UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

LUCIANA ORDAKOWSKI SCHUH

VULNERABILIDADE DIGITAL: ESTUDO DA PERCEPÇÃO DE SEGURANÇA DIGITAL DO JOVEM EM PORTO ALEGRE – RS

Porto Alegre

2017

LUCIANA ORDAKOWSKI SCHUH

VULNERABILIDADE DIGITAL: ESTUDO DA PERCEPÇÃO DE SEGURANÇA DIGITAL DO JOVEM EM PORTO ALEGRE – RS

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciências Administrativas na Universidade Federal do Rio Grande do Sul, como requisito parcial para obtenção de grau de bacharel em Administração.

Orientador: Daniela Callegaro de Menezes

Porto Alegre
2017

LUCIANA ORDAKOWSKI SCHUH

VULNERABILIDADE DIGITAL: ESTUDO DA PERCEPÇÃO DE SEGURANÇA DIGITAL DO JOVEM EM PORTO ALEGRE – RS

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Trabalho de Conclusão de Curso defendido e aprovado em: _____

Banca examinadora:

_____
Profª. Drª. Daniela Callegaro de Menezes
Orientador
(UFRGS)

_____
Prof. (titulação). (Nome do membro da banca)
(sigla da instituição)

_____
Prof. (titulação). (Nome do membro da banca)
(sigla da instituição)

AGRADECIMENTOS

Agradeço aos meus pais, Mirian e Mauri, por me ensinarem a sempre valorizar os estudos, assim como respeitar meus colegas e professores ao longo da minha vida. Agradeço por todo amor e carinho. Agradeço por terem me proporcionado muitas experiências, por todas as oportunidades e por terem aberto mão de suas próprias vontades e limitações em prol dos meus sonhos.

Agradeço a minha irmã, Letícia, por ser meu principal exemplo de força, determinação e coragem para ir em busca dos meus sonhos, não desistir e sempre olhar pelo lado bom das coisas, mesmo que à distância. Agradeço por ter sido a melhor guia de Paris, a melhor companheira de aventuras na Grécia e Turquia e a melhor convidada que tive em Lisboa no período de intercâmbio. *Close your eyes, pretend to fly*.

Agradeço ao meu irmão, Marcelo, por ter sido meu principal companheiro durante o período de faculdade. Morar contigo não é fácil, mas é muito boa a nossa parceria. Principalmente pra comer xis. Agradeço por ser o melhor engenheiro e técnico de todos os enjambres e me ajudar toda vez que meu computador estragou.

Agradeço aos meus tios, Marlene e Sidnei, por terem me dado alguns equipamentos para estudo, meus companheiros de almoços no final de semana e por terem sido meus conselheiros de carreira e de vida.

Agradeço à Maria, minha segunda mãe, por ter me criado, me educado, me tornado um ser humano melhor. Agradeço por ter me mostrado o “outro lado da vida”, por fazer parte da construção do meu caráter e por me mostrar que simplicidade e humildade são valores mais importantes do que beleza ou riqueza.

Agradeço a toda minha família por torcerem por mim.

Agradeço a todas as minhas amigas e amigos por tudo. Agradeço pela fidelidade, parceria e carinho. Agradeço pelos momentos de alegria, pelo suporte nos momentos de tristeza e estresse. Agradeço por todas as caronas. Agradeço por serem minha família e por emprestarem as suas famílias quando eu estive longe da minha.

Agradeço a minha fiel escudeira e colega de faculdade, Lívia. Agradeço por todos os semestres ao meu lado. Agradeço por todas as caronas – todos os dias.

Agradeço pelas tardes de estudo, pelos cafés e pelas dicas de saúde. Agradeço por ter ido comigo pra Lisboa, encarar uma vida diferente, sair da zona de conforto, morar em uma casa imunda e velha com mais 24 jovens e por ter sido a melhor experiência das nossas vidas. Agradeço por ter criado e validado a frase das nossas vidas, por ter acreditado e me ajudado a acreditar que no fim tudo dá certo. E dá certo mesmo. Agradeço por ter se tornado uma amiga de fé. Da UFRGS pra vida.

Agradeço a meus colegas de trabalho, principalmente ao time de Alianças da Dell CSB Brasil. Agradeço por tornarem os dias mais leves, o trabalho mais prazeroso e a vida mais interessante de se viver. Agradeço por confiarem em mim, me darem suporte, me darem seus *feedbacks* sinceros, por quererem meu bem. Agradeço pelos mimos de “caçula” e pelos almoços e Happy Hours. Agradeço pela parceria.

Agradeço a todos os professores que eu já tive a oportunidade de ter aula e de trocar experiências em sala de aula. Agradeço principalmente aos professores Daniela Callegaro e Leonardo Nicolao, por aceitarem participar deste desafio comigo e por me ajudarem a escrever um trabalho lindo, o qual tive muito prazer e orgulho de ter desenvolvido.

E por fim, agradeço a Deus. Pela vida, pelas oportunidades e pelas certas pessoas ao meu redor.

RESUMO

O tema da monografia que segue trata do estudo sobre a percepção de jovens porto-alegrenses sobre segurança digital, considerando o contexto da rápida evolução tecnológica. É uma pesquisa que engloba apenas jovens por apresentarem como característica principal o uso constante de internet e de novas tecnologias. O objetivo geral é analisar a percepção de segurança digital, assim como identificar os fatores motivadores e inibidores do consumo de *softwares* de segurança. O método utilizado é entrevista em profundidade e técnica de sondagem com informantes jovens de classe A e B entre 18 a 30 anos moradores de Porto Alegre – RS. Os resultados revelam que a maioria dos informantes se sentem seguros ao navegar na internet, apesar de todos já terem sido afetados por vírus no passado e já terem usado algum *software* de segurança. Os principais aspectos que influenciam a decisão dos jovens na compra de *software* de segurança são a garantia de proteção, a interação do usuário com o produto, a performance da máquina e notificações a cada ação do *software.* A partir destes aspectos chaves, podem ser considerados pelos jovens como motivadores ou inibidores em um processo de compra, dependendo conforme o produto se manifesta. Com base nos resultados, são apresentadas recomendações de implementação de ações de Marketing específicas para empresas do ramo de *software* de segurança, fundamentadas em três pilares principais, tais como informação da temática, relacionamento com os clientes e conversão de vendas.

Palavras-chave: Percepção; Segurança; Digital; Jovem; *Software*. Motivadores e Inibidores.

ABSTRACT

The theme of the thesis that follows deals with the study on the perception of young people from Porto Alegre about digital security, considering the context of fast technological evolution. It is a research that only includes young people because they have as main characteristic the constant use of the internet and new technologies. The general goal is to analyze the perception of digital security and also to identify the motivating and inhibitors factors of the consumption of security software. The method used is an in-depth interview and a polling technique with young respondents of social class A and B between 18 and 30 years old, living in Porto Alegre - RS. The results reveal that most informants feel safe when surfing the internet, although everyone has already been affected by viruses in the past and has already used some security software. The main aspects that influence young people's decision to purchase security software are the guarantee of protection, user interaction with the product, machine performance and notifications for each action of the software. From these key aspects, they can be considered by young people as motivators or inhibitors in a buying process, depending on how the product manifests itself. Based on the results, recommendations are presented for the implementation of specific Marketing actions for companies in the security software business, based on three main pillars, such as information on the subject, customer relationship and sales conversion.

Key-words: Perception; Security; Digital; Young; Software; Motivational and Inhibitor.

LISTA DE ILUSTRAÇÕES

Figura 1 – Processo de Percepção

Figura 2 – Processamento de informação pelo consumidor

Figura 3 – Princípios para o Mercado de Tecnologia

Figura 4 – Taxa de adoção de um produto ou serviço baseado em tecnologia

Figura 5 – Finalidades de uso de internet

Figura 6 – Percepção de “*Software* de segurança”

Figura 7 – Percepção de “Antivírus”

Figura 8 - Pilares do plano geral de Marketing

Figura 9 – Plano de ações de Marketing

LISTA DE TABELAS

Tabela 1 – Lista de Entrevistados

Tabela 2 – Atividades *online* por dispositivo

Tabela 3 – Motivadores do consumo de *Softwares* de Segurança

Tabela 4 – Inibidores do consumo de *Softwares* de Segurança

LISTA DE GRÁFICOS

Gráfico 1 – Acesso de dispositivos para uso pessoal

Gráfico 2 – Acesso de dispositivos para uso profissional

SUMÁRIO

1 INTRODUÇÃO 14

1.1 DELIMITAÇÃO DO TEMA DE ESTUDO 15

1.2 OBJETIVOS 16

1.2.1 Objetivo Geral **16**

1.2.2 Objetivos Específicos **16**

1.3 JUSTIFICATIVA 16

2 FUNDAMENTAÇÃO TEÓRICA 19

2.1 PERCEPÇÃO 19

2.1.1 Conceito de Percepção **19**

2.1.2 Características de Percepção **22**

2.2. MARKETING E A TECNOLOGIA 23

2.2.1 Comportamento do Consumidor de Tecnologia **26**

2.2.2 Disposição para Tecnologia **27**

2.3. SEGURANÇA 29

2.3.1 Segurança de Dados **29**

2.3.2. Relação de consumo e falhas na segurança digital **31**

2.4 MERCADO DE *SOFTWARE* 33

2.4.1 Classificação de *Software* **33**

2.4.1.1 Produtos de Software **33**

2.4.1.2 Serviços de Software **34**

2.4.1.3 Software Embarcado **34**

3 PROCEDIMENTOS METODOLÓGICOS **35**

3.1 CLASSIFICAÇÃO DE PESQUISA **35**

3.2 MÉTODO DE PESQUISA **36**

3.3 TÉCNICA DE COLETA DE DADOS **37**

3.4 SELEÇÃO DE INFORMANTES **38**

3.5 ANÁLISE DE DADOS **38**

4 ANÁLISE DOS RESULTADOS **40**

4.1 HÁBITOS DE USO DE INTERNET **40**

4.1.1 Finalidades de uso da internet **40**

4.1.2 Acesso por dispositivos **42**

4.1.3 Frequência de uso **44**

4.1.4 Acesso de sites e aplicativos **46**

4.1.5 Administração dos dados *online* **47**

4.1.5.1 Redes sociais **47**

4.1.5.2 Dados bancários **48**

4.1.5.3 *Backup* de dados **49**

4.1.5.4 Senhas **50**

4.2 PENETRAÇÃO E ADERÊNCIA DE *SOFTWARE* DE SEGURANÇA NO SEGMENTO JOVEM **51**

4.2.1 Navegação e segurança **51**

4.2.2 Ataques virtuais 53

4.2.3 Experiências com *softwares* de segurança 54

4.2.3.1 Busca por informações 57

4.2.3.2 Momento de compra 58

4.2.3.3 Experiências de uso 60

4.2.3.4 Ambiente de trabalho 60

4.3 FATORES MOTIVADORES E INIBIDORES NO PROCESSO DE COMPRA DE *SOFTWARE* DE SEGURANÇA 62

5 CONSIDERAÇÕES FINAIS 67

5.1 LIMITAÇÕES DO ESTUDO 71

5.2 RECOMENDAÇÕES NA IMPLEMENTAÇÃO DE AÇÕES DE MARKETING ESPECÍFICAS PARA EMPRESAS DO RAMO DE *SOFTWARE* DE SEGURANÇA 72

5.2.1 Ações de informação 73

5.2.1.1 Canais de comunicação 73

5.2.1.2 Conteúdo 74

5.2.2 Ações de relacionamento 75

5.2.3 Ações de conversão 76

5.2.4 Ações 360° 77

5.3 SUGESTÕES PARA FUTURAS PESQUISAS 79

REFERÊNCIAS 81

APÊNDICE A – ROTEIRO DE ENTREVISTA DIRIGIDA AO CONSUMIDOR FINAL 84

1 INTRODUÇÃO

Os satélites, as fibras óticas e a rede de internet marcam o avanço tecnológico do novo milênio. Computadores, smartphones e tablets estão progressivamente mais acessíveis. A magnitude da mudança tecnológica, que nas últimas décadas afetou os meios de criação, transmissão e processamento do conhecimento, trouxe o aumento de mídia digital que promoveu uma aceleração das transmissões, densificação de conexões e capacidade de gerenciamento do conhecimento (UNESCO, 2005).

Em contrapartida, por consequência do uso exacerbado da internet, através de computador e dispositivos móveis, os usuários acabam por expor seus dados pessoais nas redes. Segundo Gartner, atualmente, por estarem adequadas a esta situação tecnológica, as pessoas não percebem sua exposição com relação às ameaças virtuais e muitas vezes não refletem sobre a temática da segurança digital.

Neste contexto, este estudo busca compreender a percepção do público jovem sobre segurança digital, com o intuito de analisar os fatores motivacionais ou inibidores de um processo de aquisição de *software* de segurança. Esta discussão é pertinente devido aos números crescentes quanto ao acesso à internet, assim como aos ataques virtuais a nível mundial.

Segundo Day (1970), a percepção é o conjunto de processos pelos quais os indivíduos mantêm contato com o ambiente. O caráter individual é uma característica da percepção, pois cada pessoa pode captar o mesmo cenário de forma única e inteiramente particular. Fernandes e Pelissari (2003) concordam e afirmam que cada pessoa percebe, reage e responde de forma diferente às ações sobre o ambiente que vive.

Para atingir os objetivos deste trabalho e compreender tais influências, foi utilizada a abordagem de levantamento de experiências de jovens entrevistados. A técnica utilizada é a sondagem, escolhida a fim de compreender o cenário a partir de cada indivíduo referente ao tópico em discussão. A escolha da metodologia de pesquisa está diretamente relacionada a este objetivo.

A estrutura deste trabalho é formada pela delimitação do tema de estudo, seguido pela justificativa e descrição dos objetivos gerais e específicos de pesquisa. Posteriormente é apresentada a revisão teórica, fundamentada em autores que retomam os conceitos de percepção do consumidor, marketing e tecnologia, comportamento do consumidor de tecnologia, análise de segurança e mercado de software. A revisão teórica é seguida pelo detalhamento da metodologia escolhida, a análise de resultados, os quais apresentam as informações coletadas através das entrevistas. Por fim, são retratadas as considerações finais, citando as limitações do estudo, sugestões de continuação da pesquisa e recomendação de ações com base nas conclusões dos resultados.

1.1 DELIMITAÇÃO DO TEMA DE ESTUDO

Segundo a publicação de março deste ano no site da consultora Teleco – Inteligência em Telecomunicações, em 2016 foram vendidos cerca de 43,5 milhões de smartphones e 4,9 milhões de celulares tradicionais. Isso significa um crescimento anual de 11,2% no total de aparelhos telefônicos, com base nos dados do IDC Brasil.

A realidade na região Sul do país, segundo dados do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – CETIC, com relação ao acesso à internet em domicílio é que 53% possui acesso à internet. Com relação à frequência no uso, 77% acessa a internet todos ou quase todos os dias. Com relação à posse de aparelho celular, 87% dos indivíduos afirmam possuir, sendo 79% os que acessam a internet pelo celular todos ou quase todos os dias.

Com relação ao número de dispositivos conectados à internet, a empresa global de consultoria de tecnologia - Gartner, afirma que haverá uma futura explosão do número de dispositivos inteligentes que criará uma rede rica em informações. A consultora também prevê um aumento de 30 vezes em dispositivos físicos conectados à Internet até 2020, ou seja, a Internet das Coisas deverá chegar a 26 bilhões de unidades instaladas até 2020 e impactará significativamente o acesso à informação da cadeia de suprimentos e a exposição a riscos cibernéticos.

Neste contexto, a partir da relevância do mercado de segurança virtual e visto o crescimento de ameaças no âmbito digital, o tema proposto a ser estudado é “Vulnerabilidade Digital: estudo da percepção de segurança digital do jovem em Porto

Alegre – RS”. Portanto, a realização deste estudo tem como finalidade compreender a percepção dos consumidores jovens entre 18 e 30 anos em relação à segurança digital a partir da interação com a internet em computadores e dispositivos móveis e identificar os principais fatores que motivam ou inibem uma compra de *softwares* de segurança.

1.2 OBJETIVOS

Apresentam-se neste capítulo os objetivos que norteiam o foco do trabalho. Os objetivos são divididos em geral e específicos, sendo o objetivo geral o que descreve de forma mais ampla o que se almeja estudar e os específicos direcionam o pesquisador a responder o problema de pesquisa.

1.2.1 OBJETIVO GERAL

Analisar a percepção de segurança digital do jovem em Porto Alegre – RS.

1.2.2 OBJETIVOS ESPECÍFICOS

I- Identificar as finalidades de uso da internet pelos consumidores jovens;
II- Identificar por quais dispositivos consumidores jovens acessam a internet;
III- Identificar quais os sites mais navegados pelos consumidores jovens;
IV- Identificar com que frequência consumidores jovens acessam a internet;
V- Verificar a penetração dos produtos de proteção no âmbito digital no segmento de consumidores jovens;
VI- Verificar a aderência dos produtos de proteção no âmbito digital no segmento de consumidores jovens;
VII- Identificar os fatores motivadores e inibidores do consumo de *softwares* de segurança por jovens.

1.3 JUSTIFICATIVA

Com a tecnologia cada vez mais avançada e mais presente na vida dos brasileiros, possibilitando não só o uso da internet, por exemplo, para navegar em sites e mandar mensagens simples, como também para fazer transações

bancárias, entre outras aplicações mais avançadas, os dados e informações dos usuários acabam estando em risco de serem apropriados por malfeitores digitais para uso indevido. Dessa forma, tamanha a atual exposição de informações pessoais, há um mercado crescente de ameaças digitais, chamado cybercrime ou crime cibernético.

Em consulta às bases de dados, tais como pesquisas voltadas ao tema de segurança *online*, artigos sobre tendências de mercado digital, sites que revelam estatísticas e acervos bibliográficos acerca de temas que envolvem este projeto - tecnologia, internet, segurança digital e percepção, foram encontradas informações de que a disseminação acerca das informações sobre tecnologia no Brasil, principalmente sobre *software* de segurança para multi-dispositivos, ainda é muito baixa, acarretando então uma parcela baixa de pessoas em busca por proteção digital. Além disso, não há estudos atualizados sobre a percpeção de segurança digital ou elementos que influenciam na compra de *softwares* de segurança, o que leva a seguinte questão: **“Como os jovens percebem segurança digital?”**

Estudar e pesquisar a percepção dos jovens porto-alegrenses entre 18 e 30 anos poderá trazer dados relevantes acerca do assunto, tais como hábitos de consumo de internet, comportamento e percepção acerca de segurança digital e fatores influentes no possível processo de compra de *softwares* de segurança. Este trabalho também tem a finalidade de disseminar tais resultados entre empresas de tecnologia que oferecem produtos de segurança digital, a fim destas planejarem uma melhor comunicação de seus *softwares*, assim, sendo mais efetivas no oferecimento do produto e benefícios a partir do foco na mensagem para os jovens.

Empresas que ofertam produtos e serviços de tecnologia têm acesso às informações de mercado com relação a dados estatísticos de crescimento, índices de penetração e pesquisas de posicionamento e lembrança de marcas a partir da perspectiva dos consumidores. Porém, acabam não tendo acesso a estudos mais específicos sobre um segmento de mercado, região especial ou aderência de um tipo de produto em particular porque existem poucas ou nenhuma pesquisada voltadas a tais características singulares.

Desse modo, tais empresas na área de tecnologia podem ampliar seus conhecimentos sobre o mercado de segurança digital e desenvolver planos estratégicos para aumentar as vendas de seus produtos, assim como educar os usuários sobre o assunto, visto que é bastante pertinente no atual contexto. Além do mais, ao saber sobre os hábitos e características de tal público, o qual tem representatividade considerável na compra de computadores, tablets e smartphones em Porto Alegre, as empresas podem enriquecer seus argumentos de vendas.

