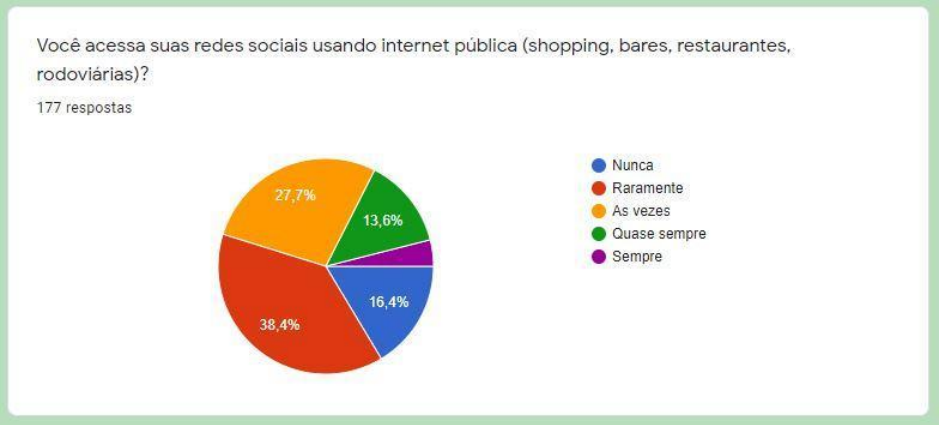
Ao abordarmos a questão de adicionar pessoas desconhecidas em redes sociais, durante a pesquisa percebemos que das 177 pessoas participantes, 38,4% ou seja, 68 pessoas disseram que raramente aceitam desconhecidos para fazerem parte da lista de amigos das redes sociais, porém 24,9% dos respondentes, que é equivalente a 44 pessoas, disseram que nunca adicionam pessoas que não conhecem em suas redes sociais.

No entanto, 41 pessoas (23,2%) disseram que às vezes aceitam pessoas desconhecidas. Já 22 pessoas (12,4%) quase sempre adicionam essas pessoas para serem seus amigos nas redes sociais. Apenas 2 pessoas (1,1%) concordam em aceitar alguém que não conhecem em suas redes sociais.

Percebe-se um dado alarmante, pois, de 177 participantes, 133 pessoas estão colocando os dados pessoais, sua localização, fotos de família, compartilhando sua rotina e seu dia a dia com 75,1% de pessoas desconhecidas em suas redes sociais.

Esse resultado mostra uma ampla margem de vulnerabilidade, tanto das informações pessoais, empresariais, local de trabalho. Assim sendo, grande parte de sua rotina está exposta em uma página externa colocando em risco sua integridade física, moral, social, haja vista que depois de conhecer os trajetos, os membros da composição familiar, os locais costumeiramente frequentados, ficaria mais acessível uma abordagem imprevisível.

Gráfico 11: Você acessa suas redes sociais usando internet pública (shopping, bares, restaurantes, rodoviárias)?



Fonte: Própria (2021).

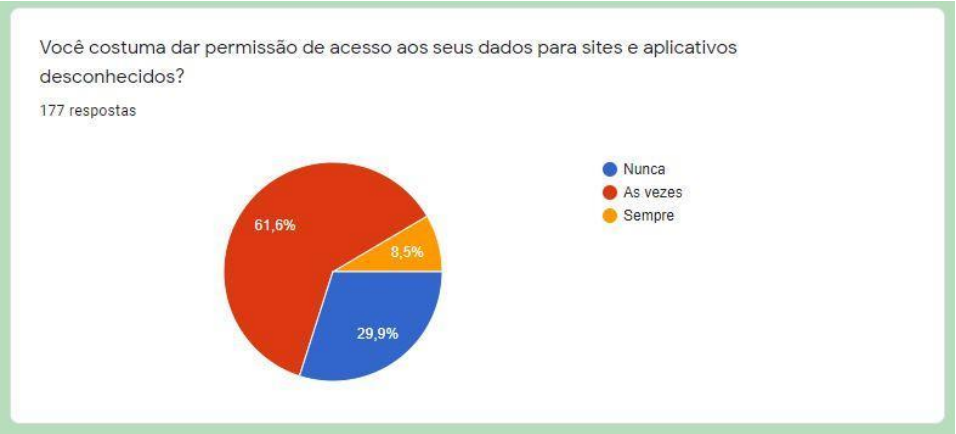
Um dos perigos mais constantes e pouco observados é a identificação se uma determinada página de internet é verídica e confiável. Visto que essa ação é uma das principais técnicas que são usadas por maliciosos para coleta de usuários e senhas de contas bancárias, acesso a sites de *ecommerce* e outros ambientes da mesma finalidade.

No decorrer da pesquisa, perguntamos aos participantes se acessam os perfis das redes sociais a partir de redes públicas como em shoppings, bares, restaurantes, rodoviárias. Para avaliarmos qual seria o comportamento dos respondentes diante desta questão e tivemos que um total de 68 pessoas, isto é, 38,4% dos participantes raramente usam redes abertas para acessarem seus perfis nas redes sociais.

Sob outra perspectiva, notamos que 49 participantes, o que representa 27,7% dos respondentes, uma vez ou outra acessam usando a internet pública e 24 pessoas totalizando 13,6% responderam que quase sempre aproveitam da internet grátis para visitarem sites e navegarem pelos perfis das redes.

Apenas 4% dos entrevistados, somam 7 pessoas, permanece o tempo todo conectado sem se importar com a violabilidade dos dados. Contudo, 29 pessoas, 16,4% são prudentes quanto ao lidar com dados pessoais na internet e nunca acessam suas redes sociais usando uma rede aberta.

Gráfico 12: Você costuma dar permissão de acesso aos seus dados para sites e aplicativos desconhecidos?



Fonte: Própria (2021).

Com referência a conceder permissão de acesso aos dados para sites e aplicativos desconhecidos, temos que 109 pessoas, que se dá em 61,6% dos participantes da pesquisa, disseram às vezes permitirem que aplicativos desconhecidos tenham acesso aos dados. Já 8,5% referente a 15 pessoas, disseram que sempre dão permissão de acesso aos dados.

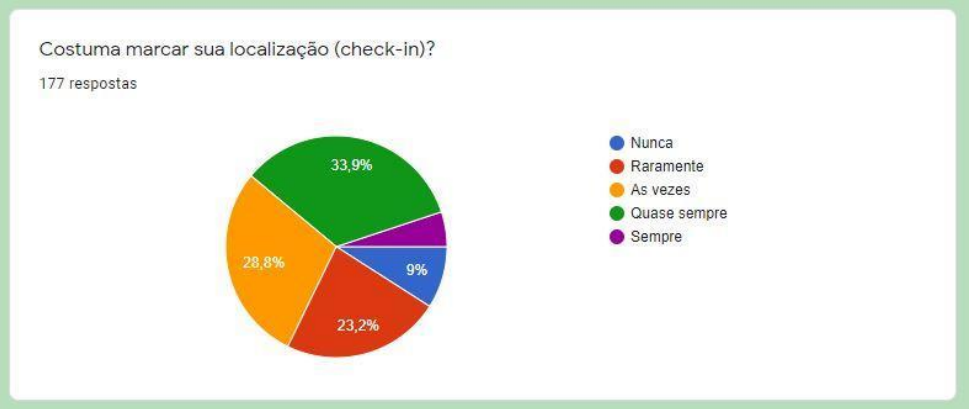
Por outro lado, temos que 53 pessoas (29,9%) nunca dá esse tipo de permissão para nenhum aplicativo desconhecido. Um fator determinante, em especial nesse quesito é fazer uso das boas práticas de segurança ao acessar determinados sites e atentar ao conceder permissão para qualquer aplicativo ter acesso ao smartphone, até porque boa parte da vida cotidiana do usuário está inserida ali.

Com a flexibilidade e a acessibilidade a informação, os smartphones têm sido uma peça fundamental para uso em pesquisas acadêmicas e até mesmo para transações comerciais.

Deste modo, dar permissão para um aplicativo que promete ser uma calculadora científica ter acesso a fotos, localização, ao microfone do dispositivo móvel, e/ou informações que não farão parte do que propõe sua tarefa.