Portanto, a pesquisa elaborada neste contexto é considerada válida, dado que não há estudos acadêmicos sobre a percepção na esfera de proteção digital, assim como há escassez de informações sobre fatores influenciadores em um processo de compra de um produto de tecnologia.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem o objetivo de reunir o conteúdo teórico existente e de relevância sobre o contexto delimitado para a pesquisa, a fim de promover tanto uma melhor contextualização e embasamento das variáveis que fazem parte deste estudo quanto fundamentar os conceitos e alinhar o entendimento sobre os mesmos. Para auxiliar nas análises do presente estudo, serão apresentados alguns dos conceitos e características sobre a percepção, a qual pode-se dizer que está muito vinculada com o contexto do indivíduo, suas experiências passadas, o ambiente em que vive e suas características fisiológicas; a abrangência do marketing em função do contexto tecnológico e como se dá o comportamento do consumidor de tecnologia; dados sobre segurança e como isso se reflete no consumidor e por fim, uma breve revisão dos principais conceitos acerca o mercado de *software*.

2.1 PERCEPÇÃO

As preferências de compras de um indivíduo são influenciadas principalmente pelos seguintes fatores psicológicos: motivação, percepção, aprendizagem, crenças e atitudes. A motivação é uma necessidade que é despertada quando existe uma disparidade entre o estado almejado de ser e o estado real (CARO, 2005, p. 35).

Para Kotler (2005, p. 194), uma necessidade transforma-se em um motivo quando atinge um determinado grau de intensidade. O motivo é uma necessidade que é importante o bastante para levar a pessoa a agir, e um indivíduo motivado significa que está pronto para agir. A maneira como o indivíduo motivado realmente age é influenciada pela percepção que ele tem da situação.

Estudar e compreender como os consumidores percebem os produtos e serviços que estão sendo constantemente ofertados sempre foi um desafio para especialistas de marketing devidos aos inúmeros fatores que englobam o processo perceptual. Sendo assim, é um assunto de grande relevância, abordado por muitos autores.

2.1.1 Conceito de Percepção

A percepção é o processo psicológico em que estímulos são selecionados, dados são organizados em padrões reconhecíveis e as informações resultantes são

interpretadas pelo indivíduo (CERTO, 2003, p. 402). Segundo Belch (2008, p. 112), é um processo pessoal que está diretamente ligado a fatores internos como crenças, experiências, necessidades, humores e expectativas de uma pessoa.

Bowditch e Buono (1992), entretanto, afirmam que a percepção é determinada pela interação de fatores psicológicos e fisiológicos. O aspecto fisiológico da percepção engloba o que as pessoas são capazes de ver, ouvir, cheirar e sentir. Apesar de certa limitação, as informações coletadas pelos órgãos dos sentidos são armazenadas e serão processadas conforme o conjunto de crenças, valores e atitudes pessoais, moldados por experiências culturais e ambientais.

Segundo Karsaklian (2000), o mecanismo de percepção rege as relações entre o indivíduo e o meio que o cerca, e todo o conhecimento e informação é adquirido através da percepção. O que o consumidor adquire reflete suas necessidades, a natureza dos produtos e serviços disponíveis ao seu redor e a forma como ele os percebe.

O processo perceptivo liga o indivíduo a seu ambiente e então é possível serem processados estímulos. Os estímulos percebidos são limitados e passam por filtros, os quais são determinados pela experiência, atitudes e crenças anteriores, levando ao comportamento do indivíduo, conforme mostra abaixo na figura 1 (CERTO, 2003).

Figura 1 – Processo de Percepção

Fonte: adaptado de Certo (2003, p. 403).

Dessa forma, a percepção pode ser considerada uma variável que intervém e influencia no processo de tomada de decisão de compra de um produto (KARSAKLIAN, 2000). Para Kotler (2005), a palavra que dá significado para percepção é o indivíduo, porque as pessoas podem ter diferentes perspectivas

referentes a um mesmo objeto e isso se deve a três processos: atenção seletiva, distorção seletiva e retenção seletiva.

A atenção seletiva diz respeito ao que acontece quando os consumidores escolhem direcionar sua atenção em certos tipos de estímulos e excluir outros. Estudos nesse campo afirmam que o consumidor comum é exposto a inúmeros estímulos por dia e só percebem ou prestam atenção em cerca de 5% dessas mensagens (BELCH, 2008, p. 112).

Existem maiores possibilidades de as pessoas notarem estímulos que se relacionem com uma necessidade atual. Kotler (2005, p. 195) exemplifica que um indivíduo que esteja motivado a comprar um computador prestará mais atenção em anúncios de computador e provavelmente não prestara atenção em anúncios de som.

É mais provável que as pessoas percebam estímulos que elas antecipam. O indivíduo possivelmente dará mais importância em anúncios de computador numa loja de computadores do que em anúncios de rádio, uma vez que não é esperado que em uma loja de computadores venda rádios (KOTLER, 2005, p. 195).

Além disso, mesmo que os consumidores prestem atenção nas mensagens, não existem garantias de que eles irão interpretá-la da maneira desejada e esse processo é classificado como *distorção seletiva*. Consumidores podem desenvolver uma compreensão seletiva, interpretando informações de acordo com suas próprias atitudes, crenças motivações e experiências (BELCH, 2008, p. 112).

Já a *retenção seletiva* ocorre quando os consumidores se recordam de todos os estímulos que ouvem, veem ou leem, depois de terem prestado atenção ou entendido os estímulos (BELCH, 2008, p. 112). Porém são propensos a guardar informações que sustentam suas crenças e atitudes. Ou seja, as pessoas tendem a lembrar dos pontos positivos colocados a respeito de um produto de que gostam e esquecer os pontos positivos relativos a produtos de concorrentes (KOTLER, 2005, p. 196).

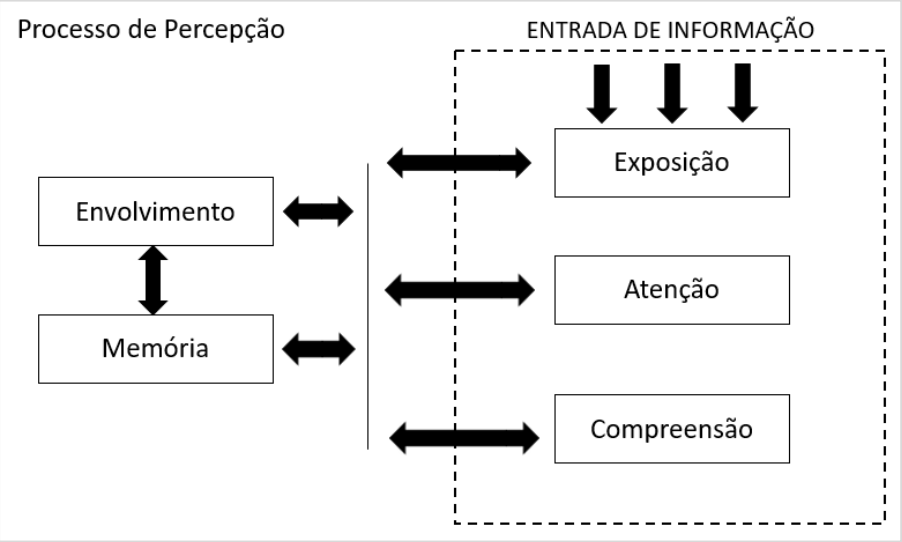
Faggionato (2005) e Oliveira (2005) acrescentam que as manifestações dos indivíduos são resultado de suas percepções, processo cognitivo, julgamentos e expectativas pessoais. Embora nem todas as manifestações sejam evidentes, elas

são constantes e afetam a conduta do indivíduo de forma inconsciente. As situações de percepção podem ser percebidas de acordo com as experiências passadas, expectativas e necessidades, além da influência de fatores circunstanciais.

As experiências positivas que os consumidores vivenciam com os produtos e serviços são o que fazem com que uns sejam mais desejados do que os outros. A percepção do consumidor sobre o mercado, produto e a marca são fatores determinantes para a tomada de decisão da compra, afirma Kotler (2005).

De acordo com Mowen e Minor (2003), há três fatores que influenciam o processamento de informação: percepção, nível de envolvimento do consumidor e memória. A percepção é o processo em que as pessoas são expostas a informações e assim pode-se dizer que prestam atenção e a compreendem, interpretando-a a fim de entender o seu significado. Tal processo pode ser observado abaixo na figura 2:

Figura 2 – Processamento de informação pelo consumidor



Fonte: adaptado de Mowen e Minor (2003, p. 44).

2.1.2 Características de Percepção

Cada pessoa tem sua própria imagem do mundo que deriva de uma série de variáveis próprias e exclusivas de cada um, como o ambiente físico e social, histórias e experiências anteriores, personalidade, próprias perspectivas psicológicas e fisiológicas (FAGGIONATO, 2005). Tais variáveis são integradas e resultam na estrutura cognitiva, a qual permite percepções de forma organizada e significativas e

assim se dá a interpretação da realidade por um indivíduo. De acordo com Karsaklian (2000, p.42), a percepção é composta das seguintes características:

a) Subjetiva: trata-se da maneira como o consumidor se apropria de um produto ou situação da qual fez uma realidade. Há discrepância entre o estímulo emitido pelo ambiente e aquele percebido pelo indivíduo (viés perceptual);
b) Seletiva: um indivíduo tem contato diário com diversas propagandas, percebendo somente algumas delas. As outras são ignoradas porque não correspondem a seus centros de interesse ou porque demandava muita concentração da parte do consumidor;
c) Simplificadora: uma pessoa não pode perceber todas as unidades de informação que compõe estímulos percebidos;
d) Limitada no tempo: uma informação percebida é conservada somente durante um certo tempo, geralmente curto, a menos que esse período seja desencadeado um processo de memorização;
e) Cumulativa: uma impressão é o somatório de diversas percepções. Um indivíduo gera sua própria impressão sobre determinado produto quando é exposto pela propaganda, quando escuta o que os outros têm a dizer sobre aquilo e quando examina a sua embalagem, por exemplo.

Karsaklian (2000) considera que o estado psicológico de um indivíduo é o fator predominante da percepção. As emoções, expectativas e motivos fazem com que a pessoa perceba preferencialmente certos estímulos do ambiente. A percepção de estímulos por sua vez é afetada pelas atitudes, que são avaliações próprias duradouras ou sentimentos e tendências proativas em relação a tal objeto ou situação.

Contudo, quando se trata de produtos com base tecnológica, além dos fatores ambientais em que o indivíduo se encontra, há fatores tecnológicos e informações deste contexto que também afetam e interferem tanto na percepção do consumidor quanto nas suas atitudes online.

2.2. MARKETING E A TECNOLOGIA

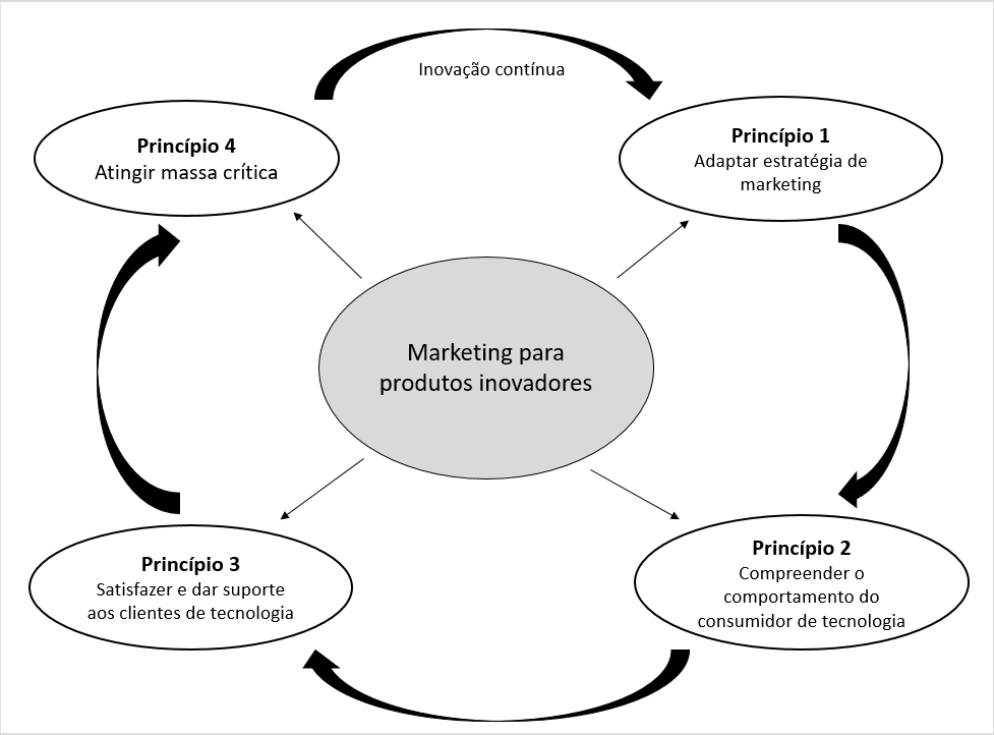
Blackwell, Miniard e Engel (2005, p. 10) definem marketing como “o processo de transformação ou mudança para que as pessoas vão comprar”. O objetivo do

marketing é satisfazer as necessidades e os desejos de seus clientes. O estudo do comportamento do consumidor permite conhecer as características dos compradores e seus processos de decisão de compra, possibilitando o desenvolvimento e comercialização de novos produtos.

O caráter do marketing para produtos e serviços inovadores é definido pelos autores Parasuraman e Colby (2002, p.17 e 18) a partir de quatro princípios básicos para o mercado de tecnologia. A figura 3 mostra como estes quatro princípios correspondem a uma prática de marketing:

a) A adoção de tecnologia é um processo distinto: o comportamento do cliente para um produto ou serviço baseado em tecnologia difere daquele para aceitação de um produto mais convencional;
b) As inovações de tecnologia exigem estratégias de marketing diferentes: as questões relacionadas ao projeto, ao preço, a comunicação, a distribuição e a assistência técnica de um produto ou serviço de tecnologia devem ser abordadas de forma específica, por envolver tecnologia no processo;
c) Garantir a satisfação do cliente é um desafio maior para o produto ou serviço baseado em tecnologia: os consumidores desses produtos precisam lidar com uma abordagem desconhecida e muitas vezes a satisfação de suas necessidades pode se tornar mais complexa. Esses clientes necessitam de treinamento e suporte técnico;
d) Os mercados de tecnologia são regidos pela lei da massa crítica, em que frequentemente o resultado é do tipo “o vencedor fica com tudo”: nesse mercado é comum uma empresa alcançar uma posição dominante, difícil de ser desafiada até a chegada de uma tecnologia completamente nova. As primeiras empresas a oferecer a nova tecnologia podem obter um sucesso relativo, porém no final, uma única empresa acaba com os concorrentes ou os coloca numa posição de nicho.

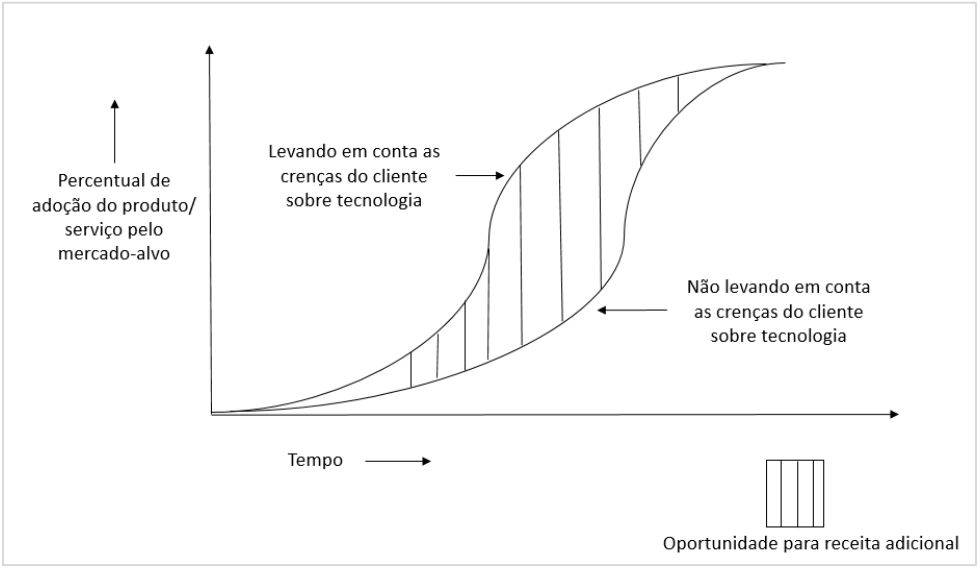
Figura 3 – Princípios para o Mercado de Tecnologia



Fonte: adaptado de Parasuraman e Colby (2002, p. 19).

Parasuraman e Colby (2002) afirmam que se uma empresa comercializa tecnologia de forma sintonizada com as necessidades dos clientes, ela irá aumentar sua adoção e atingir um volume de vendas muito maior. Ou seja, quando a empresa leva em conta as crenças e percepções do cliente sobre tecnologia, ela pode gerar diferencial competitivo e gerar maior receita, conforme mostra a figura 4, abaixo.

Figura 4 – Taxa de adoção de um produto ou serviço baseado em tecnologia



Fonte: adaptado de Parasuraman e Colby (2002, p.20).

2.2.1 Comportamento do Consumidor de Tecnologia

Segundo Kotler (2005, p. 182) a área do comportamento do consumidor estuda como as pessoas, grupos e organizações escolhem, comprar, usam e descartam artigos, serviços, ideias ou experiências. Marketing, conforme Mowen e Minor (2003), é o estudo das unidades compradoras e dos processos de troca envolvidos na obtenção, consumo e na disposição de mercadorias, serviços, experiências e ideias.

Para as empresas e os profissionais de marketing, é muito importante entender porque os indivíduos tomam suas decisões de consumo para que, depois, consigam decidir melhor as estratégias e abordagens de marketing. Estudar o comportamento do consumidor permite aos profissionais do marketing entender as fontes das percepções do consumidor e influenciá-las (CZINKOTA, 2001).

Para entender o comportamento do consumidor, é preciso entender como eles percebem, aprendem e tomam decisões para satisfazer suas necessidades e seus desejos. “São as necessidades e os desejos dos consumidores que os profissionais do marketing devem satisfazer.” (CZINKOTA, 2001, p. 139).

Uma vez que o comportamento do consumidor envolva caracteristicamente escolhas e tomada de decisão, o aspecto cognitivo tem um apelo particular para os anunciantes, notadamente para aqueles cujos produtos ou serviços envolvam importantes decisões de compra. Os processos cognitivos, tais como, concepção de crenças sobre a marca, desenvolvimento e mudança de atitude e integração, são importantes para se entender como o consumidor toma sua decisão em muitos tipos de compra (BELCH, 2008, p. 126).

Quando uma tecnologia é lançada no mercado, os consumidores reagem de maneiras diferentes. Parasuraman e Colby (2002) segmentaram o mercado em cinco grupos diferentes, sendo que cada segmento desempenha um papel distinto na movimentação de um novo produto baseado em tecnologia. Em ordem de adoção dos produtos existem os exploradores, os pioneiros, os céticos, os paranoicos e os retardatários.

Os denominados “exploradores” são os primeiros a usar as novas tecnologias, são as pessoas que se sentem atraídas e motivadas por novos lançamentos. Ao contrário dos exploradores, os “retardatários” são aqueles que são os últimos a adotar tais tecnologias. Parasuraman e Colby (2002) afirmam que muitas vezes esse tipo de cliente só compra o produto por falta de outras opções.