São técnicas de invasão usadas por cibercriminosos para coletar dados de usuários para usarem de forma maliciosa sem o conhecimento da vítima.

Gráfico 13: Costuma marcar sua localização (check-in)?



Fonte: Própria (2021).

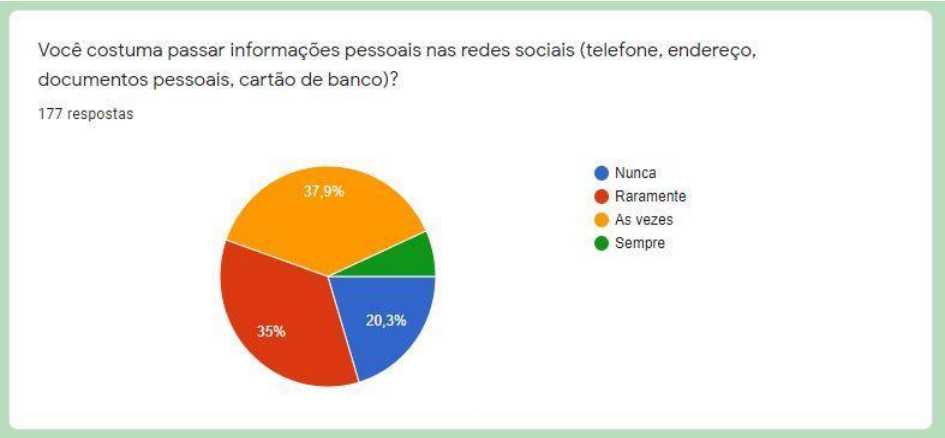
Não é novidade que as redes sociais têm opção de sinalizar a localização exata tornando público onde o usuário do perfil está naquele momento[20]. Contudo, é uma ferramenta de mão dupla podendo ser perigoso dependendo da forma que fizer uso, já que poderá deixar entendível que naquele momento, não tenha ninguém em sua residência, a qual poderá ser alvo de pessoas mal-intencionadas.

Observando por essa ótica, perguntamos se a pessoa tem costume de marcar sua localização nos lugares que visitam e temos que 60 pessoas, os equivalentes a 33,9% dos respondentes disseram quase sempre usar o recurso. 51 (28,8%) responderam que às vezes fazem *check-in* dos lugares que visitam. 41 (23,2%) raramente tornam público suas visitas a locais públicos.

Apenas 16 (9%) nunca usam essa ferramenta e 9 (5,1%) não dispensam a possibilidade de marcar a localização em todos os lugares que são frequentados.

[20] G1. GLOGO.COM. REDE SOCIAL MOSTRA LOCALIZAÇÃO DOS ASSOCIADOS. https://g1.globo.com/Noticias/Tecnologia/0,,MUL81448-6174,00 REDE+SOCIAL+MOSTRA+LOCALIZACAO+DOS+USUARIOS.html

Gráfico 14: Você costuma passar informações pessoais nas redes sociais (telefone, endereço, documentos pessoais, cartão de banco)?

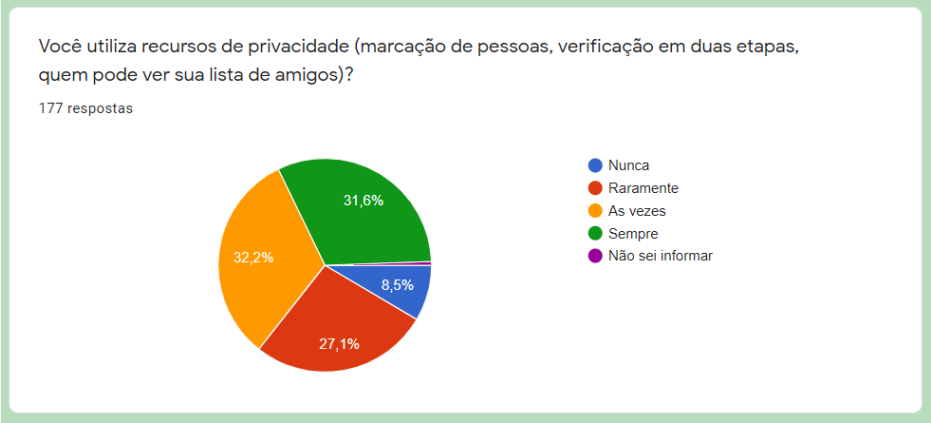


Fonte: Própria (2021).