Os “pioneiros” são otimistas e possuem as tendências inovadoras dos exploradores, porém apresentam um grau de desconforto e insegurança em relação a esses produtos. Segundo os autores, esse segmento exige atenção especial dos profissionais de marketing, porque são atraídos para o uso desses lançamentos, porém necessitam de garantias e de ajuda a entender que a tecnologia pode trabalhar para seu benefício.

O segmento dos “céticos” é denominado por aqueles que não acreditam ou não sentem desejo por tais inovações. Não significa que são contra a tecnologia, porém esse grupo necessita ser convencido de que esses produtos novos podem beneficiá-los. A partir do momento que acreditam nisso, não há mais barreiras na adoção do produto.

Por fim, os “paranoicos” são aqueles consumidores otimistas em relação à tecnologia, porém sentem alto grau de desconforto e insegurança, além de não apresentarem tendências de inovação. Neste segmento, os profissionais de marketing não precisam convencê-los de usar os produtos, porém precisam oferecer apoio e garantias técnicas de funcionamento.

2.2.2 Disposição para Tecnologia

A disposição das pessoas para tecnologia descreve o processo comportamental distinto pressuposto na adoção de produtos ou serviços baseados em tecnologia (PARASURAMAN; COLBY, 2002, p.25). É a essência do marketing para produtos inovadores, ou seja, envolve crenças e comportamentos dos consumidores com relação a esse mercado.

A disposição para tecnologia refere-se à propensão que as pessoas têm em adotar e usar novas tecnologias para alcançar seus objetivos. Assim, é abordada a partir de três itens, sendo os autores Parasuraman e Colby (2002).

a) A disposição para tecnologia varia de indivíduo para outro: qualquer pessoa pode ser consumidor de uma nova tecnologia, porém o caminho de adoção através do marketing vai depender do grau e da natureza de tal disposição de cada um. Algumas pessoas buscam por tecnologia de forma ativa, outros necessitam de ajuda ou persuasão.
b) A disposição para tecnologia é multifacetada: não é somente uma tendência de um indivíduo ser “inovador” ou “os primeiros a adotar” tecnologia. Hábitos, crenças e motivações pessoais misturam-se para produzir a disposição de uma pessoa.
c) A disposição para tecnologia prevê e explica a resposta do consumidor para novas tecnologias: pode-se prever um percentual de adoção de novas tecnologias e ser explicado como é usada. A disposição está associada ao grau de satisfação do cliente com a tecnologia e aos tipos de suporte que lhe é exigido.

Parasuraman e Colby (2002, p.32) também desenvolveram o Índice de Disposição para Tecnologia em uma de suas pesquisas. Tal índice mostra a propensão das pessoas em adotar e usar novas tecnologias, tanto em casa quanto no trabalho. A partir dessa análise, descobriram que essa escolha é muito mais relacionada ao psicológico do que à habilidade da pessoa. Uma combinação de crenças, tanto positivas quanto negativas, define a adoção desses produtos.

Essas crenças foram identificadas em quatro elementos distintos, sendo dois deles contribuintes e dois inibidores do consumo de tecnologia:

a) Otimismo: esse sentimento oferece às pessoas a ideia de que a tecnologia é uma coisa boa e oferece maior controle, flexibilidade e eficiência em suas vidas. O estudo conclui que essa crença varia de acordo com a idade, sendo mais observada nos entrevistados mais jovens;
b) Inovação: faz referência à ideia de as pessoas estarem experimentando lançamentos de produtos ou serviços que tenham tecnologias. Essas pessoas acabam se tornando líderes de opinião por acompanharem os novos produtos e por estarem abertos a novas tecnologias;
c) Desconforto: essa crença mostra que as pessoas sentem que a tecnologia não é feita para todos, usá-la pode ser complicado e, pela falta de

capacidade, acaba sendo necessário um conhecimento avançado para sua utilização. Para alguns, elas são tão complicadas que acabam não sendo úteis;

d) Insegurança: esse fator inibidor é entendido como uma desconfiança a respeito da capacidade da tecnologia em funcionar corretamente. Este sentimento está ligado ao funcionamento do sistema e não à capacidade dos usuários em lidar com a tecnologia.

Definem insegurança como “desconfiança e ceticismo a respeito da capacidade da tecnologia em funcionar corretamente” (PARASURAMAN; COLBY, 2002, p.43). O sentimento de insegurança está vinculado especialmente no contexto da Internet e do comércio eletrônico, em que os consumidores não consideram seguro dar o número do cartão de crédito pelo computador ou não estão confiantes em fazer negócios online.

2.3. SEGURANÇA

Segundo Avizienis (2004), segurança é uma composição de atributos de confidencialidade, integridade e disponibilidade que requer a existência concorrente de disponibilidade somente para ações autorizadas, confidencialidade e integridade contra acesso não autorizado. Já Stoneburner (2002, p. E-1, tradução nossa) apresenta um conceito mais amplo, a qual “Segurança em sistemas de informação é uma característica de sistema e um conjunto de mecanismos que abrangem o sistema tanto lógica como fisicamente”. Serão apresentados os cinco objetivos de segurança, os quais fornecem uma noção mais restrita: integridade, disponibilidade, confidencialidade, responsabilidade e garantia.

2.3.1 Segurança de Dados

Existem diversos conceitos que caracterizam segurança de dados. Abaixo é apresentada uma lista de conceitos abordados pelos autores citados anteriormente.

A confidencialidade se caracteriza por “a ausência de divulgação não autorizada de informações.” (AVIZIENIS, 2004, p. 3, tradução nossa). Em Goodrich (2010) confidencialidade é definida como proteção de dados, ou seja, prover acesso às informações somente a quem possui permissão. Para atingir esse objetivo,

diversos conceitos estão envolvidos, tais como criptografia, controle de acesso, autenticação, autorização e segurança física.

A integridade se caracteriza por “ausência de alterações inadequadas do sistema.” (AVIZIENIS, 2004, p. 3, tradução nossa). Goodrich (2010) também cita três conceitos envolvendo integridade: *backup, checksums* e códigos de correção de erros. Esses conceitos adicionais envolvem uma característica fundamental para se evitar alterações de dados: redundância, replicação de dados ou funções que possam ser detectadas como violações de integridade. Além de proteger os dados em si, é necessário manter a integridade dos dados de cada arquivo, isto é, informações de controle de acesso, de modificações, de proprietários, etc.

A disponibilidade é “prontidão para o serviço correto.” (AVIZIENIS, 2004, p. 3, tradução nossa). Segundo Godrich (2010) a disponibilidade é a propriedade que a informação possui de ser acessada e modificada constantemente por quem possui autorização. Para que a alta disponibilidade seja alcançada, dois conceitos fundamentais são: proteção fiscal e redundância computacional.

A responsabilidade pode ser considerada “disponibilidade e integridade da identidade da pessoa que realizou uma operação.” (AVIZIENIS, 2004, p. 14, tradução nossa). A garantia “justifica a confiança de que os outros quatro objetivos de segurança (integridade, disponibilidade, confidencialidade e responsabilidade) foram adequadamente atendidos por uma implementação específica. ‘Adequadamente atendidos’ inclui (1) funcionalidade que funciona corretamente, (2) proteção suficiente contra erros não intencionais (por usuários ou software), e (3) resistência suficiente à penetração ou a desvio.” (STONEBURNER, 2002, p. E-1, tradução nossa).

Segundo Goodrich (2010), a garantia no contexto computacional se refere a como é provida e gerenciada a confiança em sistemas computacionais. A confiança é uma característica difícil de se medir, no entanto, refere-se à percepção de que pessoas e que sistemas estão se comportando como esperado.

A autenticação é a “integridade de um conteúdo e origem da mensagem, e possivelmente de alguma outra informação, como o tempo de emissão.” (AVIZIENIS, 2004, p. 14, tradução nossa). Além do mais, em Goodrich (2010) autenticação é definido como a determinação da identidade ou do papel de alguém. Isso pode ser

realizado com uma combinação do que essa pessoa possui, com o que essa pessoa sabe e com o que essa pessoa é. Exemplo: *smartphone*, senha e impressão digital.

Criptografia, segundo Goodrich (2010) é definida como a transformação de informações usando um segredo, chamado chave de encriptação, para que as informações transformadas só possam ser lidas usando outro segredo, chamado chave de decriptação. Quando essas chaves de encriptação e decriptação são iguais, é chamado de chaves simétricas. Quando essas chaves são diferentes, são conhecidas como chaves assimétricas.

Backup é a cópia e o arquivamento periódico de dados para que, em caso de alteração indesejada ou não autorizada, eles possam ser restaurados. *Checksums* são definidos como a computação de uma função que mapeia o conteúdo de um arquivo para um número. Uma função *checksum* depende do conteúdo do arquivo de modo que qualquer alteração realizada sobre ele possui uma alta probabilidade de resultar num número diferente. Dessa maneira, é possível detectar alterações não permitidas em arquivos (GOODRICH, 2010, tradução nossa).

Segundo Goodrich (2010), o controle de acesso pode ser definido como regras e políticas que limitam o acesso a informações confidenciais às pessoas ou aos sistemas autorizados. Já a assinatura digital é considerada uma computação criptográfica que permite a uma pessoa ou a um sistema autenticar seus documentos de uma maneira única e não repudiável.

2.3.2. Relação de consumo e falhas na segurança digital

Um estudo feito pela Gemalto, companhia de segurança internacional, apontou que, para 70% dos consumidores entrevistados, os sites devem ser responsáveis por garantir a segurança online do usuário, ou seja, enquanto eles navegam na internet. Apenas 30% atribui essa responsabilidade a si próprios. Além disso, mais da metade das entrevistados (58%) afirmou acreditar que serão vítimas de perda de informações pessoais no futuro.

Para a pesquisa foram entrevistadas 9.000 consumidores de 11 países, incluindo Alemanha, Arábia Saudita, Austrália, Benelux, Emirados Árabes Unidos, Estados Unidos, França, Índia, Japão, Reino Unido e Rússia. Com relação à falha de

segurança, 66% dos consumidores disseram que dificilmente fariam negócios com uma organização se informações consideradas sigilosas, tais como dados pessoais e financeiros fossem roubados após um ataque digital (GEMALTO, 2017).

Com relação a ataques *online*, 21% dos entrevistados disseram já ter sido afetados pelo uso indevido e fraudulento de suas informações financeiras e 15% do uso de suas informações pessoais. Entre aqueles que sofreram violação, 36% disseram ter sido vítimas de um site considerado inseguro, 34% foram afetados através de cliques em link malicioso e 33% por um método de phishing. Mais de um quarto dos entrevistados (27%) atribuiu o problema a uma falha nas soluções de segurança *online* nos dados do site onde navegavam.

Desde 2013, mais de 4,8 bilhões de dados foram expostos, sendo que roubo de identidade corresponde 64% dos ataques totais. Apesar disso, as empresas e internautas não estão totalmente informados sobre as principais medidas de segurança, considerada importantes, nem tem tomado medidas mais profundas para se protegerem. Apenas quando se trata de roubo de moeda digital, muitos dos usuários afetados reclamam nas redes sociais e pedem seu dinheiro de volta.

Segundo Bevilaqua (2008), quando a relação de consumo é considerada efetivada, o Código de Defesa do Consumidor se preocupa em proteger os consumidores contra os danos causados por produtos ou serviços e busca assegurar a reparação de eventuais prejuízos. O CDC atriui ao fornecedor, fabricante, produtor ou importador a responsabilidade por danos sofridos pelo consumidor.

A responsabilidade diz respeito à existência de um defeito e nesse caso, o CDC considera a falha na segurança um defeito daquilo que foi adquirido, não importando a culpa do fornecedor ou de seus representantes. O código define duas esferas de proteção ao consumidor, a primeira buscando proteger a saúde e segurança. A segunda é voltada para a integridade econômica do consumidor, buscando resguardar seu patrimônio de prejuízos relacionados com a qualidade dos produtos ou serviços prestados, assegurando a equivalência entre prestação e contraprestação nas relações de consumo (BEVILAQUA, 2008).

2.4 MERCADO DE *SOFTWARE*

Abordar historicamente o mercado de *software* implica abordar também aspectos históricos de outros mercados relacionados, como o de computadores ou o de microeletrônica. Tais mercados alcançaram diversos avanços tecnológicos de forma a impactar positivamente o desempenho de computadores, viabilizando novas aplicações e estimulando o desenvolvimento do *software* (GUTIERREZ E ALEXANDRE, 2004).

A evolução da eletrônica tem sido marcada por um movimento de miniaturização dos circuitos e de crescente integração do *software* aos equipamentos. Dessa forma, são demandadas novas e mais complexas aplicações de *software* para controlar esses circuitos e torná-los facilmente utilizáveis, difundindo o progresso tecnológico e ganhos de produtividade (GUTIERREZ E ALEXANDRE, 2003).

2.4.1 Classificação de *Software*

O *software* é uma sentença escrita em uma linguagem computável, para a qual existe uma máquina capaz de interpretá-la. O *software* é composto por uma sequência de instruções ou comandos e declarações de dados, armazenável em meio digital. Ao interpretar o *software*, a máquina computável é direcionada à realização de tarefas especificamente planejadas, para as quais o software foi projetado. (FERNANDES, 2002).

Conforme Gutierrez e Alexandre (2004), conforme a segmentação do modelo de negócios aplicado, pode-se dividir o *software* em três categorias de modelo de negócios: produtos, serviços e embarcado.

2.4.1.1 Produtos de Software

Os produtos de *software* podem ser divididos em categorias: infraestrutura e aplicativos. Entretanto, tais categorias podem mudar tendo em vista novos produtos que são lançados incorporando funcionalidades de outros e que a evolução de um produto leva à expansão de suas próprias funcionalidades, podendo tornar, em alguns casos, indefinidas as fronteiras entre os segmentos.

No segmento de infraestrutura são compreendidos os sistemas operacionais, programa de servidores, gerenciadores de redes, gerenciadores de armazenagem, gerenciadores de sistemas e programas de segurança (GUTIERREZ E ALEXANDRE, 2004, p. 7). Já o segmento de aplicativos compreende *softwares* especializados e destinados à execução de uma determinada tarefa, sendo suas entradas e saídas associadas à atividade humana. Assim, a usabilidade e a comunicação acessíveis desses *softwares* com seus utilizadores são muito importantes para a produtividade e disseminação do uso (GUTIERREZ E ALEXANDRE, 2004).

2.4.1.2 Serviços de Software

Os serviços profissionais de Tecnologia da Informação (TI) são as atividades tradicionais que demandam conhecimentos específicos relacionados a esse setor, tais como consultoria, desenvolvimento de aplicativos (*softwares* sob encomenda), integração, treinamento, suporte e manutenção técnica, entre outros. Com o crescimento e a disseminação da TI esses serviços facilitaram a realização de outros tipos de serviços, não diretamente ligados com a informática e telecomunicação, mas o que delas fazem uso intenso, como o *call center* por exemplo (GUTIERREZ E ALEXANDRE, 2004).

2.4.1.3 Software Embarcado

Os *softwares* embarcados são aqueles que não são percebidos nem tratados separadamente do produto ao qual estão integrados. Estão presentes nas centrais eletrônicas, terminais celulares, aparelhos de DVDs, autopeças, entre outros. Portanto, pode-se dizer que todo e qualquer tipo de base eletrônica, ou que haja módulos eletrônicos presentes, carrega em si o *software* embarcado. Na maioria das vezes, são as próprias empresas que desenvolvem o *hardware* que projetam o *software* embarcado, sendo poucos os casos em que ele é desenvolvido sob encomenda.

3 PROCEDIMENTOS METODOLÓGICOS

Este capítulo apresenta as técnicas metodológicas adotadas no presente estudo, no que se refere ao tipo de pesquisa, à vertente de pesquisa, ao método e às técnicas de coleta e análise dos dados.

3.1 CLASSIFICAÇÃO DE PESQUISA

Malhotra (2006) aponta que a escolha do tipo de pesquisa é um procedimento essencial para encontrar as informações necessárias para identificação ou solução de problemas. Essencialmente, a pesquisa pode ser classificada como exploratória ou conclusiva. A primeira tem como principal objetivo ajudar a compreender uma situação problema enfrentada pelo pesquisador, sendo um processo flexível e não estruturado. Já a segunda, formal e estruturada, busca auxiliar o tomador de decisões a determinar, avaliar e selecionar o melhor rumo de ação em uma situação específica.

A partir do contexto em que as pessoas estão dispostas a utilizar novas tecnologias para alcançar seus objetivos, segundo Parasuraman e Colby (2002), é importante considerar a percepção dos usuários acerca tecnologia e uso de *softwares* de segurança.

A pesquisa qualitativa é a melhor técnica para obter a coleta de informações desejadas quando o assunto são valores, emoções e motivações (MALHOTRA, 2006), as quais estão interligadas diretamente com alguns conceitos de percepção. A pesquisa qualitativa é baseada pelas perspectivas dos participantes, nas suas práticas diárias e no seu conhecimento cotidiano sobre o tema em estudo (FLICK, 2009). Para Gaskell (2010) o que se busca é explorar as opiniões e as diferentes representações a respeito do assunto em questão.

Conforme essa concepção, este estudo é composto por uma pesquisa exploratória com vertente de natureza qualitativa que, de acordo com Malhotra (2006), esse tipo de investigação aplica-se de modo a definir o problema ou situação com maior precisão. Por isso, é apropriada para os primeiros estágios da investigação, ou seja, no momento em que o pesquisador não tem conhecimento suficiente para formular questões ou hipóteses. (MATTAR, 2008).

A pesquisa exploratória trabalha com amostras menores de respondentes e busca examinar de maneira detalhista as informações recebidas, aprofundando-se com intuito de compreender o contexto do problema de maneira mais completa, trazendo um maior entendimento e *insights* sobre a questão proposta (MALHOTRA, 2006). Aaker, Kumar e Day (2001) reiteram essa posição ao afirmarem que pesquisa exploratória abrange descobertas e esclarecimentos, devido ao fato de os procedimentos deste tipo de pesquisa serem mais flexíveis, não estruturados e qualitativos, o que permite certa liberdade na investigação de diferentes ideias ou proposições acerca do problema estudado.

Diante dessas considerações, entende-se que a pesquisa exploratória se adequa aos propósitos do presente estudo, uma vez que se busca compreender a percepção de jovens porto-alegrenses sobre segurança digital, assim como as motivações e inibições do uso de *softwares* de segurança. No entanto, no contexto desta pesquisa, *insights* são importantes, pois poderão gerar informações para empresas desenvolverem novas formas de comunicação para interagir e ofertar *softwares* de segurança a partir do entendimento da percepção do público jovem.

3.2 MÉTODO DE PESQUISA

Para a realização da pesquisa com foco na busca pela percepção, foram feitas entrevistas em profundidade, como técnica qualitativa de investigação a fim de permitir o levantamento de grande quantidade de informação e compreender o contexto do problema ou situação (MALHOTRA, 2006). A compreensão do contexto dos indivíduos é necessário, uma vez que o mecanismo de percepção rege as relações entre o indivíduo e o meio que o cerca, e todo o conhecimento e informação é adquirido através da percepção (KARSAKLIAN, 2000).

A pesquisa apresentou uma abordagem direta não encoberta, ou seja, de acordo com Malhotra (2006), os entrevistados já conhecem o verdadeiro objetivo do projeto. O roteiro utilizado para realização das entrevistas foi baseado diretamente na busca por informações acerca dos objetivos específicos, os quais contemplam os grandes tópicos sobre hábitos de consumo de internet pelos jovens, aderência e penetração de *softwares* de segurança no universo jovem e fatores influenciadores no processo de compra de tais produtos de tecnologia.

A partir de um levantamento de experiências através de um roteiro semi estruturado, na qual o entrevistado é sondado pelo entrevistador para que se investiguem as percepções, motivações e inibições referentes ao tópico em discussão. Segundo Mattar (2008, p. 10), “o objetivo do levantamento de experiências é o de obter e sintetizar todas as experiências relevantes sobre o tema em estudo, e dessa forma, tornar o pesquisador cada vez mais consciente da problemática em estudo”.

3.3 TÉCNICA DE COLETA DE DADOS

A técnica de coleta de dados empregada foi a entrevista em profundidade, também denominada entrevista focalizada individual. Para este estudo, a abordagem utilizado foi a sondagem, que tem por objetivo, segundo Malhotra (2006, pg. 395), “motivar os entrevistados a ampliar, esclarecer ou explicar suas respostas”. A sondagem também ajuda os entrevistados a manterem o foco no conteúdo específico da entrevista e darem somente as informações que realmente interessam na pesquisa.

A pesquisa baseada na na percepção do indivíduo requer uma técnica de abordagem sutil, em formato de conversa em que os entrevistados relatam suas perspectivas acerca do uso de tecnologia e o entrevistador aborda em profundidade os temas de segurança de dados, motivações e inibições no processo de compra de um produto de tecnologia, pelos quais busca maiores informações a partir do contexto dos informantes.

Mattar (2006) enfatiza que a entrevista em profundidade é uma técnica de comunicação para obtenção de dados primários e elenca as vantagens e desvantagens da sua aplicação. Apesar de ser mais versátil, rápida e de envolver menor custo, a entrevista em profundidade depende da boa vontade dos respondentes e da sinceridade dos mesmos, sendo menos precisa, além do instrumento de pesquisa, no caso o entrevistador, poder influenciar as respostas. Isso significa que, conforme afirmam Malhotra (2006) e Mattar (2008) a preparação e as habilidades do entrevistador são de suma importância para o sucesso da entrevista em profundidade.

3.4 SELEÇÃO DE INFORMANTES

A realização de pesquisas qualitativas não conta com um número exato de entrevistas, porém o recomendável é fazer a coleta até que seja atingido um nível de redundância de informação, utilizando-se então o critério de saturação, ou seja, no momento em que as informações provenientes dos informantes são muito semelhantes e não há diferentes perspectivas, é determinado o fim da etapa das entrevistas. Para este estudo, o total de 10 jovens entre 18 e 30 anos de classe social A e B (conforme o conceito de classes sociais do IBGE) foram entrevistados pessoal e individualmente.

Em todas as entrevistas os informantes autorizaram utilizar seu nome e concordaram em serem gravados com intuito de coleta de informações para observação de *insights* posteriormente. A seleção se deu a partir dos critérios de faixa etária e renda familiar, por critérios do entrevistador de conveniência e adesão para realizar os objetivos desta pesquisa. Abaixo, encontra-se a tabela 4 com os dados dos informantes selecionados.

Tabela 1 – Lista de Entrevistados

	Nome	Idade	Formação	Profissão	Classe Social
1	Pedro H.	23	Direito	Estagiário	A
2	Vanessa	24	Direito	Advogada	B
3	Marcelo	27	Engenharia	Estagiário	B
4	Nathália	26	Administração	Analista	B
5	Daniela	23	Administração	Analista	B
6	Tatiana	25	Arquitetura	Arquiteta	A
7	Pedro O.	23	Engenharia	Estagiário	A
8	Maetê	22	Moda	Empreendedora	A
9	Jéssica	26	Administração	Empreendedora	A
10	Débora	25	Administração	Estagiária	B

Fonte: a autora.

3.5 ANÁLISE DE DADOS

De acordo com Bardin (2004), a análise de conteúdo é uma técnica de investigação que, por meio de uma descrição objetiva, sistemática e quantitativa do conteúdo exposto nas comunicações, tem como fim interpretar as mesmas. Para Flick

(2009), a análise de conteúdo é um procedimento clássico para analisar o material textual.

De acordo com Malhotra (2006), existem três passos que devem ser seguidos para a análise da pesquisa qualitativa. São eles:

1. Redução dos dados: nesta etapa, o pesquisador escolhe quais aspectos dos dados serão enfatizados, minimizados ou ignorados para a pesquisa considerada;

2. Exibição dos dados: o pesquisador desenvolve uma interpretação visual dos dados por meio de ferramentas como diagramas, gráficos ou matrizes. Tal exibição ajuda a esclarecer os padrões e as interrelações dos dados;

3. Conclusão e verificação: o pesquisador considera o significado dos dados analisados e avalia suas implicações para a questão da pesquisa.

Reduzir o conteúdo é o objetivo desta abordagem, e se dá pela categorização e utilização de critérios significantes para os *inputs*, sempre de acordo com os objetivos apresentados. Sendo assim, as entrevistas em profundidade com jovens de 18 a 30 anos de Porto Alegre servirão para levantar informações sobre o uso e frequência da internet, a fim de compreender hábitos de navegação em ferramentas, sites e aplicativos via computador, smartphone ou tablet.

Roesch (2006) apresenta um roteiro simplificado para a análise de conteúdo, sendo a primeira etapa a definição de unidades de análise (palavra, sentença, tema, parágrafo, texto completo). É interessante apresentar os dados de forma criativa, seja em quadros comparativos ou mapas conceituais. Por fim, interpretam-se os dados com base em teorias conhecidas ou ilustram-se novas hipóteses.

4 ANÁLISE DOS RESULTADOS

Neste capítulo serão apresentados os resultados obtidos a partir das 10 entrevistas realizadas com jovens porto-alegrenses, no intuito de investigar as informações que tenham relação com os objetivos deste trabalho. Além de analisar a percepção de segurança digital, este trabalho também busca identificar as finalidades de uso da internet, por quais dispositivos os jovens acessam a internet, quais o sites mais navegados, a frequância que os consumidores acessam a internet, como se dá a penetração e aderência por produtos de segurança digital e quais os principais fatores motivadores e inibidores em um processo de compra de tais produtos.

Durante a coleta das informações, pode-se verificar um certo padrão em algumas respostas com relação à percepção de segurança e de hábitos de uso de internet. Também pode-se afirmar que para alguns assuntos, há grupos de respostas, ou seja, dentro o número total de entrevistados, existem grupos de opiniões semelhantes.

4.1 HÁBITOS DE USO DE INTERNET

Este tópico se baseia em verificar quais os principais objetivos dos jovens ao navegar a internet, os principais dispositivos utilizados, a frequência de uso de internet, quais os sites e aplicativos mais navegados e administração de dados *online*.

4.1.1 Finalidades de uso da internet

Para esta análise, foi perguntado quais eram os objetivos ao usar a internet. As respostas apresentadas foram muito parecidas entre todos os entrevistados, independentemente de gênero, idade ou profissão. Para fins de melhor visualização dos resultados, foi criado uma figura em formato de *wordcloud*, ou seja, ferramenta que permite verificar em fora de imagem as palavras mais citadas em um contexto, em que as palavras mais citadas são maiores, conforme abaixo.

Figura 5 – Finalidades de uso de internet

Fonte: a autora.

A figura revela que o principal objetivo dos jovens entrevistados ao usarem a internet no dia-a-dia é o entretenimento, seguido por comunicação, informação e pesquisa. Além disso, apesar de menos frequentes, foram também citados os objetivos de estudar, trabalhar e se divertir.

> Entretenimento e quando necessário, informação, quando eu quero pesquisar ou algo assim, mas eu poderia dizer que 80% é entretenimento e comunicação né. (Tatiana, 25)
>
> Eu uso pra todos os fins, pro trabalho, pra estudar, pra casualidades, pra me divertir. (Daniela, 23)
>
> Eu uso pra tudo que eu preciso, tudo tipo entretenimento, mídias sociais, pesquisas, todo meu dia-a-dia se eu preciso buscar alguma coisa eu busco na internet. (Marcelo, 27)
>
> Informação e comunicação. (Pedro H., 23)

Apesar de também citarem comunicação e entretenimento, duas entrevistadas acreditam que hoje em dia os jovens não têm um objetivo específico consciente ao usar a internet porque já estão tão acostumados em navegar que já não pensam no porquê do uso. Citam também a dependência pela internet hoje em dia como meio de comunicação principal.

> Eu acho que na verdade a gente nem acaba pensando no objetivo porque a gente depende dessas plataformas pra alguma coisa. Por exemplo, se tu quer olhar tua rede social, a única forma de fazer isso é pela internet. Então eu diria

> comunicação com as pessoas e bastante por entretenimento. E no trabalho, acho que o objetivo no uso da internet é mais pra realizar as tarefas mesmo. (Nathália, 26)
>
> Eu não sei se a gente tem objetivos né? Acho que a internet acabou virando uma coisa tipo, do nada tu viciou. Tu não faz por algum motivo, quando vê tu já tá com o celular aberto e olhando o Instagram ou fazendo alguma coisa mais pra entretenimento. Sei lá, acho que por comunicação com as pessoas também. (Maetê, 22)

A partir das respostas, foi feita uma lista de algumas atividades *online* retiradas das entrevistas e quais os principais dispositivos que os entrevistados usam para realizá-las. Assim, os dados resultantes foram compilados na tabela a seguir.

Tabela 2 – Atividades *online* por dispositivo

Atividades online	Desktop/ Notebook	Smartphone	Tablet
Uso de Mídias Sociais	4	10	0
Compras Online	9	4	0
Uso de sites/aplicativos de banco	0	10	0
Jogos online	3	0	0
Download de softwares e aplicativos	4	10	0
Download de mídia	10	10	0
Compartilhamento de conteúdo	2	10	0
Uso de aplicativos de mensagem instantânea	3	10	0
Ouvir música online	6	10	0
Assistir filmes/séries online	1	0	2
Uso de email	9	8	0
Acesso a conteúdo de eduação/conhecimento	9	10	0
Trabalhar	10	10	0
Ler artigos, notícias, jornais, livros online	8	10	1

Fonte: a autora.

A tabela mostra que das 14 atividades listadas acima, dez são realizadas através do smartphone por todos os jovens e uma é realizada pela maioria. Já a realidade de computadores e notebook é de apenas duas atividades serem realizadas por todos os jovens, sendo trabalhar e fazer *download* de mídia. No geral, tablets não são usados por jovens, a não ser por poucos para assistir séries e filmes *online*.

4.1.2 Acesso por dispositivos

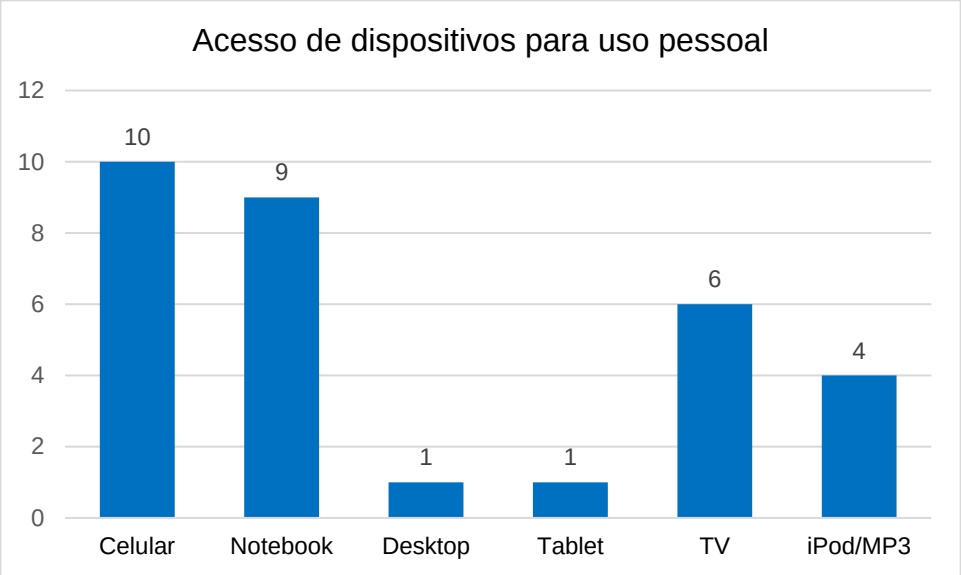
Os jovens entrevistados acessam internet basicamente por meio de três principais dispositivos: celular smartphone, notebook e desktop. Entretanto, foram

também citados em algumas entrevistas o uso por Smart TV, dispositivos de som como iPod e MP3.

Para compreender melhor o uso destes dispositivos, foi feita a segmentação entre uso pessoal, ou seja, atividades de lazer, e uso profissional, sendo as atividades vinculadas ao trabalho. Em ambos segmentos é possível afirmar que o celular smartphone é o dispositivo mais utilizado pelos jovens. Pelo menos 8 dos jovens entrevistados usam celular para trabalhar e todos usam para lazer.

Com relação ao uso para lazer, depois do celular, 9 dos 10 entrevistados citaram uso de notebook e 6 usam TV com conexão na internet. Apenas um entrevistado citou o uso de desktop e pelo menos 4 usam iPod/MP3 para uso pessoal, como é possível visualizar no gráfico abaixo.

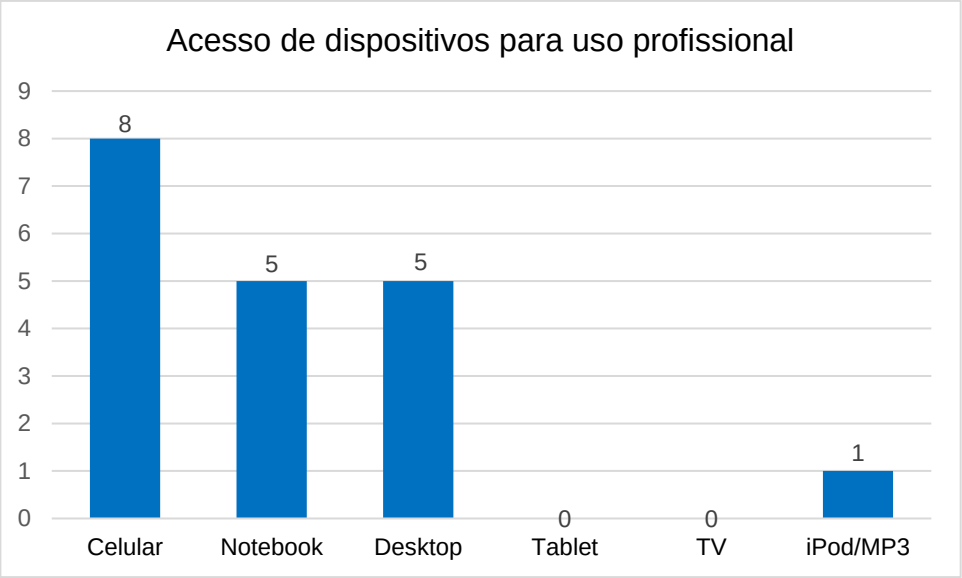
Gráfico 1 – Acesso de dispositivos para uso pessoal



Fonte: a autora.

Com relação ao uso profissional, notebook e desktop são os dispositivos mais utilizados após o celular, na mesma proporção, conforme gráfico abaixo. Apenas uma pessoa citou que utiliza iPod/MP3 conectado na internet para trabalhar e isso se dá pela área de atuação da entrevistada, sendo esta uma professora de uma modalidade de dança.

Gráfico 2 – Acesso de dispositivos para uso profissional



Fonte: a autora.

Independente da área de atuação dos entrevistados, todos afirmam utilizar o celular para trabalho, seja para atendimento ao cliente, quanto para pesquisas relacionadas às tarefas profissionais.

> Uso computador e celular. No dia a dia do trabalho prevalece o uso do computador, o notebook né, e na vida pessoal, com certeza o celular. (Nathália, 26)
>
> Eu utilizo celular, iPod e notebook, mas o mais frequente para o uso pessoal é o celular e pra trabalho notebook. (Daniela, 23)
>
> Eu só uso celular e notebook. Uso a TV, que tem internet, mas é menos. Mas o que eu mais uso é o celular. Pra trabalho, além do celular, uso muito iPod porque preciso das músicas. (Maete, 22)
>
> Uso desktop e smartphone. TV eu não uso muito, mas o principal seria o desktop. Pra trabalhar, sempre que eu pesquiso alguma coisa é pelo celular. (Marcelo, 27)

4.1.3 Frequência de uso

Este tópico tem o objetivo de compreender quantas horas por dia os jovens porto-alegrenses utilizam a internet. A partir das entrevistas, a maioria dos jovens não soube responder sem antes refletir nos seus hábitos diários de interação com a internet, porém todos afirmam que navegam a internet durante quase todo o tempo em que estão acordados.

Alguns informantes acreditam que é complicado responder um número de horas exato de navegação diária porque como estão conectados na internet através das redes de wifi ou 3G do celular, acreditam interagir a maior parte do seu tempo, mesmo quando estão realizando alguma outra atividade. Isso se dá pelo fato de estarem principalmente se comunicando através de aplicativos de mensagem instantânea, como o WhatsApp, o que já virou costume diário.

> Com relação a quantas horas, é complicado dizer porque tudo tá conectado pela internet né? Então eu diria que das 24h que tem num dia, umas 10h, 12h por dia usando a internet. (Pedro O., 23)

> Eu fico conectada o dia todo eu acho. Sei lá, mas pelo menos umas 10h, porque eu meu celular pra tudo, pra rede social, pra trabalhar, então é bastante tempo mesmo. (Jéssica, 26)

> Eu uso internet pelo menos metade do dia, com certeza. Basicamente o tempo que a gente tá acordado, tá mexendo, ou numa rede social ou trabalhando, ou mandando alguma mensagem. (Vanessa, 24)

> Eu uso internet todo dia, mais que 10 anos. Eu fico conectado no celular praticamente o dia todo, no computador, no celular, sempre que tô no estágio, fazendo TCC, tô assistindo um vídeo, então tô sempre conectado, quando tô ligado meu computador tá conectado na internet. (Marcelo, 27)

Quando se trata de trabalho, os entrevistados tinham uma noção melhor de quanto tempo estão conectados na internet, porém quando se trata de conexão para atividades pessoais como acesso a redes sociais, e-mails, entre outros, os jovens acabam não se dando conta de quanto tempo passam navegando. Nesse caso, foi também perguntado como se dava o acesso nos dispositivos e se os entrevistados se conectavam em redes públicas.

Alguns jovens afirmam que se conectam em redes públicas sem nenhum receio da fonte da internet. Alguns até podem saber que há possibilidade de risco com seus arquivos pessoais, mas mesmo assim preferem ter o acesso.

> Eu me conecto, acho que até pode ser que tenha algum problema, mas eu saio me conectando assim, se tem a possibilidade. (Pedro H., 23)

> Eu utilizo e não tenho prevenção nenhuma. Não tenho medo ou algum problema com isso. (Nathália, 26)

> Eu uso na rede pública e eu sempre tento não acessar minhas informações de banco, mas redes sociais e email eu acesso normalmente. (Daniela, 23)

Entretanto, alguns dos jovens preferem não utilizar as redes públicas no dia-a-dia quando não há necessidade ou urgência para tal. Afirmam que costumam não acessar para não se arriscar com relação à segurança dos dados do dispositivo.

> Eu não costumo acessar, num lugar público seria só por uma necessidade, senão eu uso a 3G. Dificilmente eu chego num lugar e ligo na rede, mas nunca me preocupou isso, a internet do lugar. (Vanessa, 24)
>
> Eu não uso, eu tenho medo de arriscar, principalmente aeroporto, que já teve casos de roubo de dados, né? Mas se for uma urgência e eu não tiver rede, tipo quando eu tava viajando fora, daí eu me conectei. (Maete, 22)
>
> Se for num bar, numa rede pública que eu não sei quem é que tá administrando ela, eu não uso, até porque a internet do celular é suficiente pro que eu preciso. (Marcelo, 27)

4.1.4 Acesso de sites e aplicativos

Este aspecto busca identificar os principais sites e aplicativos navegados a fim de entender os hábitos e principais necessidades do usuário com relação aos objetivos citados. Os entrevistados dividiram suas respostas por acesso para uso pessoal e profissional, assim como alguns citaram os principais sites e aplicativos por dispositivo utilizado.