No quesito de privacidade quanto aos dados de telefone, endereço, documentos pessoais e até mesmo dados de cartão de crédito, podemos perceber que 62 que significa 35% dos respondentes disseram que raramente passa informações sigilosas.

Já 67 respondentes, isto é, 37,9% relataram que às vezes ocorre de enviar informações por esse meio. No entanto, 36 que somam 20,3% recomendam que de forma nenhuma enviam informações pessoais ou nenhum outro dado importante por meio de rede social. Os demais 6,8% que são 12 respondentes disseram não ver perigo e sente segurança em usar esse meio para transmitir seus dados.

Gráfico 15: Você utiliza recursos de privacidade (marcação de pessoas, verificação em duas etapas, quem pode ver sua lista de amigos)?



Fonte: Própria (2021).

No que concerne a utilização de recurso de privacidade de dados, 57 respondentes do questionário proposto, o que se torna 32,2% disse que as vezes faz uso desse método, 56 (31,6%) relataram que sempre utilizam os recursos de privacidade das redes sociais, já 48 (27,1%) disseram que raramente fazem uso do mecanismo.

Os que nunca usaram ou nunca usam tem o percentual um pouco menor chegando a apenas 15 pessoas, o que representa (8,5%) dos participantes da pesquisa. Somente 1 pessoa (0,6%) não soube informar se utilizam ou não dos recursos de privacidade oferecidos pelas redes sociais.

Gráfico 16: Você costuma salvar suas senhas no navegador de internet?

Fonte: Própria (2021).

Quando se trata de senhas, os cuidados precisam ser acentuados, até porque memorizar várias senhas não é uma tarefa tão simples e exige muito cuidado, não podendo deixar anotadas em qualquer lugar, pois geralmente se trata de acesso a informações de alto valor.

Ao perguntar se as pessoas costumam salvar suas senhas nos *browsers*, comumente conhecidos como navegadores de internet, tivemos que das 117 pessoas que participaram da pesquisa, 65 (36,7%) disseram que as vezes salvam as senhas nos navegadores, decisão tomada possivelmente por não confiarem tanto na segurança dos navegadores. 39 (22%) confiam na segurança oferecida e sempre deixam suas senhas salvas, o que torna o acesso mais ágio, uma vez que não precisa digitar todas as vezes que for acessar uma determinada aplicação web.

Por outro aspecto, temos que 29,9% representado por 53 pesquisados, raramente deixam as senhas salvas. 10,7% é a parcela que nunca deixam esse tipo de informação salva nos navegadores, sendo equivalente a 19 pessoas, provavelmente por acreditar que alguém tenha acesso a esses dados. E apenas 1 pessoa (0,6%) não soube informar se costuma ou não salvar as senhas.

Deste modo, 31% pessoas de 15 a 25 anos deixam os dados visíveis somente para amigos, são solteiros, do sexo masculino, moram na cidade, sempre salvam as senhas nos navegadores de internet e são os que mais acessam as redes sociais usando internet pública. Como mostra gráfico 17.

Gráfico 17: Resultado do cruzamento de dados do formulário de pesquisa

Fonte: Própria (2021).

De acordo com o resultado do cruzamento de dados a respeito da quantidade de pessoas na faixa etária de 15 a 25 anos que informam dados pessoais, empresariais, bancárias nas redes sociais e com que frequência essas pessoas utilizam as redes sociais acessando internet pública, temos que: 44% das pessoas informaram que passam informações nas redes sociais e 13% tem essa atitude usando internet pública.