No geral, os principais sites e aplicativos são Instagram, Facebook e Whatsapp. Quando se trata de lazer, todos os entrevistados citaram Facebook e Instagram. Já quando se trata de atividades de trabalho, os principais sites acessados são aqueles vinculados com a área da empresa, sites de pesquisa e de tradução, assim como email.

> Redes sociais, Instagram e Facebook, pesquisa acadêmica, pesquisa de mercado. No celular é praticamente Facebook e Instagram e no desktop é site da Jusbrasil, por causa do trabalho. (Pedro H., 23)
>
> Eu uso internet bastante no celular pra redes sociais e meios de comunicação, uso diretamente no meu trabalho, todos os dias bastante email e sites de pesquisa. (Vanessa, 24)
>
> Principal aplicativo no celular é o Whatsapp, Facebook, Instagram, Outlook (email) e do banco, bastante. E no notebook eu uso principalmente os sites do trabalho, assim como o Outlook (email). (Daniela, 23)
>
> Durante o dia eu uso mais o celular pra Facebook, Instagram, Twitter, Pinterest, mais esse estilo, e computador mais voltado pra pesquisa pra faculdade, coisas que eu preciso ler mais, ou fazer compras (Maete, 22)

As entrevistadas que usam as redes sociais como ferramenta de trabalho afirmaram que acessam principalmente Whatsapp, Facebook e Instagram.

> Como eu trabalho no computador, quando eu tô projetando, eu acabo usando mais a internet no computador, inclusive o Whatsapp, mas eu tô o tempo todo no Instagram e no Whatsapp. (Tatiana, 25)

> Nossa, muito Instagram e Facebook. Uso a internet pra trabalhar também, daí eu uso Instagram e Facebook pro trabalho direto. Ah, eu uso muito o Whatsapp também. (Jéssica, 26)

Apesar de poucos entrevistados terem citado voluntariamente o Whatsapp, o qual é a principal ferramenta de comunicação instantânea através da internet, todos afirmaram que este é o principal aplicativo utilizado no dia-a-dia no momento em que a entrevistadora perguntou sobre tal aplicativo. Pode-se verificar que tal aplicativo é tão utilizado que já virou hábito pelos usuários jovens, os quais acabam por esquecer que esta ferramenta é considerada como “acesso na internet”.

4.1.5 Administração dos dados *online*

A pergunta sobre a administração de dados no ambiente digital tinha o intuito de compreender como os jovens disponibilizam suas informações com relação às respostas anteriores sobre sites e aplicativos mais navegados por eles. Neste tópico forem observados resultados muito parecidos.

4.1.5.1 Redes sociais

Os entrevistados têm hábitos muito parecidos com relação à disponibilidade de informações online quando se trata de perfil pessoal nas redes sociais. Muitos afirmaram que geralmente colocam fotos e mensagens em formato privado, ou seja, somente pessoas com acesso às contas conseguem visualizar. Na maioria dos casos, essas pessoas com acesso são da família, amigos e pessoas conhecidas.

> Disponibilizo informações principalmente pros meus amigos, ou amigos de amigos, mas modo público quase nunca. No Facebook, 90% das coisas são fechadas. (Pedro H., 23)

> Pra aplicativos como Facebook e Instagram tão sempre conectados e as informações são bloqueadas, disponíveis só pra amigos. (Vanessa, 24)

> Questões de fotos e informações pessoais eu tenho somente liberado nas redes sociais pra amigos, eventualmente eu faço postagens abertos ao público mas daí é com o propósito de compartilhar uma informação relevante. (Nathália, 26)

> Nas redes sociais eu bloqueio todas minhas informações pro público e só por meio de convite que a pessoa pode acessar o que eu posto. (Débora, 25)

Apenas uma entrevistada afirmou que possui todas as suas contas de redes sociais disponível em modo público. Outra entrevistada contou que apenas uma rede

social é aberta ao público. No entanto, ambas já bloquearam ou bloqueiam algumas pessoas, ou seja, não permitem que aqueles perfis visualizem suas publicações.

> As minhas redes sociais são todas abertas, não tenho muito problema com isso. Já aconteceu de eu bloquear pessoas, mas pra eu não me incomodar. A partir do momento que eu me sentisse insegura eu ia tornar não público, se isso acontecesse. (Maete, 22)

> Eu acho que eu sou de épocas, eu posto muito Snapchat, mas posto poucas fotos. Inclusive no Snapchat eu tenho mais de 100 pessoas bloqueadas porque eu posto muita coisa pessoal, então eu só deixo ver minhas histórias quem eu quero que veja. (Tatiana, 25)

Entretanto, quando se trata de perfil profissional, alguns entrevistados que têm tal configuração afirmaram que publicam informações em modo público, ou seja, todos que tiverem acesso à internet podem vir a visualizar tais dados.

> Nos perfis que eu uso pra trabalhar é tudo aberto, porque não faria sentido pra mim se fosse só pros meus amigos. Eu quero é divulgar mesmo, daí acho que como não tem nenhuma informação pessoal minha, é tranquilo. (Jéssica, 26)

> Meus perfis são todos bloqueados, só o meu perfil profissional que é aberto ao público porque preciso divulgar meu trabalho né, daí é pra qualquer pessoa mesmo ver. Daí tenho até meus dados de contato pra caso alguém queira falar comigo e tal. (Tatiana, 25)

4.1.5.2 Dados bancários

Com relação a dados financeiros e hábitos de compra online, alguns entrevistados afirmam que verificam o site antes de realizar a compra e disponibilizar os dados de cartões de crédito. Buscam informações que trazem sentimento de segurança e procuram na internet comentários de pessoas que já compraram anteriormente.

> Eu só faço compra em sites que é ou pelo PayPal, PagSeguro, que eu sei que são coisas que são feitas pra dar segurança pros teus dados ou quando o site mesmo disponibiliza uma coisa assim de segurança que tu vê, ou seja, sites que são confiáveis, conhecidos, que são de pessoas que já compraram, que meus amigos já falaram. (Maete, 22)

> Eu busco um site que apresente o mínimo de segurança, ou seja, sites que tem uma estrutura, que tenha público fiel, acho que dar uma olhada no Reclame Aqui. (Pedro H., 23)

> Pra comprar na internet eu sempre dou uma olhada quando é um site que eu não conheço, mas geralmente compro nas mesmas lojas e sei que são confiáveis. (Vanessa, 24)

> Eu compro muito pouco *online*. Dá um medinho, mas assim, eu não compro totalmente num site desconhecido. (Tatiana, 25)

Quando é um site de seu conhecimento, de indicação de pessoas próximas ou que já tiveram experiência positiva de compra e entrega, os entrevistados afirmam

que disponibilizam suas informações bancárias, porém não costumam salvar os dados do cartão no computador.

> Depois que considero confiável, eu ponho meus dados sem problema, só nã constumo deixar salvo pra evitar qualquer problema. (Pedro H., 23)
>
> Eu tenho no celular aplicativo de banco, mas eles nunca são salvos, sempre que eu vou usar eu tenho que inserir os dados. (Vanessa, 24)

Alguns dos entrevistados citaram possuir um tipo de cartão que só faz compra no crédito, porém não existe conta corrente, oferecido pela marca Nubank. Nesse caso, as pessoas podem receber mensagens no celular após cada compra. Este fato, na concepção dos usuários do cartão, é considerado uma forma segura de compra porque há um controle das informações.

4.1.5.3 *Backup* de dados

Os entrevistados comentaram sobre seus hábitos de arquivamento dos seus dados. Alguns preferem fazer a transferência manualmente para um HD externo, outros programam seus dispositivos a fazer *backup* automático recorrente, a fim de não perder nenhuma informação.

A maioria tem o processo automatizado no celular que salva os arquivos na nuvem, porém quando se trata de notebook ou desktop, a maioria ou não realiza, ou faz manual com menos frequência.

> Com relação às fotos, eu guardo tudo num HD externo sempre. (Daniela, 23)
>
> Eu usava muito o HD externo, mas hoje uso cada vez mais o iCloud e o Google Drive. No celular já é backup automático e no notebook eu ainda não tenho *backup*. (Pedro O., 23)
>
> No celular é automático, faz semanal, mas no computador eu nunca faço até porque ali tem poucos arquivos e coisas que eu precisaria depois, sabe? Então acabo não fazendo mesmo. (Maete, 22)
>
> Eu faço sempre no notebook, passo pro Google Drive porque tenho trabalho de faculdade, fotos antigas e tal. E no celular também, mas daí é automatizado, eu nem vejo quando é feito. (Débora, 25)
>
> Faço a cada 2 meses mais ou menos. Faço tudo manual pela conta do Google, na nuvem, e às vezes salvo num HD externo. (Pedro H., 23)

Apenas um entrevistado comentou que o principal motivo por realizar *backup* dos seus dados é por questões de apego pessoal com as fotos e contatos de amigos. Segundo ele, não está preocupado com o roubo ou danos das suas informações pessoais, mas sim o fato de que há insegurança física em Porto Alegre e ele tem receio de ter seu aparelho celular roubado.

Este mesmo informante também traz outro ponto de relevância, pois foi o único entrevistado que citou não se sentir ameaçado por roubo de dados porque sabe que todas as informações que estão no seu backup estão criptografadas, ou seja, ocorre modificação codificada em cada arquivo, de forma a impedir a compreensão pelos que não conhecem os caracteres ou quem não tem permissão de acesso na nuvem.

> Eu faço no celular mais por prevenção nos casos de roubo, perda ou estragar o telefone lá... Se me roubassem o celular e minhas fotos e tal eu ia me sentir lesado, mas não tenho problema porque pelo que vejo no iCloud é tudo criptografado, então sem a senha de acesso ninguém vai entrar nos dados que eu tenho. (Pedro O., 23)

4.1.5.4 Senhas

Este tópico apresentou o mesmo resultado para todos os entrevistados: todos usam uma mesma base de criação para suas senhas. O principal motivo pelo qual fazem isso é por memorização e por praticidade de uso.

> Eu uso as mesmas, como senhas padrões e no máximo faço uma alteração conforme o sistema pede, mas sempre é uma adaptação. (Pedro H., 23)
>
> Eu normalmente uso a mesma senha pra tudo. No máximo uma ou outra quando eu tenho que variar, mas mais por questão de memorizar. (Vanessa, 24)
>
> Eu tenho sempre o mesmo início de senha e com o tempo eu vou trocando o final dela, e ela tem algumas variações. Todas têm a mesma base, porque eu acho mais fácil de escrever, de lembrar, é mais simples. (Daniela, 23)
>
> É tudo igual. Na verdade, não são todas iguais, eu tenho umas 3 ou 4 senhas, mas são todas parecidas. (Tatiana, 25)
>
> Eu uso a mesma senha pra todas as coisas praticamente, inclusive eu misturo a senha do pessoal com o profissional. Eu só mudo as terminações delas, mas a raiz costuma ser a mesma. (Nathália, 26)
>
> Eu tenho um padrãozinho que eu tenho uma parte das minhas senhas que, em todos os lugares que eu tenho senhas, são iguais. (Pedro O., 23)

Afirmam que costumam deixar salvas nos seus dispositivos quando se trata de contas de redes sociais, mas em algumas situações específicas alguns anotam em um papel. Eles apontam que, nos casos de esquecimento, acabam sempre tentando acessar suas contas com essas senhas, pois sabem que uma delas vai ser a correta.

> Eu costumo salvar no próprio computador pra escrever automaticamente. (Pedro H., 23)
>
> Não anoto, mas se é uma senha nova eu costumo anotar num papel até memorizar, ai depois eu descarto o papel. (Vanessa, 24)

> Não armazeno, não anoto, eu só tenho elas salvas tipo a do Facebook e tal. As únicas senhas que eu tenho anotado são de companhia aérea, porque são diferentes das outras. (Tatiana, 25)
>
> Eu não tenho escrito em nenhum lugar, então muito frequentemente eu esqueço minhas senhas. Só no trabalho eu tenho um arquivo onde eu tenho todas as minhas senhas salvas. (Nathália, 26)

Apenas dois entrevistados afirmaram que criam suas senhas de forma diferente. Aponta que o principal motivo disso é que acreditam ter contas mais complexas e menos complexas, portanto criam senhas consideradas mais difíceis de serem descobertas ou mais fáceis de lembrar.

> No caso da criação de novas senhas, geralmente quando é uma coisa mais importante por exemplo email eu faço aleatório, eu mesmo penso, misturo letras maiúsculas e minúsculas, números, caracteres especiais. São sempre diferentes (as senhas). O que eu acho mais importante eu uso diferente. E aí nesses casos eu anoto no papel. (Marcelo, 27)
>
> Eu troco dependendo do nível de complexidade, por exemplo, pro meu email pessoal ela é de nível médio, pras redes sociais é um nível baixo, pra um aplicativo bobo, de calendário é um nível baixo, mas pro banco ele é o máximo, o mais complicado possível. (Daniela, 23)

Entretanto, nenhum dos jovens comentou em seus relatos sobre os riscos de usar as mesmas senhas para todas suas contas, então pode-se dizer que os entrevistados, no geral, não percebem a importância de terem senhas senhas diferentes para cada conta.

4.2 PENETRAÇÃO E ADERÊNCIA DE *SOFTWARE* DE SEGURANÇA NO SEGMENTO JOVEM

Esta etapa da pesquisa buscou verificar qual o sentimento e a percepção de segurança dos entrevistados aos navegarem na internet, assim como verificar a adesão do produto de proteção digital a partir da compreensão das experiências dos entrevistados com relação a ataques virtuais. Além do mais, buscou-se compreender se os entrevistados já compraram ou utilizaram algum *software* de segurança em seus dispositivos e como foi a experiência de uso, compreendendo a penetração deste produto no segmento jovem.

4.2.1 Navegação e segurança

Para esta análise, foi perguntado como os entrevistados se sentiam ao navegar na internet em termos de segurança. A maioria dos jovens afirmou se sentir

seguros ao navegar, pois acreditam ter hábitos básicos preventivos com relação a ameaças digitais.

> Me sinto seguro. Não é uma coisa que navegando eu tenha medo de clicar em algum link assim, eu acho que os que podem apresentar algum tipo de insegurança assim são bem escancarados, tipo é aqueles banners que tu já vê que ou que é uma proposta muito distante da realidade. (Pedro H., 23)

> Eu me sinto tranquilo ao navegar porque eu uso a internet há muito tempo e então eu sei onde tem um potencial vírus, fazer download de arquivos na internet, abrir e-mails e tal. (Marcelo, 27)

> Olha, eu me sinto segura porque eu não costumo entrar em sites muito suspeitos. Eu uso sites que são aparentemente seguros, de grandes empresas e tudo mais. (Nathália, 26)

> Eu me sinto bem segura, são poucos os sites que eu entro e tenho alguma notificação do antivírus ou algum problema e ainda assim tô acostumada a fazer compras, acessar vários sites, coloco meu email e meu contato em vários sites, não tenho nenhuma restrição assim. (Daniela, 23)

> Ah eu me sinto... ok assim, eu não tenho medo de né, sei lá acontecer qualquer coisa, tanto no lado financeiro quanto ter intimidade exposta ou coisa assim. Não tenho medo. (Tatiana, 25)

Duas entrevistadas, entretanto, afirmam que se sentem desconfortáveis ao navegar na internet por conta das atividades de remarketing praticadas por algumas empresas através da compra de dados de navegação de usuários (*cookies)*. Uma afirma se sentir com medo e alega o sentimento de estar sendo vigiada. A outra alega se sentir nervosa quando pensa sobre o assunto.

> Eu percebo o quanto as coisas são interligadas. No sentido de segurança, eu sinto um pouco de medo, né? No sentido de que tem alguém monitorando tudo que eu faço. Parece que as coisas são muito sensíveis, que a qualquer momento alguém pode pegar meus dados, minhas informações, ter acesso ou controle. (Vanessa, 24)

> Coisas que me deixam muito nervosas são entrar num site de compra, daí fechar esse site e abrir outro site e aparecem coisas daquele primeiro site. Então claramente tão te perseguindo. É, sei lá, não é nada seguro. E isso é o que me deixa nervosa, mas daí é só não pensar muito nisso. (Maete, 22)

Uma entrevistada, inclusive, acrescenta sua opinião sobre algumas empresas estarem no comando de dados digitais de todos os usuários e como passam a imagem de segurança para os navegantes *online*.

> Eu acho que fazem a gente acreditar que existe segurança, mas que na verdade a segurança ela é colocada nas “mãos” de algumas pessoas, algumas empresas e elas que decidem se tu tá seguro ou não. Tipo, elas decidem se elas vão vender teus dados ou não. Porque elas podem vender pra outras empresas, enfim e isso ir passando as tuas coisas e vai tá na “mão” de todo mundo. (Maete, 22)

Apenas um entrevistado comentou que não se sente seguro porque já havia tido problemas com vírus no passado por conta de navegação e *downloads* de arquivos da internet de fontes desconhecidas ou duvidosas. Ele conta que joga *online*, porém não se sente ameaçado, pois sua real identidade não é revelada.

> Eu já tive problemas com vírus uma vez, então não me sinto tão seguro. No caso de jogos *online*, é bem tranquilo. Jogando eu não tenho medo, ainda mais que não usa nenhum nome pessoal, nenhuma informação pessoal, é tudo apelido. (Pedro O., 23)

4.2.2 Ataques virtuais

Os entrevistados contaram suas experiências de ataques virtuais e como acreditam ter contraído as ameaças. Apenas um entrevistado alega nunca ter sido afetado por vírus.

> Não, acho que o máximo que aconteceu foi o computador trancar assim, dificultar alguma coisa, mas nada que afetou diretamente. Acho que nunca fui afetado no meu computador. (Pedro H.,23)

Já os demais contam que suas experiências com vírus foram negativas e a maioria recorreu a um especialista em tecnologia para resolver o problema. Muitos dos jovens afirmam que não têm muito conhecimento sobre o assunto, por isso acabam confiando e contando com suporte técnico.

> Meu notebook teve vírus e ele ficava abrindo sites de internet o tempo todo então eu não conseguia usar ele de forma efetiva. Com certeza foi uma experiencia negativa, mas passei o computador pra um técnico e ele teve que limpar o vírus. (Vanessa, 24)

> Só na época que tinha computador de casa em uso coletivo, aconteceu de entrar uns vírus meio loucos perdemos tudo, tive que chamar um técnico. (Nathália, 26)

> Eu acho que sim, meu computador e meu notebook já pegaram uma vez. Foi há muito tempo, eu não lembro bem, mas eu acho que eu mandei pro meu técnico. (Tatiana, 25)

> Já fui afetado, mas minha experiência foi horrível. Foi de chamar um técnico e ter que ver o que aconteceu. Ele teve que apagar o que tinha sido afetado e salvar o que não tinha sido. Perdi quase tudo. Foi horrível. (Pedro O., 23)

Apenas um entrevistado afirmou ter resolvido o problema.

> Já fui afetado, então eu tive que salvar, fazer um *backup* dos meus documentos e formatar o computador. A última vez já foi há vários anos, mas frequentemente eu faço um scan no computador pra detectar *malware*, cavalo de troia, esse tipo de coisa. (Marcelo, 27)

Alguns entrevistados afirmam que no passado seus hábitos na internet eram diferentes: faziam *downloads* de arquivos de fontes e sites duvidosos, clicavam em links e acessavam sites desconhecidos. Hoje em dia, entretando, alegam ter maior cuidado ao navegar na internet e raramente fazem *downloads*.