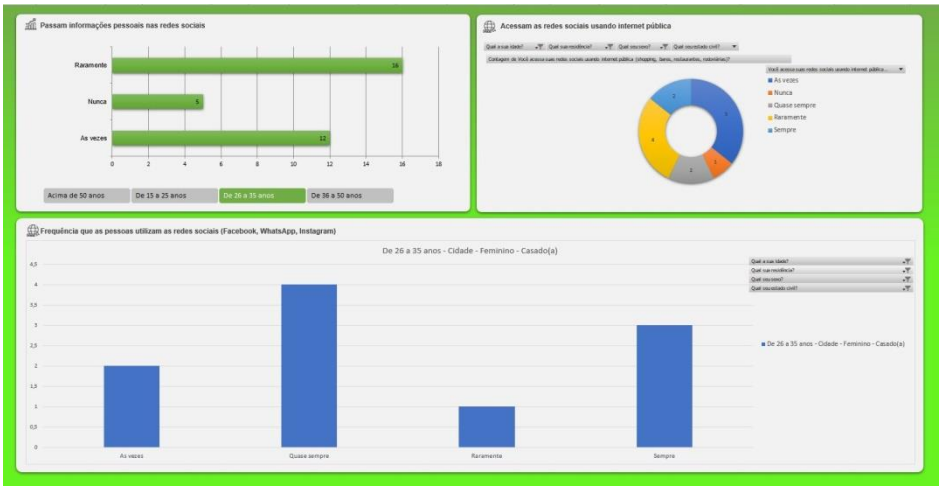
As pessoas solteiras, do sexo masculino, que moram na cidade, são os que acessam a internet pública com mais frequência. Como mostra gráfico 18.

Gráfico 18: Resultado do cruzamento de dados de pessoas que passam informações pessoais acessando internet pública.

Fonte: Própria (2021).

De outro lado, agora com o resultado do cruzamento de dados a respeito da quantidade de pessoas na faixa etária de 26 a 35 anos que informam dados pessoais, empresariais, bancárias nas redes sociais e com que frequência essas pessoas utilizam as redes sociais acessando internet pública, temos que: 28% das pessoas informaram que passam informações nas redes sociais e 36% tem essa atitude usando internet pública. Nessa atuação, as pessoas casadas do sexo feminino que moram na cidade, são as que acessam a internet pública com mais frequência. Como mostra gráfico 19.

Gráfico 19: Resultado do cruzamento de dados de pessoas do sexo feminino que passam informações pessoais através internet pública.



Fonte: Própria (2021).

CONSIDERAÇÕES FINAIS

À proporção em que a progressão da ciência e tecnologia vem assenhoreando os dias que ocorrem, alcançando cada vez mais o espaço nas grandes corporações de modo a substituir numerosa parte do feitio humano, há em contrapartida o desdobramento dos grandes centros acadêmicos. Nas formações de desenvolvedores de tecnologias que são imperantes ao tangente dessas tecnologias substitutivas, de modo a criar necessidade haver a seletiva intervenção intelectual e interação humana no desenvolvimento de linguagens de programação, hardwares e componentes para programar tais dispositivos.

Embora não se possa ter a asseveração de que uma aplicação é totalmente segura, visto que não depende tão somente dos critérios de segurança tomados durante o desenvolvimento. Subsiste nesse ínterim, o processo com uma série de parâmetros lógicos a serem seguidos para que se tenha uma medida protetiva ou uma espécie de *firewall* nativo refreando as ações maliciosas que advém do ambiente externo. E daí a dimensão para se prevenir de riscos de maneira a atenuar ao máximo as fragilidades da aplicação.

E fundamentado nisso, infere-se que a segurança se dá início, como a cautela na seleção que o Departamento de Recursos Humanos precisa dar prioridade, quando se diz respeito à contratação de um colaborador, exigindo ou propondo treinamento e capacitação adequados à investidura ao cargo. Expor nitidamente as diretrizes de segurança da organização, na autorização de acessibilidade ao ambiente de trabalho com a inserção de inflexível controle de acesso físico aos departamentos de tecnologias, onde são operados os datacenters, servidores de hospedagens, provedores de internet, gerenciadores de banco de dados. Haja vista que as condutas de segurança devem ser abordadas em todos os aspectos, referindo-se aos físicos, lógicos e pessoais.