> Ele surgiu quando a gente foi baixar uma legenda pra um filme e ai esse site baixou o vírus. Hoje em dia eu não costumo mais baixar fotos, vídeos ou músicas, só navego na internet mesmo. (Vanessa, 24)

> Teve uma vez que eu baixei um documento pra faculdade e eu achei que era seguro, mas tava com vírus e praticamente não tinha como tirar do computador mais. (Marcelo, 27)

> Foi naquela época em que eu baixava coisa na internet, tipo naqueles sites de Baixaki e tal, foi por aí assim que acho que pegou o vírus. Hoje eu só baixo coisa da internet que eu tenho certeza que é confiável assim, porque é pro trabalho, daí preciso. (Tatiana, 25)

> Ah, era na época do MSN e Orkut que a gente baixava um monte de coisa na internet. Eu nunca cuidava, mas daí um dia meu computador estragou e depois que botei o antivírus. (Débora, 25)

Uma entrevistada acredita que, apesar de ter sido afetada por um vírus, nunca teve sérios problemas em função de usar *software* de segurança. Ela afirma que, por ter sido avisada das ameaças pelo sistema, o vírus nunca chegou a danificar seus arquivos.

> Na época eu usava Torrent pra baixar filmes e séries e nessa época tinha mais o risco de ser afetado por vírus, só que dai o antivírus “pegava” e eu não abria o arquivo, então nunca chegou realmente a ter alguma coisa por causa disso, mas já fui afetada de certa forma por um vírus sim. (Daniela, 23)

4.2.3 Experiências com *softwares* de segurança

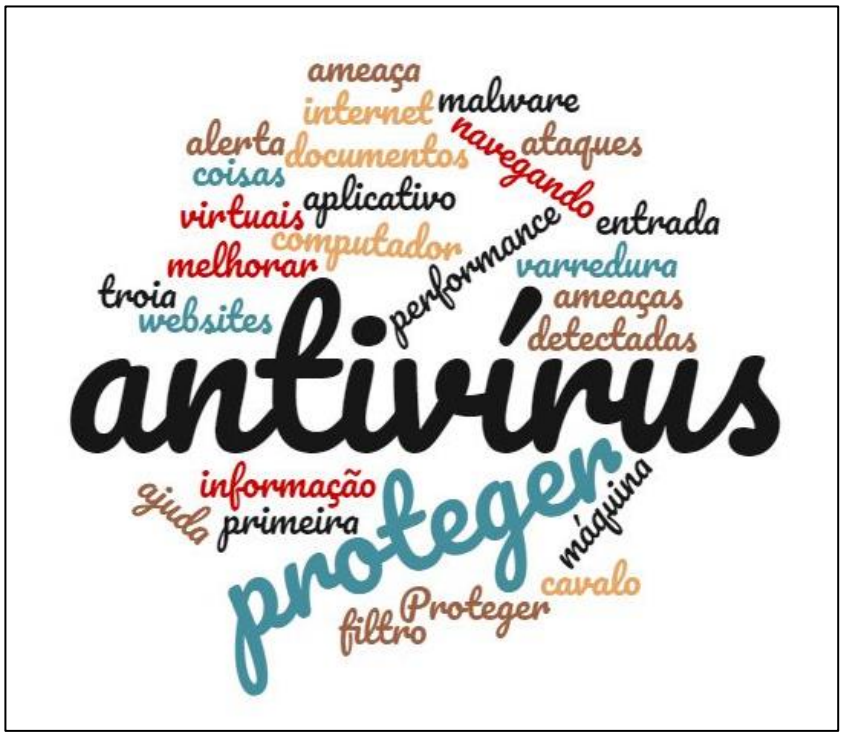
Os entrevistados contaram suas experiências de aquisição e uso de produtos de proteção digital em seus dispositivos, além de trazer seus hábitos com relação à busca de informações sobre este tipo de produto. Nesta etapa da pesquisa, os informantes revelaram o que entendem por *software* de segurança e antivírus, conceitos que remetem a um mesmo produto, porém posicionado de forma diferente pelas empresas de tecnologia.

Software de segurança, segundo algumas empresas do ramo, na realidade são além de antivírus. No mesmo *software* em que há proteção contra diferentes ataques de vírus, há também proteção durante a navegação na internet, filtros de páginas configuradas pelo usuário, proteção de conexão em redes consideradas

como ameaças, varredura de arquivos e proteção e armazenamento de senhas. Para as versões de celular e tablet há também proteção para aplicativos, rastreio do aparelho em caso de roubo e bloqueio de chamadas.

Entretanto, apesar de haver uma série de outros recursos em um mesmo *software*, quase todas os entrevistados associaram "*software* de segurança" com antivírus. Para fins de melhor visualização das respostas, segue imagem em formato de *wordcloud*, em que as palavras mais citadas são maiores, conforme abaixo.

Figura 6 – Percepção de "*Software* de segurança"



Fonte: a autora.

A expressão "*software* de segurança" não é muito utilizada pelos jovens, nem na mídia. As empresas deste ramo vêm tentando se posicionar de forma diferenciada, não utilizando mais "antivírus" como especificação do seu produto. Entretanto, apesar da primeira expressão já estar sendo adaptada nos sites de compra, o reposicionamento ainda não está na lembrança do consumidor.

Além de "antivírus", os entrevistados também falaram muito em "proteger", ou seja, o *software* de segurança remete diretamente a uma ideia de proteção contra "ameaças", "ataques", "malware" "detectados" e "cavalo de troia", segundo a imagem.

Além disso, a figura revela que os entrevistados associam a expressão com “performance”, “filtro”, “ajuda”, varredura”, “alerta”, “computador”, “aplicativo” e “melhorar”, então acreditam que o produto de um modo geral serve para dar segurança para os usuários de computadores e celulares (associado a aplicativos).

Quando foi perguntado o entendimento por “antivírus”, os entrevistados associaram diretamente a expressão com “computador”, conforme imagem *wordcloud* abaixo, gerada a partir das respostas. Além disso, foram associadas também as palavras “proteger”, “vírus”, “ameaças”.

Muitos citaram que “antivírus” seria uma defesa do computador, um sistema que protege o computador de entrada de vírus, proteção de informações com relação ao acesso externo, proteção ativa da internet, prevenção, detecção e sinalização de ameaças.

Figura 7 – Percepção de “Antivírus”

Fonte: a autora.

A expressão “antivírus” têm sido trabalhada desde que produtos que combatem vírus digitais foram criados. Na época, este produto apenas sinalizava e bloqueava as possíveis ameaças *online*.

Mesmo que o produto venha sendo melhorado e abrangente para demais características, continua sendo chamado informalmente de “antivírus”. As empresas deste ramo, entretanto, estão começando a se posicionar de forma diferente para que o produto seja considerado mais que apenas um “anti-vírus”.

Apesar de alguns informantes terem citado a questão de proteção de aplicativos, associados ao celular, e uma entrevistada já ter usado um software em seu dispositivo móvel, a grande maioria trouxe a palavra “computador” em suas respostas. A partir disso, pode-se dizer que antivírus está associado a computador, principalmente.

Historicamente, faz muito sentido, até porque esta geração entrevistada para esta pesquisa teve bastante experiências com computadores, especialmente desktop. Com o avanço da tecnologia, aos poucos o notebook ganhou espaço e agora os smartphones praticamente dominam o mercado de eletrônicos.

Então, a partir de tais dados, é possível perceber que tal associação de “antivírus” com “computador” faça sentido, pois todos os informantes já experienciaram o software apenas neste tipo de máquina por enquanto.

4.2.3.1 Busca por informações

Os entrevistados falaram onde buscam informações sobre *softwares* de segurança e por qual motivo o fazem. Alguns mencionam o momento em que procuraram ou procurariam por tais informações.

Prevaleceu a resposta de que os entrevistados ainda não haviam buscado por informações deste tipo de produto, pois não precisaram desse conteúdo no passado ou não tiveram interesse pelo assunto. Porém alguns confessam que buscariam saber sobre programas de proteção digital para entender melhor do assunto. Afirmam que fariam no momento em que precisassem comprar este produto, seja porque o anterior está expirando, seja para usar melhores opções.

> Olha, não busquei, mas acho que eu buscaria se eu quisesse entender mais sobre, buscando referencias na internet, mas nunca foi um tema que me interessou. (Nathália, 26)

> Quando a licença expirar, eu acho que eu pesquisaria um com o melhor custo benefício pra mim, mas acho difícil deixar sem. (Vanessa, 24)

> Eu pesquisaria muito provavelmente pra eu melhorar a performance do computador ou do celular, em primeiro lugar, e o segundo motivo talvez seria pra ver qual a segurança de usar aplicativos sem antivírus no celular. Por último talvez pra fazer backup de dados automático na nuvem pra não depender de HD externo. (Daniela, 23)

> Seria uma pesquisa pra uma futura compra, dependendo dos benefícios dos outros antivírus. (Débora, 25)

A maioria disse que o Google, atualmente o maior site de buscas, é a principal ferramenta usada para pesquisar. Alguns preferem navegar em sites de tecnologia ou em sites de comparação de produtos para facilitar na decisão de compra.

> Eu acho que em pesquisa do Google, naquele Technomundo, nesses sites assim. Eu busquei na internet e no caso já mostrava um comparativo de entre antivírus e acho que me apresentou uma resposta melhor.

> Geralmente eu procuro no Google referência de programas, quando eu procuro programa de scan e de antimalware, o que mais tá se usando, o que é mais efetivo. Leio comparativos, reviews e aí decido qual que eu vou usar. (Marcelo, 27)

> Eu pesquisaria na internet, no Google. Eu nunca pesquisei, mas sei mais por indicação de amigos sobre antivírus. (Vanessa, 24)

> Eu buscaria informações na internet, mas nunca busquei. Eu jogaria a informação no Google, muito provavelmente. (Daniela, 23)

Alguns entrevistados que alegam não terem buscado tais informações anteriormente justificam o fato porque optam por opiniões e sugestões de técnicos da área, pessoas em quem confiam. Entretanto, eles dizem que se fosse o caso, pesquisariam na internet, também no Google, assim como os demais.

> Eu nunca busquei por esse tipo de coisa. Eu confio no meu técnico, só que agora eu gostaria de pesquisar, porque expirou mesmo. Mas não sei direito onde pesquisar, talvez no Google. (Tatiana, 25)

> Informações foi muito do que o técnico me passou, ele me recomendou uma licença de um software e daí a família inteira comprou. Não pesquisei, eu confiei na informaçã que o técnico me passou mesmo. (Pedro O., 23)

> Acho que não buscaria, acho que, como eu não entendo muito, eu sempre ia acabar perguntando pra alguém que saiba, que seja algum amigo que entenda de TI, enfim. Mas se eu buscaria, seria no Google ou no Youtube, essas coisas. Mas eu sempre vou preferir apelar por uma pessoa ou técnico. (Maete, 22)

4.2.3.2 Momento de compra

Todos afirmam já terem usado algum tipo deste produto, porém nem todos foram os responsáveis pela escolha ou compra do mesmo. Alguns ganharam ou

adquiriram *online* a versão gratuita disponibilizada por algumas empresas do ramo ou o produto já veio embarcado na máquina.

Todos usaram o *software* de segurança em computadores e apenas uma pessoas já usou no celular, mas ninguém usou ou usa ou em outros dispositivos. O motivo pelo qual os jovens não usam em demais dispositivos não foi aprofundado nessa pesquisa.

> Já usei pro computador. A gente tava pagando na época e eu não achei ele muito diferente dos que a internet oferece de graça. Na época, eu fui o decisor da compra. (Pedro H., 23)
>
> Eu nunca comprei, mas por exemplo quando eu comprei um notebook veio um antivírus instalado. Eu percebo de forma efetiva porque eu recebo as mensagens “ah uma ameaça foi detectada”, aí eu percebo o quanto a gente tá suscetível a um vírus o tempo todo. (Vanessa, 24)
>
> Eu já usei vários *softwares*. Eu sempre usei os gratuitos e quando era pago eu ganhei, mas nunca fiquei satisfeito com a qualidade dos serviços dos antivírus gratuitos, achei que tudo que era oferecido era melhor ficar sem ou usar só um *software* de *scan*. (Marcelo, 27)
>
> Só no computador, um *software* de antivírus, comprei junto com a máquina e depois no momento que ele expirou eu comecei a utilizar um que era gratuito. (Nathália, 26)
>
> Já usei e uso atualmente também, mas somente no notebook. Agora é uma licença gratuita, mas já usei o antivírus pago. Com relação a performance da máquina, eu não consegui observar uma diferença, só quando usei no meu celular, ele ajudou a otimizar espaço, limpar os aplicativos, mas quando eu usei ele no computador eu não vi a diferença. (Daniela, 23)
>
> Não comprei, foi o técnico quem comprou. A experiência foi boa. É um *software* que não precisa de muita interação minha. Até agora não tive nenhum problema. (Pedro O., 23)
>
> Quando eu comprei o computador veio um junto, mas acho que a gente comprou um antivírus junto pra uns dois anos, coisa assim e daí ficou, mas agora não tem mais. (Jéssica, 26)

Os jovens entrevistados falaram muito acerca de licenças pagas e gratuitas, principalmente quando haviam uma paga e no momento que expira acabam migrando para um *software* gratuito. Porém, nenhum jovem afirma saber a diferença entre os modelos oferecidos e nenhum questiona o desempenho do produto gratuito ou questiona a confiança de que este formato irá desempenhar seu papel de forma extraordinária.

4.2.3.3 Experiências de uso

Nesta parte da entrevista, os informantes contam o que acharam do *software* de segurança que usaram e qual o tipo usado. A maioria já usou o software gratuito, poucos usaram o produto pago e quase ninguém sabe a real diferença entre os dois tipos.

Revelam também aspectos positivos de suas experiências, como por exemplo instalação tranquila, máquina protegida de vírus desde o início do uso e baixa interação com *software.* Já os aspectos negativos citados foram demora e lentidão de varredura, mensagens *pop ups* exigindo interação com o programa, sistemas muito complexos.

> Achei que foi tranquilo em termos de instalação mas em termos de resultado não me satisfez muito. Eu achava que o que eu tava usando naquela época era muito pesado e quando ele fazia a varredura ele demorava muito então eu tava procurando uma opção mais rápida. (Pedro H., 23)
>
> Como eu não baixo muita informação e não tenho grandes atividades, não preciso de muita proteção. Então não precisa ser um sistema muito complexo, poderia ser um mais básico. (Vanessa, 24)
>
> O que eu sinto é que o pago não me incomodava tanto no sentido de trazer tantas notificações quanto o gratuito me trás. O gratuito é muito “ativo” assim, queria algo mais assertivo e menos frequente. (Nathália, 26)
>
> O que eu achei do pago é que ele mandava muita notificação de “ah lembrar de fazer isso, limpar tal coisa” e eu achei ruim a experiência porque justamente tinha muitas notificações. Eu queria um antivírus que só avisasse caso alguma coisa desse errada, então por isso que eu não gostei do pago. O gratuito oferece menos opções de cuidado, mas ele também envia menos notificações, ele só faz o que eu quero que é só avisar sobre algum vírus. (Daniela, 23)
>
> Ele atende minhas necessidades, até hoje não tive mais vírus. Minha principal necessidade num antivírus é que eu não precise ficar mexendo e que eu não tenha problema com vírus de novo. Estou satisfeito nesses dois quesitos. E com relação a performance da máquina, eu não associei ao *software* de antivírus. (Pedro O., 23)
>
> Quando eu tive, eu acho que ele fazia tudo sozinho porque ele não abria uma janela, sabe, ele só fazia e depois avisava “ah, sua segurança foi feita” ou algo do gênero. (Débora, 25)

4.2.3.4 Ambiente de trabalho

Nesta etapa, foi abordada a pergunta que se refere a percepção de segurança digital no ambiente de trabalho em comparação com o ambiente pessoal. Nesse sentido, alguns entrevistados que não trabalham em casa afirmaram que se conectam na rede de internet de seus empregos, pois acreditam ser segura.

> Eu utilizo a rede pública de onde eu trabalho. Geralmente eu só uso de casa e no trabalho. Até porque como ali é um lugar mais controlado, fico mais seguro de usar a rede wifi. (Marcelo, 27)

> Eu uso tranquilamente a rede da empresa, acho que não tem problema porque aqui ninguém vai querer roubar meus dados - eu espero. (Débora, 25)

Entretanto, algumas pessoas confessam que se sentem ameaçadas ou mais ameaçadas no ambiente de trabalho. Isso se dá porque acreditam que as empresas e ambientes profissionais, por terem arquivos e dados importantes armazenados, correm mais risco de serem *hackeados* ou de serem atacados por diversos vírus.

> Então, eu sinto que no trabalho a gente tem muito mais chance de ter uma procura de um *hacker* externo, acho que tem muito mais informação, muito mais coisas importantes que talvez atraia uma pessoa má intencionada. (Pedro H., 23)

> Com certeza no local de trabalho a ameaça é maior, pode ser que tem alguma coisa lá mais importante e acho que lá tem mais segurança porque lá é público, tem mais visibilidade que uma pessoa normal. (Marcelo, 27)

Alguns entrevistados citaram que informações de clientes ou financeiras podem ser motivos pelos quais as empresas estão mais expostas. Acreditam que *hackers*, pessoas de má índole que têm intuito de roubar dados digitais, acabam procurando corromper o sistema de segurança de grandes corporações a fim de ganhos financeiros.

Em janeiro deste ano, foi informada pela Folha de São Paulo a notícia de *hackers* que roubaram dados de 29 mil clientes da XP Corretora de Valores. Ou seja, é verídico que as empresas acabam sendo também alvo de roubos de dados em troca de *bitcoins*, a moeda utilizada *online.*

Então, os informantes acreditam que as empresas, justamente por serem alvos de *hackers*, têm sistemas fortes de segurança, a fim de impedir que algo ou alguém possa corromper. Em alguns depoimentos, foi possível identificar que tal sistema de segurança foi definido além de apenas *softwares* e programas de proteção digital, mas também conta com uma equipe de tecnologia da informação para dar suporte ao negócio e garantir maior proteção.

> A gente tem uma equipe de técnicos e eles cuidam da rede, então acredito que tenha um sistema bem forte de segurança. Sinto que as informações do trabalho estão mais protegidas porque tem uma equipe por trás cuidando desse sistema. (Vanessa, 24)

> No escritório ou numa empresa tu precisa ter essa equipe porque eles precisam estar em constante vigilância. Só o *software* não faz esse papel sozinho. Eu acho que por mais que a pessoa saiba usar o programa, o programa por si só não resolve todos os problemas. (Pedro H., 23)

> A estrutura deles é bem maior, eles têm *firewall* que filtra informações que tão chegando e saindo, todos os computadores lá têm antivírus, então acho que lá é mais controlado e mais protegido. (Marcelo, 27)

> Me sinto mais segura no trabalho porque a própria empresa coloca vários filtros quando eles consideram algum site suspeito ou que não vá agregar. Então só de ter um trabalho nesse sentido, eu me sinto mais segura. Tenho a sensação dos meus dados estarem mais protegidos dentro da empresa. (Nathália, 26)

> Dentro da empresa eu acho que é mais seguro, ainda mais por ser uma corporação desse tamanho, deve empregar mais *softwares* e operaçõs de segurança pra fazer com que nenhum vírus afete o trabalho. (Débora, 25)

Já aqueles que trabalham de casa contaram que não sentem diferença entre acessos pessoais e profissionais, com relação a perfis de contas em redes sociais e também a partir das experiências anteriores em ambientes corporativos. Acreditam que estão vulneráveis a ameças digitais da mesma forma.

> Os escritórios que eu trabalhei eram meio que nem em casa assim, tem até o mesmo técnico em um deles que montou os computadores, mas assim, não era periódico. (Tatiana, 25)

> Eu não sinto a diferença de acessar a internet de empresa ou em casa, acho que pode acontecer alguma coisa com a gente em qualquer lugar sabe? E meus perfis profissionais nunca aconteceram nada, acho que ninguém pensaria em atacar com vírus ou roubar alguma coisa. (Jéssica, 26)

> Não vejo nenhuma diferença porque eu trabalho de casa sempre nos útlimos tempos, mas não me sinto mais ameaçada nos meus perfis profissionais nas redes sociais, acho que é meu trabalho, então as pessoas respeitam mais. (Maete, 22)

4.3 FATORES MOTIVADORES E INIBIDORES NO PROCESSO DE COMPRA DE *SOFTWARE* DE SEGURANÇA

Esta etapa da pesquisa buscou verificar quais os principais aspectos motivacionais e inibidores que influenciariam os entrevistados em um possível processo de compra, a partir de suas experiências anteriores com o produto. Também responderam se já indicaram ou indicariam um *software* de segurança e o motivo pelo qual o fizeram.

A partir das entrevistas foi possível perceber que os informantes elencaram os principais aspectos chaves que, dependendo de como se manifestam, se tornam motivadores ou inibidores em um processo de compra. A relação da experiência do

software com o desempenho de suas funções são importantes e influenciam diretamente na decisão do usuário tanto para comprar quanto para indicar o produto.

Os informantes alegaram que o principal fator que influencia sua opinião no processo de compra e indicação é a garantia de proteção. Se o *software* cumpre seu papel de proteger a máquina, bloquear as ameaças provenientes da navegação na internet e limpar arquivos de risco, este se torna um fator motivacional. No caso do *software* não funcionar, ou seja, a máquina ser afetada por alguma ameaça durante seu período ativo, os entrevistados elencaram isto como principal fator inibidor.

Outros fatores considerados importantes foram interação com o usuário, performance da máquina e mensagens de notificação do *software*. Em casos de o programa não exigir interação do usuário para que realize suas funções de proteção, o programa não alterar a performance da máquina enquanto estiver realizando alguma varredura ou outra função e por último, o programa não enviar mensagens *pop ups* ao realizar qualquer função, os informantes consideram fatores motivacionais.

No caso do *software* enviar muitas notificações, afetar negativamente na velocidade e perfomance da máquina enquanto usada e acionar o usuário com comandos, os entrevistados consideram estes aspectos como fator inibidor na compra do produto. Abaixo foram elencados os aspectos citados em forma de tabelas, a fim de melhor visualização das respostas.

Tabela 5 – Motivadores do consumo de Softwares de Segurança

Motivadores do consumo de Softwares de Segurança	
Aspecto	**O que significa**
Proteção	Desde a instalação do software, os usuários não tiveram mais problemas com vírus e ameaças digitais
Interação	O programa não exigir ação por parte dos usuários para realizar as funções na máquina
Performance	O programa não interferir no desempenho da máquina e na velocidade de navegação na internet
Mensagens	O programa não enviar sinalizações a cada função realizada, sobrecarregando o usuário de informações os quais não tem interesse

Fonte: a autora.

Tabela 6 – Inibidores do consumo de Softwares de Segurança

Inibidores do consumo de Softwares de Segurança	
Aspecto	**O que significa**
Proteção	Desde a instalação do software, os usuários tiveram problemas com vírus e ameaças digitais
Interação	O programa exigir ação por parte dos usuários para realizar as funções na máquina
Performance	O programa interferir negativamente no desempenho da máquina e na velocidade de navegação na internet
Mensagens	O programa enviar sinalizações a cada função realizada, sobrecarregando o usuário de informações os quais não tem interesse

Fonte: a autora.

Considerando tais aspectos, alguns entrevistados relatam que, a partir de suas experiências positivas anteriores, eles já indicaram ou indicariam o *software.*

> Eu já recomendei e indicaria por funcionalidade de uso, um antivírus que não vai ficar incomodando, que não vai pedir pra fazer alguma coisa, que vai ser simples de usar e fácil de instalar. Em segundo lugar, um antivírus que seja leve. E leve seria o que não impacta a performance do computador durante o uso. (Marcelo, 27)

> Já indiquei pra amigos, mas só indiquei porque a pessoa perguntou e eu falei o que eu usava porque a experiência foi legal. Se eu tivesse problemas, não indicaria. (Daniela, 23)

> Eu indicaria porque eu nunca tive problemas com esse que eu tenho, me parece ser bom. Como eu uso muito programa pesado pra trabalhar e ele não interfere em nada, pra mim é ótimo. (Tatiana, 25)

> Indicaria pelos quesitos que me deixam satisfeitos, ou seja, de não mexer nele frequentemente e até hoje, eu to com um bom tempo com ele, não ter tido vírus. Pra mim é ótimo porque é muito prático. (Jéssica, 26)

Um entrevistado, porém, disse que apesar de já ter indicado antivírus, ele indicaria um *software* específico de varredura porque ele acredita que as pessoas que estão perguntando provavelmente o fazem porque já sofreram com ataque de vírus. Nesse caso, ele acha melhor o programa de varredura que além de funcionar o tempo todo, detecta e combate todas as ameaças.

> Como eu tenho mais experiência em *software* de scan, não antivírus, eu recomendo esse tipo de *software* até porque quando uma pessoa pergunta sobre *software* de antivírus eles perguntam depois de pegar um vírus e não antes. Então sempre o que vai ajudar vai ser um *scan* de *malware*, esse tipo de coisa. (Pedro O., 23)

Outros entrevistados, apesar de terem tido experiências positivas com *softwares* de segurança, não indicariam por motivos de ninguém ter perguntado ou por não dominarem o assunto, então não se sentiram à vontade de fazê-lo.

> Eu nunca indiquei porque nunca ninguém me pediu indicação e porque eu não entendo muito disso pra indicar, acho que não tenho tanta propriedade pra falar sobre isso. (Vanessa, 24)

> Nunca indiquei e não indicaria porque não tenho conhecimento na área pra poder dizer o que é melhor. Preferia dizer pra pessoa pesquisar na internet ou com alguém que entenda do assunto. (Maete, 22)

> Nunca indiquei por falta de oportunidade, mas se me perguntassem eu daria os dois que já usei como referência. (Nathália, 26)

Alguns entrevistados comentaram que não indicariam o *software* em caso de experiências negativas com o produto.

> Eu acho que se ele for muito pesado seria um ponto definitivo, importante nessa indicação. Pesado é a varredura demorada, que enquanto o *software* tá fazendo uma busca de algum vírus eu não consigo usar outro sistema/programa. (Pedro H., 23)

> Eu acho que o que é mais importante é que o *software* tem que estar lá pra ajudar e não pra causar mais problemas. Eu não indicaria porque pra pessoa que não tem tanta prática, não sabe o que fazer, eu acho que não é legal. O *software* tem que tá lá pra cumprir o papel dele e não causar mais incômodo do que precisa. (Marcelo, 27)

> Qualquer falha no *software*, tipo, tu tá achando que tá protegido e não tá na verdade, acho que faria com que eu não indicasse ou só se eu tivesse uma experiência muito ruim nesse sentido de tirar a produtividade. (Nathália, 26)

> Eu não gosto das muitas notificações, eu prefiro um *software* silencioso que faça o trabalho só quando eu precisar, só quando for necessário avisar sobre o vírus. Então eu não indicaria *softwares* que fazem muitas notificações. (Daniela, 23)

> Se ele for ruim, se ele der vírus quando não deveria. Sei lá, ele tá ali, então tem que proteger, né? (Maete, 22)

Por fim, os entrevistados também revelaram que um fator motivacional para a compra de um *software* de segurança é com relação ao armazenamento e criação de senhas. Este fator se mostrou bastante importante como característica de vantagem de um produto para algumas pessoas, pois conforme informações anteriores, a maioria usa as mesmas senhas ou as senhas são muito parecidas, gerando certo risco de segurança.

> Com certeza eu compraria porque eu perco muita senha, as minhas senhas eu acho que acabo criando de forma fácil já que eu não tenho programa de armazenamento. Já entraram nas minhas contas online inclusive porque

> minhas senhas são muito óbvias, então com certeza eu compraria. (Jéssica, 26)
>
> Sim, eu compraria e usaria muito porque eu preciso de um *software* desses, especialmente pro trabalho que eu esqueço todas as minhas senhas e eu sempre tenho criar novas senhas. Então sim, com certeza. (Daniela, 23)

Outros entrevistados afirmam que também comprariam, porém só o fariam se o programa tiver credibilidade e na condição de que o sistema funcionaria por completo, sem riscos das senhas serem roubadas, e se fossem práticos de usar.

> Sim, se fosse um programa de credibilidade estabelecida. (Tatiana, 25)
>
> Compraria com certeza se nunca fossem roubadas, mas se houvesse a mínima chance não usaria por medo. (Vanessa, 24)
>
> Me parece um produto atrativo em uma realidade que a gente tem cada vez mais acessos por senha e cada site pede pra criar um tipo diferente de senha. Acho que é um produto interessante, porém para eu comprar, dependeria muito do quão prático o programa fosse. (Pedro H., 23)
>
> Eu compraria se ele fosse conveniente usar, ou seja, se tivesse uma integração com o browser, assim como é o Google Chrome, por exemplo. (Marcelo, 27)

Apenas um entrevistado afirmou que não compraria nem usaria. Ele argumenta que não tem confiança em deixar todas suas senhas em um mesmo lugar. Ele comenta que esse fator seria ignorado num momento de compra, ou seja, tal caracterísitica de armazenamento de senhas não seria considerado uma vantagem. Entretando, outros dois comentam que não usariam por receio ou por limitação de dispositivos.

5 CONSIDERAÇÕES FINAIS

A presente monografia teve o propósito de estudar principalmente a percepção dos jovens de Porto Alegre – RS sobre segurança digital. Além disso, o estudo buscou analisar hábitos dos jovens na internet, hábitos de segurança digital e fatores motivadores e inibidores em um processo de compra de *software* de segurança.

De forma a realizar a investigação do tema, foi realizada uma pesquisa qualitativa por meio da técnica exploratória de entrevista em profundidade. A partir desse método, foram obtidas as informações que serviram como instrumentos de análise, a fim de que os resultados da pesquisa fossem desenvolvidos.

Através do processamento das informações provenientes da amostra entrevistada, composta por 10 informantes-chave, foi possível identificar as finalidades e frequências de uso da internet, apontar por quais dispositivos os jovens acessam a internet e quais os principais sites que navegam. Além disso, foi possível verificar a penetração e aderência dos produtos de proteção no âmbito digital no segmento jovem, assim como identificar os principais fatores motivadores e inibidores em um possível processo de compra.

De modo geral, as respostas das entrevistas ilustraram o cenário de que os jovens porto-alegrenses estão sempre conectados na internet, navegando, em média, 10 horas por dia. Apesar de não haver um controle de tempo e frequência de navegação por parte dos mesmos, sabem que é tempo demasiado *online*.

Seus principais objetivos ao usar a internet é entretenimento e comunicação. Os jovens acessam principalmente sites de redes sociais, como Facebook e Instagram, porém também gostam de ver vídeos no YouTube, assistir a séries e filmes na ferramenta *streaming* do Netflix e ouvir músicas no Spotify.

Além disso, os jovens preferem ler notícias nos sites dos principais canais de comunicação e se entretêem com blogs. Nem todos os jovens de 18 a 30 anos jogam *online,* porém todos utilizam ferramentas de procura como o Google para estudar ou buscar informações do dia-a-dia.

Os jovens utilizam muito mais o Smartphone em comparação com computador, notebook ou demais dispositivos. Para realizar o que julgam como principais atividades *online,* eles utilizam principalmente o celular.

Quando se trata de ambiente de trabalho, os jovens têm um controle maior de quanto tempo estão conectados. Todos usam sistema de *e-mail* e a maioria acessa páginas relacionadas à área da empresa, plataformas de tradução, assim como usam *softwares* específicos em suas áreas.

O principal objetivo com o uso da internet é otimizar e realizar as tarefas do dia-a-dia. Para realizar as atividades vinculadas ao trabalho, os jovens utilizam principalmente o computador ou notebook. Muitos jovens também utilizam smartphone para algumas atividades e alguns utilizam o celular como principal ferramenta de trabalho, pois julgam mais praticidade em atender clientes e na administração de contas *online* da marca ou empresa.

Em relação à segurança digital, os jovens entrevistados, na grande maioria, se sentem seguros quando refletem sobre seus hábitos de navegação, os quais julgam serem preventivos durante o uso da internet. Entretanto, quando analisam o contexto em que estão inseridos mais a fundo e percebem a vulnerabilidade digital a qual estão expostos o tempo todo que estão conectados, pode-se dizer que se preocupam com a segurança *online*.

Os informantes entendem a necessidade de proteção, entendem que o *software* de segurança existe nas máquinas justamente para detectar e combater qualquer ameaça proveniente de arquivos, links, sites, *downloads*, etc. Todos usam ou já usaram algum *software* de segurança para prevenir possíveis ameaças *online*, pois afirmaram que já sofreram ataques por vírus alguma vez na vida.

Os principais aspectos positivos revelados através de experiências com o uso do *software* de proteção foram a instalação tranquila, a máquina protegida de vírus desde o início do uso e a baixa interação com *software.* Já os principais aspectos negativos citados foram a demora e lentidão de varredura enquanto navegavam na internet, mensagens *pop ups* exigindo interação com o programa e sistema do *software* muito complexo.

Com relação à renovação, alguns jovens possuem a programação automática no sistema, pois se sentem satisfeitos com o desempenho do produto. Outros jovens comentaram que no momento em que a licença expira, não realizam a renovação. Buscam por outras soluções mais baratas do mercado tecnológico ou acabam aderindo um *software* gratuito, apesar deste último tipo não ter os mesmos benefícios e características de um pago.

Com relação à criação e ao uso de senhas nas contas da internet, pode-se dizer que os jovens entrevistados não percebem os riscos de utilizar a ou as mesmas senhas. Entretanto, em dezembro de 2016 foi noticiado na página da Forbes Tech sobre centenas de contas *premium* do Spotify terem sido expostas por conta de roubo de senhas.

Em abril de 2017 a Globo anunciou em sua página *online* que as algumas contas de usuários da Uber do Brasil foram invadidas e usadas até na Rússia. Ou seja, a partir de um roubo de uma conta em um local, as pessoas más intencionadas utilizaram os dados das vítimas para tirar vantagem em outro local.

O grande problema do uso das mesmas senhas é, na verdade, que através de um aplicativo, considerado de não muita relevância financeira para o usuário, pode ser a porta de entrada para outros aplicativos que revelam dados mais importantes e confidenciais. Quando o indivíduo usa a mesma senha para o Facebook e Uber, por exemplo, ele não se importa com o primeiro pois não há dados financeiros. Porém, se um *hacker* possuir a senha de um, poderá utilizar o outro e causar danos, às vezes, irreparáveis para a vítima.

Com relação aos termos, os informantes desta pesquisa associaram a expressão “*software* de segurança” diretamente com “antivírus”. Está claro que percebem isso como um produto que trabalha apenas combatendo diversos tipos de vírus. Entretanto, é pouco sabido que há muitas outras características em um *software*, assim como também não sabem a diferença entre um *software* pago e gratuito.

Quando se trata da expressão “antivírus”, os jovens associam diretamente com computadores. Isso se dá pelo fato de que os produtos Antivírus, quando surgiram no mercado, foram produzidos especialmente para máquinas como

computadores com o intuito de proteger os usuários de ameaças *online*. Na época, não existia smartphones e hoje em dia pouco se fala sobre proteção de dados para aplicativos em dispositivos móveis.

Essa questão também é controversa. De acordo com uma pesquisa feita com mais de 2 mil jovens, divulgada em julho de 2015 pelo Comitê Gestor da Internet (CGI), 82% dos jovens acessam a internet também por meio de smartphones e 32% através de tablets e a partir das análises deste estudo, os entrevistados utilizam principalmente aparelhos celulares para realizar a maioria das atividades *online*, incluindo no âmbito profissional, mas não usam nenhum aplicativo ou software de proteção para tal dispositivo. Apenas uma informante afirmou usar o *software* de segurança no seu smartphone, porém a grande maioria usa o produto apenas em seus computadores.

Pode-se afirmar, então, que se sentem seguros ao navegar na internet, apesar de estarem desprotegidos ou mais vulneráveis em seus smartphones. Entretanto, estão protegidos quando estão ou no ambiente de trabalho (por se tratar de corporações, acreditam que há equipe e programas de segurança digital) ou quando navegam de seus computadores (desktop e notebook).

Contudo, pode-se concluir através das respostas das entrevistas que os principais fatores elencados como motivacionais e inibidores são os mesmos, porém a forma como acontecem pode se tornar positivo ou negativo no ponto de vista do usuário.

O principal fator considerado pelos jovens é a questão do *software* realizar ou não sua principal função: proteger a máquina de ameaças digitais, detectando e combantendo-as. Se isso acontece, se torna o principal motivo pelo qual os jovens comprariam um software de segurança, do contrário, seria o principal motivo inibidor.

Com relação aos demais fatores, elencaram interação, performance e mensagens informativas aspectos importantes a serem considerados em um momento de compra. Os jovens preferem não interagir com o programa enquanto este realiza suas funções de proteção, bloqueio e varredura, além de que não querem ser impactados de nenhuma forma negativa enquanto utilizam sua máquina, seja a trabalho ou por lazer. Também julgam importante quando o software funciona de

forma a informar somente o que for necessário, pois preferem menor quantidade de mensagens *pop up*.

Nenhum jovem entrevistado citou preço, formas de pagamento ou tempo de duração da licença como fatores motivadores ou inibidores em um processo de compra.

5.1 LIMITAÇÕES DO ESTUDO

As limitações deste estudo incluem o fato de existir poucas pesquisas sobre segurança digital, principalmente quando se trata de Brasil, Rio Grande do Sul ou Porto Alegre. Além do mais, as poucas pesquisam que existem ou se dão à nível mundial ou se dão com foco no mundo corporativo, com objetivo de revelar a percepção ou aspectos de segurança empresarial. Acredita-se que a escassez de produções acadêmicas sobre este assunto possa ser em função da contemporaneidade desta temática.

Houve também certa dificuldade em encontrar bibliografia consistente sobre conteúdo de tecnologia, sobre *softwares* de segurança e marketing vinculado com produtos tecnológicos, assim como houve obstáculos na pesquisa sobre comportamento do consumidor sobre falhas de segurança digital. Há poucas publicações de referência que abordam estes temas de forma ampla. Grande parte das pesquisas na área possui enfoque em sistemas da computação e pesquisas qualitativas com índices em torno desta ciência.

Considerando o estágio de amadurecimento do tema deste estudo, optou-se uma pesquisa qualitativa para trazer dados e *insights* necessários para compreeder a percepção de segurança digital e os aspectos principais no momento de compra para então ser possível realizar posteriormente um estudo sobre o comportamento do consumidor jovem deste tipo de produto. A partir do número de jovens entrevistados para este estudo, não é possível ainda auferir uma generalização das conclusões. Assim, sugere-se uma pesquisa posterior que contemple outros aspectos da segurança digital ou pesquisa de forma quantitativa, utilizando os insumos obtidos nesta pesquisa qualitativa, a fim de verificar as conclusões levantadas com os 10 informantes-chave deste estudo.

5.2 RECOMENDAÇÕES NA IMPLEMENTAÇÃO DE AÇÕES DE MARKETING ESPECÍFICAS PARA EMPRESAS DO RAMO DE *SOFTWARE* DE SEGURANÇA

Empresas de tecnologia que ofertam produtos e serviços de proteção para eletrônicos costumam não diferenciar sua comunicação a partir dos segmentos de mercado. A partir das análises deste estudo sobre a percepção dos consumidores jovens acerca segurança digital e as informações coletadas sobre seus hábitos *online* e experiências com o produto, foi possível elencar algumas ações de marketing específicas com o intuito de informar, se aproximar e ofertar de forma assertiva para este público alvo.