De acordo com a Norma NBR ISO/IEC 17799, uma área segura é onde se tem uma barreira, tal como uma parede, um portão de entrada controlado por cartão ou um balcão de recepção com atendentes.

Há paralelos onde o próprio usuário torna seus dados em situação comprometedora, como ao fazer o download de aplicativos de fontes desconhecidas que em sua totalidade são aplicativos *crackeados*, ou seja, tem sua estrutura modificada para finalidades múltiplas, se expondo a uma extensa fragilidade no que diz a segurança de dados, outrora fazendo uso de versões betas, que são versões de testes, que ainda não se encontra em um estágio seguro ou estável para se tornar de acesso público nas lojas de aplicativos para serem baixados por em sua maioria de forma grátis.

Uma das formas mais eficazes de proteção de dados é a utilização dos Softwares Antivírus, os quais tem função de identificar um arquivo malicioso e o excluir antes mesmo que adentre ao disco rígido infectando os arquivos do Sistema Operacional e obtendo informações sigilosas, abrindo portas de acesso a arquivos confidenciais. Evidencia-se que os e-mails são grandes responsáveis por infecções de arquivos através dos *malwares* e suas variantes.

Os Antivírus proporcionam a integridade dos dados, contudo não basta apenas instalar a ferramenta de segurança e proteção, é preciso ser treinado para identificar os ataques, pois todos os dias são criados novos vírus.

No entanto, a segurança da informação, de forma geral, está diretamente correlacionada com a maneira em que cada usuário se comporta ao lidar com seu dispositivo, atentando aos sites que são acessados, à exposição de informações nos

perfis das redes sociais, no fluxo de mensagens que são comutadas quer seja de texto, áudio, imagem ou e-mail, que nelas contenham dados privativos.

Em análise realizada com o cruzamento dos dados coletados durante a pesquisa e temos que, para o quesito de exposição de dados nos perfis das redes sociais, 28% das pessoas são da faixa etária de 15 a 25 anos. Deixam os dados visíveis ao público, são solteiros, do sexo masculino, moram na cidade, sempre salvam as senhas nos navegadores de internet e são os que mais acessam as redes sociais usando internet pública.

Sendo assim, percebemos que os objetivos da pesquisa foram atendidos, tendo em vista que a importância dessa pesquisa em buscar conhecer as causas dos vazamentos de dados na internet, buscar compreender se as ações do usuário em deixar público os dados pessoais nos perfis das redes sociais e a forma que utilizam o compartilhamento de dados, interferem diante desses acontecimentos.

Baseado nisso, notamos que um importante percentual do comportamento dos aplicativos móveis é a resposta das ações dos usuários diante da usabilidade como vimos nos resultados estatísticos. Além disso, a hipótese foi confirmada pelo fato de que a exposição de dados pessoais nos perfis de redes sociais, e atitudes semelhantes, de certa forma favorecem para o vazamento de dados.

Contudo, é importante que essa pesquisa seja continuada no futuro. Não somente com um público relacionado à tecnologia e também com maior duração para que se possam fazer novas análises, novos estudos, de modo que venha conhecer os comportamentos dos mais variados tipos de pessoas e assim, obter resultados mais elaborados e concisos.

REFERÊNCIAS

_____. **Não li e concordo**. Revista Super Interessante, ed. 307, p.80, agosto/2012.

ABRAMCZUK, André A. **A prática da tomada de decisão**. São Paulo: Atlas, 2009.

ALVES, Gustavo Alberto. **Segurança da Informação: uma visão inovadora da gestão**. Rio de Janeiro: Ciência Moderna Ltda, 2006.

APPLE. Apple Store, **Instagram** 2021. Disponível em: https://apps.apple.com/br/app/instagram/id389801252. Acesso em: 20 maio de 2021.

APPLE. Apple Store, **Whatsapp** 2021. Disponível em: https://apps.apple.com/br/app/whatsapp%20messenger/id310633997. Acesso em: 20 maio de 2021.

APPLE. Apple Store, 2021. Disponível em: https://apps.apple.com. Acesso em: 20 maio de 2021.

ARRUDA, Felipe. **Contrato de licença: concordou e não leu, sua alma você vendeu**. Disponível em: https://www.tecmundo.com.br/consumidor/10206-contrato-de-licenca-concordou-e-nao-leu-sua-alma-voce-vendeu.htm Acesso em 7 nov. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Primeira edição 31.03.2006. Disponível em: https://jkolb.com.br/wp-content/uploads/2016/09/ABNT-NBRISOIEC27001 20060331Ed1.pdf Acesso em: 07 mar 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Normalização Definição** Disponível em http://www.abnt.org.br/normalizacao/o-que-e/o-que-e acesso em 09 nov. 2020.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** - São Paulo: Atlas, 2005.

BOAVIDA, Fernando; BERNARDES, Mario. **Introdução à Criptografia**. 1ª Ed. FCA, 2017.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**. Brasília, 30 de novembro de 2012.

CASTELLS, M. **A SOCIEDADE EM REDE**. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **A galáxia da Internet**. Rio de Janeiro: Jorge Zahar, 2003.

DANTAS, Marcus Leal - **Segurança da Informação: uma abordagem focada em gestão de riscos**. -Olinda: Livro Rápido, 2011.

ESCOLA, Equipe Brasil. **Internet no Brasil"; Brasil Escola**. Disponível em: https://brasilescola.uol.com.br/informatica/internet-no-brasil.htm. Acesso em 20 de jun. 2020.

FIGUEIREDO, N. M. DA **NECESSIDADE DE PROMOVER O USO DA INFORMAÇÃO**. Ciência da Informação, Brasília, v. 16, n. 1, p. 75-9, jan.-jun. 1987.

FONTES, Edison. **Segurança da Informação: O Usuário faz a diferença**. São Paulo: Saraiva, 2006.

G1. GLOGO.COM. REDE SOCIAL **MOSTRA LOCALIZAÇÃO DOS ASSOCIADOS**. https://g1.globo.com/Noticias/Tecnologia/0,,MUL81448-6174,00 REDE+SOCIAL+MOSTRA+LOCALIZACAO+DOS+USUARIOS.html

GAGNE, R. M. **Instructional Technology:Foundations**. Routledge,NY, 16 de dez de 2013.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GIL, A. C. **COMO ELABORAR PROJETOS DE PESQUISA**. 4. ed. São Paulo: Atlas, 2009.

GOOGLE PLAY STORE. Disponível em: https://play.google.com/store/apps/details?id=com.whatsapp&hl=pt_BR&gl=US Acesso em: 20 maio de 2021.

GOOGLE PLAY STORE. Disponível em: https://play.google.com/store/apps/details?id=com.instagram.android&hl=pt_BR&gl=US Acesso em: 20 maio de 2021.

HISTÓRIA DA INTERNET DO BRASIL Disponível em: https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html Acesso em: 20 de jun. 2020.

HOUAISS, Antônio. **Dicionário Houaiss** da Língua Portuguesa. Rio de Janeiro, Ed. Objetiva, 2001. Acesso em: 20 jun de 2021.

JORNAL NACIONAL (São Paulo) (ed.). **Empresa diz que mais de 100 milhões de brasileiros tiveram dados de celulares expostos**. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/10/empresa-diz-que-mais-de-100-milhoes-de-brasileiros-tiveram-dados-celulares-expostos.ghtml. Acesso em: 10 mar. 2021.

KUNSCH, Margarida Maria Krohling. **Planejamento De Relações Públicas Na Comunicação Integrada**. São Paulo: Summus, 2003.

LÉVY, Pierre. **O Que é Virtual?** Rio de Janeiro: Editora 34. 1996.

LEVY, Pierre. **A inteligência coletiva**. São Paulo: Edições Loyola, 1998.

LEVY, Pierre. **A máquina universo**. Porto Alegre: ArtMed, 1998.

MICROSOFT, **Termos e políticas de privacidade**. 2021. Disponível em: https://privacy.microsoft.com/pt-br/privacystatement. Acesso em: 12 fev. 2021.

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar. São Paulo: Pearson Education, 2003.

MORENO, João Brunelli. **A história do ENIAC: o primeiro computador do mundo. o primeiro computador do mundo**. 2011. Disponível em: https://tecnoblog.net/56910/eniac-primeiro-computador-do-mundo-completa-65-anos/. Acesso em: 10 fev. 2021.

OLIVEIRA, Gabriella Domingos de *et al*. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO**: perspectivas baseadas na tecnologia da informação (t.i.). 2012. 12 f. TCC (Graduação) - Curso de Biblioteconomia, Universidade Federal do Rio Grande do Norte (Campus Natal), Natal, 2012. Acesso em 10 mar. 2021

ROCHA, DOUGLAS. ENGENHARIA SOCIAL: **COMPREENDENDO ATAQUES E A IMPORTÂNCIA DA CONSCIENTIZAÇÃO**. Disponível em: < https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm>. Acesso em: 21/07/2021.

ROSA, Emanuel Motta da. **Lei de acesso à informação: Diretrizes dos procedimentos de acessibilidade à informação** (art. 3o). 2014. Disponível em:. Acesso em: 11 mar. 2021.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital**. Trad. de Daniel Vieira. Rio de Janeiro: Campus, 2001.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva** - 2 ed. São Paulo: Elsevier, 2014.

SILVA, Pedro Tavares; CARVALHO, Hugo. TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial**. Portugal: Centro Atlântico, 2003.

STALLINGS, William. **Criptografia e segurança de redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

Software One. **O que é virtualização** 2020. Disponível em: https://blogbr.softwareone.com/virtualizacao-2. Acesso em: 19 jun. 2020

VEJA (São Paulo) (ed.). **Como se proteger de aplicativos que exageram na coleta de dados** pessoais. 2021. Disponível em: https://veja.abril.com.br/tecnologia/como-se-proteger-de-aplicativos-que-exageram-na-coleta-de-dados-pessoais/. Acesso em: 10 mar. 2021.

WHATSAPP. **Criptografia de ponta-a-ponta**, FAQ (Geral). Disponível em: <https://www.whatsapp.com/faq/pt_br/general/28030015>.Acesso em: 29 set. 2020.

APÊNDICES

APÊNDICE A – formulário para coleta de dados

Qual a sua idade?

◯ De 15 a 25 anos ◯ De 26 a 35 anos ◯ De 36 a 50 anos

◯ Acima de 50 anos

Qual seu estado civil?

◯ Solteiro (a) ◯ Casado(a) ◯ Divorciado(a) ◯ Viúvo(a)

Qual seu sexo?

◯ Masculino ◯ Feminino

Qual sua residência?

◯ Cidade ◯ Zona Rural

Com que frequência você utiliza as redes sociais (Facebook, Instagram, WhatsApp)?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre

◯ Sempre

Você deixa suas informações pessoais nas redes sociais em modo público?

◯ Sim ◯ Não

Você utiliza datas comemorativas como senha em aplicativos?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre ◯ Sempre

Você costuma deixar seus dados visíveis em suas redes sociais (telefone, endereço, emprego, relacionamento)?

◯ Visível somente para amigos ◯ Visível a todos (Público) ◯ Somente eu

◯ Não costumo informar esse tipo de dado ◯ Não sei informar

Você adiciona pessoas desconhecidas em suas redes sociais?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre

◯ Sempre

Você acessa suas redes sociais usando internet pública (shopping, bares, restaurantes, rodoviárias)?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre ◯ Sempre

Você costuma dar permissão de acesso aos seus dados para sites e aplicativos desconhecidos?

◯ Nunca ◯ As vezes ◯ Sempre

Costuma marcar sua localização (check-in)?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre ◯ Sempre

Você costuma passar informações pessoais nas redes sociais (telefone, endereço, documentos pessoais, cartão de banco)?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Quase sempre ◯ Sempre

Você utiliza recursos de privacidade (marcação de pessoas, verificação em duas etapas, quem pode ver sua lista de amigos)?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Sempre ◯ Não sei informar

Você costuma salvar suas senhas no navegador de internet?

◯ Nunca ◯ Raramente ◯ As vezes ◯ Sempre ◯ Não sei informar