As principais recomendações seriam desenvolver um plano de ação e manutenção a partir de três pilares, tais como: Informação, Relacionamento e Conversão. Abaixo, segue imagem que ilustra de forma geral os três pilares do plano de marketing sugerido para as empresas da área.

Figura 8 – Pilares do plano geral de Marketing

Fonte: a autora.

O primeiro pilar trata de trazer conhecimento acerca segurança *online*, tópicos sobre a temática abordando conteúdos do dia-a-dia dos jovens e dicas de proteção, já o segundo tem como objetivo se aproximar e manter relação com tais clientes, a fim

de criar experiências, convidando jovens a participarem em eventos e palestras. O último pilar seria a base para ações de conversão, ou seja, a partir de programas de incentivo de compra, os jovens podem aproveitar ofertas especiais do produto para adquirir.

A partir desta estrutura, as empresas podem elaborar ações 360°, ou seja, ações que interliguem todos os aspectos, trazendo melhor experiência para o jovem com o assunto e o produto. Contudo, tais pilares sugeridos têm o intuito de serem a base de uma comunicação estruturada e integrada com ações que causem reflexão por parte dos jovens e mudança de comportamento com relação à segurança, fazendo com que percebam a segurança como aspecto fundamental em suas vidas digitais.

5.2.1 Ações de informação

A internet proporciona acesso a uma infinidade de informação, diversão e entretenimento. Mas, durante a navegação, todo usuário está sujeito a diversos tipos de ameaças. Com o intuito de educar os jovens sobre a temática da segurança digital, as empresas que ofertam *softwares* de segurança ou eletrônicos que têm o *software* embarcado podem realizar ações através de canais de comunicação, tais como as mídias sociais, site de conteúdo e *newsletter,* veiculando conteúdos de segurança na internet, principais riscos e demais temáticas que sejam de interesse jovem, tais como privacidade, jogos *online*, entre outros.

5.2.1.1 Canais de comunicação

O grande papel dos canais de comunicação é levar informação para o público em que se quer abordar. É sugerido para as empresas deste ramo criar canais sólidos de comunicação com os jovens a fim de levar conhecimento sobre o tema segurança digital e afins. É importante que os jovens estejam informados sobre os riscos aos quais estão expostos e que tenham uma melhor compreensão da internet, podendo então aproveitar seus benefícios de forma segura.

A criação de contas nas redes sociais é fundamental, pois é o que os jovens principalmente acessam no seu dia-a-dia e o canal por onde mais interagem. Os principais sites e aplicativos são Facebook e Instagram, seguidos por YouTube e Twitter, pelos quais recebam a inforamação de forma rápida e prática a partir de fotos,

vídeos e pequenos textos. Nestas páginas também é possível que os jovens interajam com a empresa e entre eles a partir de curtidas, comentários e compartilhamento.

Além das redes sociais, é importante para as empresas terem um banco de dados atualizado com as principais informações dos jovens, principalmente o endereço de email e residencial. A partir destes dados, é possível enviar informações em formato de *newsletter*, ou seja, distribuição regular para assinantes que aborda geralmente um determinado assunto, e catálogos de produtos e principais benefícios.

As empresas também podem manter páginas *online* ativas, tais como blog e portais de informação ou desenvolver páginas que direcionem para estes formatos em seu site comercial. É importante que dentro do site da empresa haja um espaço para que os consumidores possam esclarecer suas dúvidas e compartilhar suas opiniões sobre o produto.

5.2.1.2 Conteúdo

As empresas deste ramo devem trazer conteúdos de forma clara e objetiva para os jovens, podendo ser veiculados em forma de infográficos, banners online, publicações nas redes sociais, vídeos informativos e até em cartazes e flyers nos principais ambientes onde os jovens se encontram, como escolas, universidades e shoppings. Os principais conteúdos sugeridos a serem abordados são:

- Segurança na internet
- Termos digitais
- Golpes e ataques na internet
- Mecanismos de segurança
- Administração de contas e senhas
- Privacidade na internet
- Plágio e violação de direitos autorais
- Jogos *online*

É importante que os jovens tenham um referencial de segurança *online* para que possam tomar medidas preventivas necessárias enquanto navegam. Os conteúdos podem abranger aspectos mais básicos, como por exemplo a diferença entre os termos “antivírus” e “*software* de segurança”, diferença entre as ofertas pagas

e gratuitas, e mais técnicos, como explicação de termos digitais (spam, malware, criptografia, etc), levando a informação de ponta a ponta para os jovens.

Para os jovens não se tornarem mais um vítima de ameaças digitais, as empresas deste ramo podem publicar dicas de segurança para os internautas se manterem em alerta em relação as eventuais armadilhas. As principais dicas para os jovens prestarem atenção devem se basear principalmente em conteúdos sobre furto de dados e identidade pessoal, diferentes tipos de vírus e como atacam, espionagem digital e propagação de aplicativos e links falsos.

Assuntos interessantes a serem trazidos em formato de textos em blogs ou publicação nas redes seriam comportamento de compra na internet, dicas de como podem se prevenir, proteger seus dados e como podem identificar sites inseguros no momento de compra. Tais conteúdos fazem parte dos hábitos dos jovens, os quais têm costume de realizar compra online.

Além do mais, temas como *cyberbullying* e nudez são bastante atuais e podem impactar negativamente a vida os jovens quando se expõem *online*. Estes assuntos não estão diretamente associados com o produto de *software* de segurança, porém são fundamentais para criar aproximação com os jovens e mostra que a empresa se importa com este público, trazendo relevância para a marca do produto.

5.2.2 Ações de relacionamento

A partir do momento que as empresas estão levando informação sobre o tema de segurança para os jovens, é muito importante que desenvolvam interação e mantenham contato para que se crie uma relação sólida entre as partes. O relacionamento é fundamental para que as empresas conheçam as perspectivas dos clientes e então possam gerar satisfação aos jovens.

Ações que possibilitam esta interação são realizações de eventos, palestras e *workshops*, ou seja, cursos intensivos de curta duração com demonstrações de técnicas e saberes sobre um tema. Além do mais, criação de fóruns *online*, assim como pesquisas de satisfação e de compreensão do perfil do cliente também são importantes para estabeler laço de confiança com os jovens.

Eventos, palestras e *workshops* seriam interessantes acontecer nas principais escolas e universidades de Porto Alegre, pois é o local onde mais se concentram os jovens e onde as empresas poderiam ter abertura e espaço para trazerem um conteúdo importante dentro do contexto atual. Nestes tipos de ações, técnicos de TI podem participar e trazer conteúdos mais técnicos para estudantes do ramo, por exemplo.

Neste espaço, jovens que já foram afetados de alguma forma *online* (roubo de dados, clonagem de cartão, ataques de vírus, entre outros) podem ser convidados a relatarem suas experiências, contarem a quem recorreram e como buscaram por proteção após o dano. Assim, é possível que os jovens criem maior identificação e possam compartilhar entre eles suas experiências e opiniões acerca do assunto.

As empresas também podem participar de feiras de tecnologia em que produtos eletrônicos são vinculados à internet, mostrando como seus produtos funcionam, comunicando os principais benefícios e entregando folhetos informativos para o público. Feiras do ramo *gaming*, ou seja, de jogos digitais, como a *Brazil Game Show* por exemplo, também são importantes de haver a participação destas empresas de segurança digital, pois o público alvo é focado em jovens.

Os jovens que têm costume de jogar *online* também precisam ser abordados para que reflitam sobre seus hábitos de uso de internet e tenham cautela enquanto jogam. Na maioria dos casos suas informações pessoais não são divulgadas, porém a rede em que se conectam tornam o ambiente muito vulnerável a ataques de vírus.

5.2.3 Ações de conversão

Quando as empresas desenvolvem estratégias de comunicação assertiva através dos principais canais de interação, elaboram conteúdos relevantes sobre uma temática e planejam os formatos de como vão se relacionar e se comunicar com seus clientes, o próximo passo é converter tais ações em vendas. A partir do engajamento anterior, as empresas do ramo podem criar e estruturar programas de incentivo à compra de produtos de segurança digital.

Tal estratégia de conversão se baseia na interação anterior e nos dados pessoais dos jovens que são ou podem vir a ser novos clientes. Quando jovens são

captados pela empresa, estes estão automaticamente aptos a participar de programas de incentivo.

As ações podem ser diversas e as empresas podem sortear produtos, brindes, experiências ou fornecer cupons de desconto específicos para o público jovem. O incentivo pode ser divulgado em específico a partir do cadastro do cliente no site da empresa ou podem haver campanhas e sorteios nas redes sociais.

O programa também pode ter o formato de pontuação, ou seja, aquele que realizar compra de certo produto ou indicar alguém para compra pode acumular pontos a serem trocados por outros produtos ou viagens. Com relação à renovação da licença do *software* de segurança, podem ser feitas ações focadas em desconto, a fim de alavancar o número de renovações.

Com o intuito de facilitar a compra por jovens, opções diferenciadas de pagamentos podem ser estudadas e condicionadas dentro do programa. Assim, os jovens podem ter maior interesse em participar porque estará experienciando os benefícios financeiros além dos benefícios de conhecimento e conscientização.

5.2.4 Ações 360°

A partir da estrutura com base na informação, relacionamento e conversão, as empresas podem elaborar ações que englobem os três pilares, a fim de abranger todas as áreas e impactar o jovem 360°. É fundamental que todos os canais que a empresa optar por utilizar estejam em harmonia quanto ao processo de atendimento, ao histórico do cliente e quanto à identidade visual.

O uso de todos os canais de interação e o fato de eles estarem todos conectados é denominado pelo termo *Omni-channel*, o qual se caracteriza pela conexão entre os canais de comunicação e o cliente usufruir simultaneamente os canais. Então, ações que envolvam todos os canais são interessantes para que os jovens possam interagir de todas as formas com a empresa.

Ações como criação de campanha de *software* de segurança nas redes socias, vinculando com uma *hashtag* específica sobre o tema segurança, ou seja, um composto de palavras-chave, ou de uma única palavra que é usado junto com o símbolo cerquilha (#) a fim de se referir a alguma coisa. Assim, os jovens que aderirem

à campanha nas mídias sociais, curtirem e divulgarem podem ser sorteados a ganhar uma licença do produto ou cupom de desconto, ganhando um convite para participar de um *workshop* ou palestra.

As campanhas e programas de incentivo podem ser divulgadas também através dos próprios eventos de relacionamento e aqueles que interagirem nas redes sociais, vinculadas com a campanha, podem ganhar algum brinde da marca, como canetas, *pendrives*, entre outros. Outro formato poderia ser de divulgação através do site, blog ou redes sociais para participarem de um evento ou palestra e, aqueles que forem e realizarem cadastro durante o evento vão receber ofertas exclusivas e dicas de segurança através de *newsletter* ou email marketing.

Tais ações podem fortalecer a relação com os jovens, ganhar credibilidade de marca e ampliar o mercado de *softwares* de segurança através das abordagens dos conteúdos. Os jovens são os principais alvos das ações, porém se os resultados forem positivos, seria possível fazer um estudo para identificar a pertinência das ações para demais segmentos.

Abaixo, segue figura ilustrativa compilando as principais ações abordadas nos tópicos de cada pilar, assim como exemplos de ações que podem ser feitas em ações de 360º para o público jovem.

Figura 9 – Plano de ações de Marketing

Fonte: a autora.

5.3 SUGESTÕES PARA FUTURAS PESQUISAS

Para fins de continuar a investigação sobre o tema de segurança digital, recomenda-se ainda pesquisar os principais motivos pelos quais os jovens não aderiram ao *software* de segurança em dispositivos móveis, tais como smartphones e tablets. Além disso, neste presente estudo não foi investigado a fundo a questão de renovação ou nova compra de licenças do *software* de segurança, assim como não foram pesquisados os impactos dos aspectos financeiros, como preços e formas de pagamento relativos à compra.

Neste estudo também não foi abordado com profundidade os principais motivos os quais levam os jovens a criarem o mesmo padrão de senhas e quais suas percepções acerca do uso das mesmas senhas para todas suas contas *online.* Além do mais, o tempo de duração da licença também foi um aspecto não mencionado e investigado ao longo do estudo, não podendo então ser refletido nas análises e não corresponder com os presentes resultados.

Temas como *cyberbullying* e nudes, vinculados ao uso de internet e que podem ter relação com a questão de segurança *online* associada à privacidade e intimidade dos jovens porto-alegrenses, não foram abordados no estudo, nem mencionados nas

entrevistas, podendo ser assuntos relevantes em ações de marketing, a fim das empresas se aproximarem da realidade deste público em específico. Com relação à falha de segurança, nenhum informante mencionou experiências passadas ou como foi seu comportamento, podendo ser outro tópico a ser abordado em futuras pesquisas.

Essas informações que não foram trazidas na presente pesquisa também seriam importantes e fundamentais para continuar a compreensão sobre os hábitos dos jovens com relação ao uso de *softwares* de segurança, a fim de as empresas do ramo poderem analisar os resultados e, posteriormente, elaborar um plano de comunicação de marketing mais estruturado, podendo comunicar e ofertar seus produtos e benefícios de forma mais assertiva para este público em questão.

A fim de comparação, podem ser estudadas as estratégias de marketing de campanhas paralelas que já aconteceram na cidade, as quais tenham utilizado em seus planos de ações o apelo ao medo. Entender se tais ações obtiveram sucesso no objetivo e adesão por parte dos consumidores pode ser relevante para verificar a eficácia do apelo ao medo e desenvolver este tipo de abordagem nas ações voltadas para a temática da segurança digital, fazendo com que mais jovens usem *softwares* de segurança e estejam protegidos, principalmente em seus smartphones.

REFERÊNCIAS

AAKER, D. A.; KUMAR, V.; DAY, G. S. **Pesquisa de marketing**. São Paulo: Atlas, 2001.

ABINEE. **Base de dados do setor eletrônico.** Disponível em: <http://www.abinee.org.br/abinee/decon/dados/> Acesso em: 18 de abril de 2017.

AVIZIENIS, A.; LAPRIE, J.; BRIAN, R.; CARL, L. Basic Concepts and Taxonomy of Dependable and Secure Computing. **IEEE Transactions on Dependable and Secure Computing,** 2004.

BELCH, G. E.; BELCH, M. A. **Propaganda & promoção: uma perspectiva da comunicação integrada de marketing**. São Paulo: McGraw-Hill, 2008.

BEVILAQUA, B. Ciméa. **Consumidores e seus direitos: um estudo sobre conflitos no mercado de consumo.** São Paulo: Humanitas; NAU, 2008.

BLACKWELL, R. D.; MINIARD, P. W.; ENGEL, J. F. **Comportamento do Consumidor.** São Paulo: Pioneira Thomson Learning, 2005.

CARO, Abrão. **Fatores críticos do comportamento do consumidor online**. São Paulo, 2005.

CERTO, Samuel C. **Administração moderna.** 9 ed. São Paulo: Prentice Hall, 2003.

CETIC. **Pesquisa e Indicadores.** Disponível e: <http://cetic.br/pesquisas/> Acesso em: 19 de abril de 2017.

CZINKOTA, M. R. **Marketing: as melhores práticas.** Porto Alegre, RS: Bookman, 2001.

FERNANDES, Jorge H. C. **O que é um Programa (Software).** UNB, 2002.

FLICK, Uwe. **Desenho da Pesquisa Qualitativa**. Porto Alegre: Artmed, 2009.

FUSTAINO, J.; PONCHIO, M. C.; GIULIANI, A. C. **Cultura de Consumo - la evolución en la Sociedad Brasileña y Mexicana.** In: GIULIANI, A. C.; MORALES, M. A. P. (Org.). Marketing contemporáneo: un enfoque latinoamericano. 1ed. México: Fomento Editorial UMAD, v. 1., 2009.

GARTNER. **Previsões de Gartner sobre Internet das Coisas (IoT).** Disponível em: <http://www.gartner.com/newsroom/id/2688717> Acesso em: 27 de abril de 2017.

GASKELL, G. Entrevistas Individuais e Grupais. In: BAUER, M. W; Gaskell, G. (Org.). **Pesquisa Qualitativa com Texto, Imagem e Som:** Um Manual Prático. 8. ed. Petrópolis: Vozes, 2010.

GOODRICH, M.; TAMASSIA, R. **Introduction to Computer Security.** 1st ed. New York: Addison Wesley, 2010.

GUTIERREZ, R. M. V.; ALEXANDRE, P. V. M. Complexo Eletrônico: introdução ao *software*. **BNDS Setorial,** Rio de Janeiro, n.18 e n.20, set. 2004

KARSAKLIAN, Eliane. **Comportamento do Consumidor.** São Paulo: Atlas, 2000.

KOTLER, Philip. **Administração de Marketing: a edição do novo milênio.** São Paulo, Pearson Prentice Hall, 2005.

LINS, B. F. E. (coord.). **O mercado de softwares no Brasil: problemas institucionais e fiscais.** Caderno de Altos Estrudos – 3. Brasília: Câmara dos Deputados, 2007.

MALHOTRA, N. **Pesquisa em Marketing:** uma orientação aplicada**.** 4. ed. Porto Alegre: Bookman, 2006.

MATTAR, F. N. **Pesquisa de Marketing, edição compacta**. 4. ed. São Paulo: Atlas, 2008.

MOWEN, J. C.; MINOR, M. S. **Comportamento do consumidor.** Pearson Prentice Hall, 2003.

PARASURAMAN, A.; COLBY, C. L. **Marketing para Produtos Inovadores: Como e por que seus clientes adotam tecnologia.** Porto Alegre: Bookman, 2002.

ROESCH, S. M. A. **Projetos de estágio e de pesquisa em administração:** guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. 3. ed. São Paulo: Atlas, 2006.

SITE BLINDADO. **70% dos consumidores acreditam que segurança online é responsabilidade dos sites.** Disponível em: <http://blog.siteblindado.com/2017/03/03/70-dos-consumidores-acreditam-que-seguranca-online-e-responsabilidade-dos-sites/> Acesso em: 26 de novembro de 2017.

SOFTEX. **Software e serviços de TI**: A indústria brasileira em perspectiva. Campinas: Publicação SOFTEX, 2009.

SOLOMON, M. R. **O comportamento do consumidor: comprando, possuindo e sendo.** 5. Ed. Porto Alegre: Bookman, 2002.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology.** National Institute of Standards and Technology, 2002.

TELECO. **Vendas de smartphones em 2016.** Disponível em: <http://www.teleco.com.br/smartphone.asp> Acesso em: 18 de abril de 2017.

UNESCO. **Towards Knowledge Societies.** Unesco Publishing, 2005.

VERIZON ENTERPRISE. **A secure cyberspace: who's responsible?** Disponível em: <http://www.verizonenterprise.com/resources/reports/rp_dbir_secure-cyberspace_en_xg.pdf> Acesso em: 27 de abril de 2017.

APÊNDICE A – ROTEIRO DE ENTREVISTA DIRIGIDA AO CONSUMIDOR FINAL

1. Qual a sua interação com a internet?
2. Quais são seus objetivos ao usar a internet?
3. Quais dispositivos utiliza para acessar à internet?
4. Como você administra seus dados (fotos, informações pessoais etc) na internet?
5. Como você se sente ao navegar na internet, em termos de segurança?
6. Já foi afetado por algum tipo de vírus ou ameaça virtual alguma vez? Conte a experiência.
7. Como e onde você busca informações sobre segurança digital?
8. Você já comprou ou utilizou algum *software* de segurança em seus dispositivos? Conte a experiência.
9. Você indicaria (ou já indicou) um *software* de segurança que já tenha utilizado para alguém? Por quê?
10. O que lhe faria não indicar um *software* de segurança?
11. O que você entende por “software de segurança”?
12. O que você entende por “antivírus”?

Dados Pessoais

Nome:

Idade:

Formação:

Profissão:

Renda: