CENTRO UNIVERSITÁRIO UNIHORIZONTES

Programa de Pós-graduação em Administração Mestrado

Marciana Carvalho Pereira de Souza

O PAPEL DA TRÍADE SOCIEDADE, GOVERNO E INDIVÍDUO NA PREVENÇÃO DE CIBERCRIMES: Um estudo no âmbito do marketing macrossocial

Belo Horizonte
2023

Marciana Carvalho Pereira de Souza

O PAPEL DA TRÍADE SOCIEDADE, GOVERNO E INDIVÍDUO NA PREVENÇÃO DE CIBERCRIMES: Um estudo no âmbito do marketing macrossocial

Projeto de dissertação apresentado à banca de qualificação, no Mestrado Acadêmico em Administração do Centro Universitário Unihorizontes, como requisito parcial para obtenção do título de Mestra em Administração.

Orientadora: Profª. Drª. Caíssa Veloso e Sousa

Área de concentração: Organização Estratégica

Linha de pesquisa: Estratégia, inovação e competitividade

Belo Horizonte
2023

SOUZA, Marciana Carvalho Pereira de

S729p

O papel da tríade sociedade, governo e indivíduo na prevenção de cibercrimes: um estudo no âmbito do marketing macrossocial. Belo Horizonte: Centro Universitário Unihorizontes, 2023.

159p.

Orientadora: Drª. Cassia Veloso e Sousa

Dissertação (mestrado). Centro Universitário Unihorizontes. Programa de Pós-graduação em Administração.

1. Marketing social – macrossocial – cibercrimes – tríade sociedade I. Marciana Carvalho Pereira de Souza II. Centro Universitário Unihorizontes – Programa de Pós-graduação em Administração. III. Título

CDD: 658.8

Ficha catalográfica elaborada pelo Bibliotecário Unihorizontes
- Bruno Tamiett de Almeida CRB6 3082 -

ATA DE DEFESA

DECLARAÇÃO DE REVISÃO DE PORTUGUÊS
DISSERTAÇÃO DE MESTRADO

Declaro ter procedido à revisão da dissertação de mestrado intitulada **O PAPEL DA TRÍADE SOCIEDADE, GOVERNO E INDIVÍDUO NA PREVENÇÃO DE CIBERCRIMES: Um estudo no âmbito do marketing macrossocial**

apresentada ao curso de Mestrado Acadêmico Centro Unihorizontes, como requisito parcial para obtenção do título de

MESTRA EM ADMINISTRAÇÃO

de autoria de

MARCIANA CARVALHO PEREIRA DE SOUZA

contendo 165 páginas

sob orientação de

Profª. Drª. CAISSA VELOSO E SOUSA

ITENS DA REVISÃO:

- Correção gramatical
- Inteligibilidade do texto
- Adequação do vocabulário

Belo Horizonte, 19 de março de 2023

Fernando José de Sousa
REVISOR

Registro: 20710, Livro LR-36 – Decreto nº 5786/2006, Processo 2758814/2014
Licenciado em LETRAS
Centro Universitário de Belo Horizonte
UNI-BH

REVISADO

AGRADECIMENTOS

À Deus, pelo dom da vida e por guiar os meus passos.

À minha família, pela paciência e tolerância com o tempo despendido na elaboração deste estudo. Aos meus avôs paternos (*in memoriam*), Joaquim e Alice, e avôs maternos (*in memoriam*), Ambrósio e Eva, que me deram pais incríveis, apoiaram nossa família e me dedicaram amor. Aos meus pais, Francisco e Vera Lúcia, que me deram a vida, cuidaram com muito amor nos momentos difíceis e sempre se preocuparam com nossos estudos. Aos meus queridos irmãos pela união fraterna que fortalece nossos caminhos. Aos meus sobrinhos que alegram as nossas vidas.

Aos amigos que me ajudaram participando da pesquisa e me incentivaram para a conclusão do trabalho.

Aos funcionários do Hospital das Clínicas da UFMG que participaram da pesquisa.

À PRORH da UFMG que me incentivou ao término deste curso.

À Profª. Drª. Caíssa Veloso e Sousa, responsável pela orientação desta pesquisa que habilidosamente e carinhosamente me ensinou sobre o marketing macrossocial.

À banca que se dispôs a ler a minha pesquisa: Prof.ª Dr.ª Renata Francisco Baldanza e Prof. Dr. Jersone Tasso Moreira Silva.

Ao Prof. Dr. Luiz Rodrigo Moura, responsável pela técnica de análise dos dados dessa pesquisa.

Ao Prof. Fernando José de Sousa, responsável pela revisão desse trabalho.

Aos demais Professores da Unihorizontes e da UNA que contribuíram com a minha formação.

Aos Funcionários da Unihorizontes e da UNA, que tornaram possível o término dos meus estudos.

À Cristina Vieira e funcionários do Terminal Rodoviário Governador Israel Pinheiro em Belo Horizonte, pela acolhida durante a coleta dos dados da pesquisa.

Aos colegas do curso de Mestrado pela convivência enriquecedora durante o processo de redação do projeto dessa pesquisa.

A coisa mais indispensável a um homem é reconhecer o uso que deve fazer do seu próprio conhecimento.
(Platão)

RESUMO

As ameaças e a falta de segurança no ciberespaço tornaram-se um problema social complexo, tendo em vista que os indivíduos, a sociedade e o governo são alvos dos cibercriminosos. Neste contexto, esta pesquisa tem como objetivo identificar a influência dos três níveis do marketing macrossocial na adoção de comportamentos digitalmente seguros. O referencial teórico baseia-se em estudos desenvolvidos em segurança de rede e marketing macrossocial em um contexto digital. Quanto ao método trata-se de um estudo descritivo com abordagem quantitativa adotando-se o método de análise multivariada. A amostra foi composta de 294 indivíduos com aplicação de questionários para aqueles com idade acima de 18 anos. Os resultados indicam, quanto ao nível *downstream*, que as pessoas percebem e se preocupam com a segurança no ambiente digital e agem de forma apropriada. De outro lado, verifica-se que o nível *midstream* impacta os comportamentos de segurança. No nível *upstream*, as ações públicas são capazes de afetar o comportamento dos indivíduos. Conclui-se haver a necessidade do governo brasileiro de promover leis, campanhas para um ambiente digital seguro e oferecer recursos educativos digitais para a segurança na internet.

Palavras-chave: Marketing macrossocial. Marketing e Sociedade. TI e Sociedade. TI e Governo.

SUMMARY

Threats and lack of security in cyberspace have become a complex social problem, given that individuals, society and the government are targets of cybercriminals. In this context, this research aims to identify the influence of the three levels of macrosocial marketing on the adoption of digitally safe behaviors. The theoretical framework is based on studies developed in network security and macrosocial marketing in a digital context. As for the method, it is a descriptive study with a quantitative approach adopting the multivariate analysis method. The sample consisted of 294 individuals who administered questionnaires to those over 18 years of age. The results indicate, at the downstream level, that people perceive and care about security in the digital environment and act appropriately. On the other hand, it appears that the midstream level impacts security behaviors. At the upstream level, public actions are capable of affecting the behavior of individuals. It is concluded that there is a need for the Brazilian government to promote laws, campaigns for a safe digital environment and offer digital educational resources for internet security.

Keywords: Macrosocial marketing. Marketing and Society. IT and Society. IT and Government.

RESUMEN

Las amenazas y la falta de seguridad en el ciberespacio se han convertido en un problema social complejo, dado que los individuos, la sociedad y el gobierno son objetivos de los ciberdelincuentes. En este contexto, esta investigación tiene como objetivo identificar la influencia de los tres niveles del marketing macrosocial en la adopción de comportamientos digitalmente seguros. El marco teórico se basa en estudios desarrollados en seguridad de redes y marketing macrosocial en un contexto digital. En cuanto al método, se trata de un estudio descriptivo con enfoque cuantitativo adoptando el método de análisis multivariado. La muestra estuvo compuesta por 294 individuos que administraron cuestionarios a mayores de 18 años. Los resultados indican, a nivel descendente, que las personas perciben y se preocupan por la seguridad en el entorno digital y actúan de manera adecuada. Por otro lado, parece que el nivel intermedio afecta los comportamientos de seguridad. En el nivel superior, las acciones públicas son capaces de afectar el comportamiento de los individuos. Se concluye que es necesario que el gobierno brasileño promueva leyes, campañas para un entorno digital seguro y ofrezca recursos educativos digitales para la seguridad en internet.

Palabras clave: Marketing macrosocial. Marketing y Sociedad. TI y sociedad. TI y gobierno.

LISTA DE ILUSTRAÇÕES

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS *(continua)*

LISTA DE TABELAS *(concluso)*

LISTA DE ABREVIATURAS *(continua)*

ABNT	Associação Brasileira de Normas Técnicas
AC	*Alpha de Cronbach*
ADCE	Associação dos Dirigentes Cristãos de Empresas
AFE	Análise fatorial exploratória
Anpad	Associação Nacional de Pós-Graduação e Pesquisa em Administração
ANPD	Autoridade Nacional de Proteção de Dados
ARPAnet	*Advanced Research Projects Agency Network*
AVE	Variância média extraída
Capes	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CBM	*Common Method Bias*
CC	Confiabilidade composta
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
CETIC.br	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CFI	Índice comparativo de ajuste
CGI.br	Comitê Gestor da Internet no Brasil
EFTA	*European Free Trade Association*
FBI	*Federal Bureau of Investigation*
GDPR	Regulamento Geral de Proteção de Dados da União Europeia
GFI	Índice de qualidade do ajuste
HIV	Vírus da Imunodeficiência Humana
HTTPS	*HyperText Transfer Protocol Secure*
IBGE	Instituto Brasileiro de Geografia e Estatística
IDS/ IPS	*Intrusion Detection and Prevention System*
IFI	Índice incremental de ajuste

LISTA DE ABREVIATURAS *(continua)*

IM	Gerenciamento Interativo
IPSec	*Internet Protocol Security*
ISO	*Internacional Organization for Standardization*
LGPD	Lei Geral de Proteção aos Dados
KMO	Teste de *Kaiser-Meyer-Olkin*
K-S	Teste de *Kolmogorov-Smirnov*
MAS	Teoria do Mecanismo, Ação, Estrutura
ML	*Maximum Likelihood*
MLP	Teoria da Perspectiva Multinível
MPF	Ministério Público Federal
MSA	Medida de Adequacidade da Amostra
NAC	*Implement a network access control*
NAP	*Network access protection*
NBR	Normas Brasileiras
NEPS	National Educational Panel Study
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONG	Organizações não Governamentais
PGP	*Pretty Good Privacy*
PIAAC	*Programme for the Internacional Assessement of Adult Competencies*
PNAD	Pesquisa Nacional por Amostra de Domicílios
RADIUS	*Remote Access Dial-In User Service*
RMSEA	Raiz do erro quadrático médio de aproximação

LISTA DE ABREVIATURAS *(concluso)*

Scielo	*Scientific Eletronic Library Online*
SEM	Modelagem de equações estruturais
SGSI	Sistema de Gestão de Segurança da Informação
Spell	*Scientific Periodicals Eletronic Library*
SSL	*Secure Sockets Layer*
SSM	Marketing dos Sistemas Sociais
TACACS+	*Terminal Access Controller Access Control System Plus*
TI	Tecnologia da Informação
TICs	Tecnologias da informação e da comunicação
TLI	Índice de *Tucker-Lewis*
TLS	*Transport Layer Security*
UE	União Europeia
VPN	*Virtual Private Network*
WAP	*Wireless Application Protocols*
ZTNA	*Zero Trust Network Acess*

SUMÁRIO *(continua)*

SUMÁRIO *(concluso)*

1 INTRODUÇÃO

O ataque cibernético compreende importante ameaça mundial, pois, penetra nas redes de computadores domésticos, organizacionais e governamentais. Para mitigar esse risco é preciso desenvolver ações de segurança da informação e comunicação para garantir dentro do espaço cibernético a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

A integração da tríade indivíduo, sociedade e governo se faz necessária para o engajamento e sincronicidade no que tange à segurança cibernética no país. Essa preocupação se torna mais evidente a partir do cenário, no qual as trocas de informações digitais são crescentes para os serviços das mais diversas naturezas como bancários, de comércio eletrônico, em redes sociais, dentre outros, além de cruciais na manutenção das infraestruturas críticas de um país. Portanto, é um desafio que exige um esforço amplo de trabalho para proteção da sociedade e do Estado Brasileiro (Brasil, 2010).

Diante do risco de ataques cibernéticos às redes e aos sistemas de informações em suas diversas esferas, mitigá-los e definir as fronteiras do espaço cibernético impactam o cotidiano dos indivíduos, dos empreendedores e do governo. Isso requer conversação e troca de ideias para que dados e informações conhecidas sobre o tema possam ser utilizados e se desenvolvam iniciativas e melhores práticas na sociedade, nas organizações, seja dentro do país ou entre países (Brasil, 2010).

A vulnerabilidade dos indivíduos aos cibercrimes está relacionada à facilidade em se ocultar a identidade que o criminoso encontra no mundo virtual, ao analfabetismo digital da população e ao desconhecimento sobre como e onde denunciar para se evitar recorrências. Também, a diversidade das ameaças e a rapidez que se inovam contribui com a criminalidade, pois, o indivíduo não consegue acompanhar as atualizações dos mecanismos de segurança digital diante de ataques ao sistema operacional e *software*, erros do servidor web, brechas nos códigos de programação dos sites, fragilidades nas redes entre outros (Tambara, Batista & Freitas, 2014; Cavedon, Ferreira & Freitas 2015).

O grande interesse dos cibercriminosos são os dados pessoais ou informações que possam ser transformadas em dinheiro. Fato é que o tempo de exposição e a rotina do dia-a-dia por meio virtual, expõem o indivíduo ao fornecimento de dados de interesse dos criminosos e deixam rastros na internet. Além disso, os indivíduos acabam confiando nas recomendações que recebem nas páginas de compras, bancos, etc. que solicitam dados, reforçando a

vulnerabilidade desse em uma época que a exposição no mundo digital se tornou frequente nas redes sociais (Tambara, Batista & Freitas, 2014; Cavedon, Ferreira & Freitas, 2015).

De acordo com Tambara, Batista e Freitas (2014) e Cavedon, Ferreira e Freitas (2015), o indivíduo mostra seus interesses, gostos, hábitos com muita naturalidade nas redes sociais e o mesmo comportamento com seus dados na internet. A influência das redes sociais sobre o indivíduo induz a comportamentos inconscientes que comprometem sua segurança diante da sua falta de resistência e defesa provocado pelo neuro marketing da cultura de exposição. Assim, a proteção nesse ambiente torna-se imprescindível, porém, ainda difícil de ser garantida diante da incipiência da polícia e da justiça nesta área que vem ganhando robustez com as alianças em diversos níveis no combate ao cibercrime.

Conforme Oliveira Júnior (2016), as organizações governamentais e privadas podem realizar técnicas de detecção de intrusão para levantamento de ataques cibernéticos para proteção de informações e de sistemas. Entretanto, essas tecnologias de detecção fornecem informações acerca de fatos já ocorridos, quando em caso de interrupção ou anomalia no funcionamento dos serviços. O ambiente *HoneySELK* propõe amenizar esses danos provocados por ciberataques, isto é, um ambiente de pesquisa ao alcance dos atacantes capaz de controlar, capturar, analisar e visualizar em tempo real os ataques e as vulnerabilidades.

Os prejuízos causados pelos ciberataques são difíceis de serem estabelecidos, porque as empresas atacadas não podem divulgar as informações para não expor suas vulnerabilidades, ou serem consideradas inseguras ou possuidoras de sistemas pouco confiáveis. Essas têm investido em medidas preventivas para evitar ataques contra a confidencialidade, a integridade e a disponibilidade. As perdas causadas incluem, além do roubo dos dados pessoais, manipulação do mercado financeiro, redução de confiança nas atividades *on-line*, interrupção de serviços, custo para proteção das redes, contratação de seguros, danos à reputação da empresa invadida, risco de responsabilização, risco à marca da empresa, entre outros (W. Silva, 2018).

Conforme Pezzella e Wenczenovicz (2015) e Parchen, Freitas e Meireles (2018), a proteção das redes é importante na segurança dos dados pessoais e empresariais para garantir que não se tenha acesso aos dados confidenciais não autorizados, evitando-se danos acidentais e intencionais. Esses podem ser ocasionados pela coleta excessiva de aplicativos e de *sites* ou pela perda de dados, por meio da ação de códigos maliciosos e pela invasão de contas e golpes de engenharia social, ou seja, a manipulação, por criminosos, para engendrar e induzir o usuário a enviar dados privados, infectar dispositivos com *malware* ou clicar em *links* para sites infectados. Portanto, a adoção de medidas educativas auxilia na prevenção dos ataques

cibernéticos.

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Núcleo de Informação e Coordenação do Ponto BR (NIC.br), Comitê Gestor da Internet no Brasil (CGI.br) e Autoridade Nacional de Proteção de Dados (ANPD) (2021) destacam a importância dos *backups* dos arquivos como forma de proteção dos dados, caso ocorram problemas com os equipamentos ou se perca o dispositivo. Simultaneamente, a conversão do texto claro em texto incompreensível nos dispositivos permite maior segurança na transmissão, reduzindo as chances de alterações no conteúdo, como também bloqueia a leitura por pessoas não autorizadas. Para isso, usam-se algoritmos e chaves para impedir que dados sejam lidos por intrusos e para garantir a segurança da informação, o que é conhecido por criptografia.

Outras medidas, elencadas no documento publicado pelo CERT.br se referem a evitar colocar na nuvem arquivos confidenciais ou com dados privados, a criação de senhas fortes, a verificação em duas etapas ou multivariadas, a notificação de *login*, a instalação de aplicativos somente de fontes confiáveis, a atualização dos sistemas e aplicativos e evitar clicar em *links* via mensagens públicas. Contudo, ainda assim, a utilização da internet deixa rastros digitais que podem ser utilizados indevidamente. Então, deve-se reduzir a quantidade de dados pessoais na internet, sendo seletivo com quem se compartilha informações e ao preencher dados cadastrais. Para isso, deve-se usar sempre conexões seguras, configurar o modo de privacidade nos aplicativos e navegadores, limitar os dados de coleta por *cookies* e limpar sempre o histórico de navegação (CERT.br, NIC.br, CGI.br & ANPD, 2021).

Independentemente do dispositivo utilizado, a privacidade pode estar em risco porque, mesmo que existam restrições de acesso às informações em rede, não há como controlar para quem são transmitidas. Assim, as informações pessoais disponibilizadas na internet tornam-se alvo para a criação de identidades falsas usadas para atividades maliciosas e para propagandas direcionadas, além de colocar em risco a segurança física, causar problemas financeiros, de reputação e de crédito (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021).

Esse problema tem sido debatido na área das ciências humanas na tentativa de conhecer profundamente o tema e combater os cibercrimes. Sob a ótica do direito, Sales e Bonat (2022) afirmam que com o advento da tecnologia 5G, a velocidade da transmissão de dados tornou-se mais rápida. Entretanto, também, trouxe implicações de ameaças sistêmicas, tais como, a repressão digital, a vigilância em massa, o perfil do usuário aprimorado e microssegmentação, os riscos à privacidade e os *deepfakes* que se referem aos materiais de áudio e vídeo manipulados por meios digitais.

Agrega-se a esse fato que as redes sociais se tornaram a fonte de notícias preferida no Brasil, até mesmo em relação à TV, conforme o relatório *Reuters Digital News Report* da Universidade de Oxford de 2020. O brasileiro está conectado por dispositivos móveis com tecnologias 3G, 4G e 5G, mesmo em áreas mais remotas do país, sendo as informações disseminadas rapidamente. Mas, podendo gerar desinformação e desconfiança nos usuários, também (Sales & Bonat, 2022).

Enquanto para Zuboff (2020), sob um ponto de vista da área da administração, a sociedade digital está alienada em consequência de um capitalismo que o indivíduo se expõe voluntariamente na internet que se traduz em dados comportamentais que geram algoritmos que produz informações que podem ter alto valor nesse mercado de comportamento. Além disso, explica que essa tecnologia formata, monitora, controla e explora o indivíduo que sofre invasão de privacidade, mas que não está disposto a dar um "basta".

Tem-se um novo negócio que se utiliza das experiências humana como fonte de matéria-prima por meio de camuflagem de operações agressivas de extrações de dados capazes de minerar a privacidade do usuário nem sempre legais. Contudo, esse mercado, também, molda o comportamento para beneficiar resultados comerciais, influenciando e transformando o comportamento em escala seja por protocolos do Facebook ou em jogos como o Pokemón Go da Google, entre outros (Zuboff, 2020).

Portanto, a expansão do espaço cibernético tem como consequência o crescimento dos cibercrimes. Assim, a proteção cibernética torna-se imperiosa como medida de segurança da informação dos dados governamentais e privados. Pois, esse é um problema do governo, das organizações e dos indivíduos, uma vez que envolve toda a sociedade para a adoção desses comportamentos seguros citados anteriormente como prática diária.

1.1 Problemática de pesquisa

O ciberespaço tem deixado evidentes as vulnerabilidades nos serviços e nas operações desse mercado tecnológico devido à falta de segurança cibernética (Vidigal, 2004). Entende-se que se trata de um problema complexo e multifacetado em diferentes níveis do sistema, desde o individual ao macroeconômico que se perpetua no tempo. Neste contexto, reside a motivação da pesquisa, pois o desenvolvimento mundial vem acontecendo por meio das revoluções industrial, tecnológica e do conhecimento.

Os ataques cibernéticos vêm mostrando essas vulnerabilidades às quais os indivíduos, a sociedade e o governo estão expostos. Foram cerca de 41 bilhões de tentativas desse tipo de

ataque na América Latina e Caribe, sendo 8,4 bilhões direcionados ao Brasil, em 2020 (Fortinet, 2021). Os cibercriminosos utilizam as ferramentas tecnológicas disponíveis para obterem êxito no roubo de senhas e dados na invasão de contas pessoais, empresariais e governamentais.

Esse tipo de problema, para o qual a solução é complexa e exige uma dinâmica conjunta entre diversos entes sociais, pode receber contribuições relevantes no âmbito da discussão empreendida a partir da abordagem do marketing macrossocial. Essa abordagem extrapola os parâmetros do marketing convencional, que se preocupa com questões estritamente comerciais (Levy, 1978). A abordagem do marketing macrossocial compreende uma ampliação da perspectiva conhecida como social, sem o intuito da venda de produtos ou marcas e suas ações objetivam a transformação de valores, atitudes e comportamentos (Kotler & Lee, 2011).

O marketing macrossocial busca a partir de uma perspectiva que objetiva melhorar o bem-estar social, seja implementando-se ou identificando-se a possibilidade de intervenções em diversos níveis sociais (Nguyen, Brennan & Parker, 2014; Kennedy, 2016). Enquanto o marketing social envolve-se com questões da saúde, do meio ambiente, do lazer ou outras questões que podem ampliar o bem-estar social, objetivando a conscientização social para criar um comportamento capaz de promover melhorias na sociedade (Leonardo Rezende, Sousa, Pereira, Liliane Rezende, 2015; J. Pereira, Sousa, Matos, Rezende, Bueno, & Dias, 2016; Sousa, Pereira, Lousanne Resende & Leonardo Rezende, 2017; J. Pereira, Sousa, Shigaki & Lara, 2018).

Em relação às ações do marketing social, essas são promovidas pelos governos e Organizações não governamentais sem fins lucrativos (ONG), tais como no combate ao álcool e ao uso de drogas (Duailibi, Pinsky & Laranjeira, 2007), nas campanhas de incentivo à doação de sangue (J. Pereira, Sousa, Matos, Rezende, Bueno & Dias, 2016) e de prevenção do Vírus da Imunodeficiência Humana (HIV) (Wei, Herrick, Raymond, Anglemyer, Gerbase & Noar, 2011; Buyucek, Kubacki, Rundle-Thiele & Pang, 2016; Batista, 2018), entre outras.

Contudo, Kennedy e Parsons (2012) afirmam que para disseminar a conscientização de problemas sociais complexos é necessária a execução de intervenções nos diversos níveis da sociedade. Isso é explicado por se tratar de uma questão cultural e de estrutura de um país, nos quais esses problemas tornam-se precipitantes para que a sociedade esteja suscetível às mudanças desejadas em nível macro.

Desse modo, pode-se influenciar e modificar comportamentos que beneficiam os três níveis sociais: *downstream* (individual), *midstream* (grupos de referências) e *upstream* (atividades políticas e governamentais) (Dibb, 2014). Essa influência de um nível social sobre

outro pode contribuir na adoção de comportamentos digitalmente seguros pelos usuários.

No nível *downstream* é possível a adoção de medidas para o indivíduo se proteger no comércio eletrônico, no *internet banking*, nas redes sociais e nos dispositivos móveis. Enquanto no nível *midstream*, as escolas, as agências do setor público, as organizações sem fins lucrativos e as fundações desempenham papel importante na segurança da rede de computadores mediante ações educativas e de treinamentos. Além disso, no nível *upstream*, tem-se a desenvoltura da elaboração da estrutura regulatória necessária para o funcionamento das organizações e da cadeia mercadológica da área, assim como melhorar a prestação de serviço ao público (Dibb, 2014).

Assim, a abordagem macrossocial é desenvolvida no sistema social, avaliando-se as prováveis barreiras e os agentes facilitadores (Nguyen, Brennan & Parker, 2014; Kennedy, 2016). O marketing macrossocial trata-se de uma perspectiva de marketing adequada para promover mudanças sistêmicas, como a adoção de hábitos saudáveis e o combate a comportamentos prejudiciais. Essa persperctiva do marketing macrossocial é baseada na influência de um nível social sobre outro, tal como, pode ser desenvolvida no nível *upstream* por meio de políticas públicas.

Alves e Barbosa (2019) mostram no estudo sobre o processo da literacia da saúde da mulher à luz do marketing social no interior do nordeste brasileiro que os problemas relacionados a comunicação entre os três níveis impediu que opiniões e necessidades dos níveis *downstream* e *midstream* chegassem ao nível *upstream*, também, a baixa a participação nas campanhas por falta de divulgação. Esse estudo constata que a adoção de uma comunicação mais eficaz entre os níveis *downstream* e *midstream* podem contribuir para que o nível *upstream* produza ações para atender os problemas e as necessidades daquelas pessoas, evidenciando um dano na influência entre os níveis que poderá ser corrigido diante da ciência desses resultados.

Em se tratando de políticas públicas, a evolução da segurança pública tem acompanhado os fatores desencadeantes da criminalidade no decorrer do tempo. Medidas adotadas para conter os crimes decorrentes de fatores da motivação criminal e da ocasião referem-se ao emprego de tratamentos médicos e psiquiátricos, as reformas sociais, ao planeamento urbano, a iluminação pública, as câmaras de videovigilância, entre outras.

Entretanto, com o avanço da criminalidade torna-se necessário a utilização de instrumentos de Políticas Públicas de segurança, sejam voluntários, combinados ou compulsórios. Os instrumentos voluntários dizem a respeito da família e comunidade, das organizações voluntárias e dos mercados privados. Os instrumentos combinados estão

relacionados à informação e sensibilização, aos subsídios, aos impostos e taxas de utilização. Enquanto os instrumentos compulsórios trata-se da regulação, das empresas do setor público e do provisionamento direto (Santos, 2018).

No que concerne ao cibercrime, medidas de prevenção, de resposta e de aprendizagem são relevantes na mitigação em segurança de sistemas de informação. Quanto às medidas de prevenção do risco, há a preocupação em diminuir a frequência e/ou a magnitude dos ataques. Para isso, emprega-se a segurança física e *environmental; firewalls*; ferramentas de antivírus; autenticação e controle de acessos por meio da biometria, de senhas e de *tokens*, etc.; a encriptação por certificação digital, redes privadas virtuais conhecidas por *Virtual Private Network* (VPN) e *Wireless Application Protocols* (WAP); e *Intrusion Detection and Prevention System* (IDS/IPS) (Santos, 2018).

As medidas de resposta relacionam-se ao controle do risco por meio de ações planejadas capazes de facilitar as respostas, diminuindo a frequência e/ou magnitude das perdas. Assim, são utilizados Processos de *Disaster* Recovery responsáveis em recuperar o sistema e manter o funcionamento diante de falhas; *Sistemas fail-over* capazes atuam por meio de um componente secundário tais como um *hardware* redundante ou *software* redundante; e *backups* frequentes (Santos, 2018).

As medidas de aprendizagem são ações de avaliação do risco que propiciam a aprender sobre a frequência e/ou magnitude das perdas. Nesse sentido, usam-se Sistemas IDS configurados com base em dados estatísticos, aprendizagem bayesiana com dados de amostras pós-auditorias, análise/auditorias de logs, scans/auditorias de Sistema, auditorias de sistema e análise de vulnerabilidades, exercícios de ataque e penetrações ao sistema (Santos, 2018).

Para Camargo (2023), a influência do nível *midstream* sobre seus funcionários e seus clientes na utilização de soluções *Private Acess* fundamentada em tecnologia *Zero Trust Network Acess* (ZTNA) traz a inovação e o diferencial na privacidade dos dados, uma vez que os dados empresariais migraram para o ambiente *cloud*, ou seja, os negócios das empresas estão literalmente nas nuvens, requerendo um nível de proteção redobrada.

Conforme Camargo (2023), a tecnologia ZTNA é um avanço da VPN, pois, impede que pessoas não autorizadas acessem a rede da empresa e o cliente entra apenas em aplicações necessárias e permitidas após validação a cada acesso. Essa adoção da ZTNA nas empresas garantem a segurança dos dados corporativos. A análise dessas ações governamentais por meio de políticas públicas e empresariais permitem verificar como essas influenciam a adoção de comportamentos virtuais seguros, mostrando a complexidade envolvida na promoção da cibersegurança e contribuindo para a elaboração de estratégias eficazes para prevenção do

cibercrime.

Diante das considerações apresentadas emerge a seguinte questão de pesquisa: **Como os indivíduos que acessam regularmente a internet percebem a influência dos três níveis do marketing macrossocial na adoção de comportamentos digitalmente seguros?**

1.2 Hipóteses e modelo hipotético

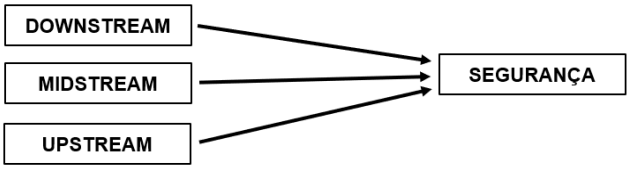
As hipóteses utilizadas nesta dissertação para verificar como os indivíduos que acessam regularmente a internet percebem a influência dos três níveis do marketing macrossocial na adoção de comportamentos digitalmente seguros foram:

a) As ações do nível *downstream* influenciam a adoção de comportamentos seguros no ambiente virtual.
b) As ações do nível *midstream* influenciam a adoção de comportamentos seguros no ambiente virtual.
c) As ações do nível *upstream* influenciam a adoção de comportamentos seguros no ambiente virtual.

O modelo empregado está apresentado na Figura 1.

Figura 1

Modelo hipotético



Fonte: Elaborado pela autora (2023).

A seguir são apresentados os objetivos da pesquisa.

1.3 Objetivos

A fim de responder o problema de pesquisa, foram traçados os seguintes objetivos:

1.3.1 Objetivo geral

Identificar como os indivíduos que acessam regularmente a internet percebem a influência dos três níveis do marketing macrossocial na adoção de comportamentos digitalmente seguros.

1.3.2 Objetivos específicos

Para alcançar o objetivo geral, delineou-se os seguintes objetivos específicos:

a) Identificar se as ações do nível *downstream* influenciam a adoção de comportamentos seguros no ambiente virtual.
b) Identificar se as ações do nível *midstream* influenciam a adoção de comportamentos seguros no ambiente virtual.
c) Identificar se as ações do nível *upstream* influenciam a adoção de comportamentos seguros no ambiente virtual.
d) Propor e testar um modelo analítico que avalie como os indivíduos que acessam regularmente a internet percebem a influência dos três níveis do marketing macrossocial em prol de comportamentos digitalmente seguros.

1.4 Justificativa

Os argumentos mercadológicos, acadêmicos e sociais são suficientes para se incentivar pesquisas tais como esta proposta sobre a influência dos três níveis do marketing macrossocial na adoção de comportamentos seguros na internet. A justificativa mercadológica fundamenta-se no crescente aumento de ciberataques no Brasil e no mundo. A proteção aos dados é necessária para amenizar a vulnerabilidade empresarial e governamental. Investimentos na gestão de senhas e autenticação, controle de acesso aos dados armazenados, seleção correta de privilégios dos usuários, regras e análise auditorias de governança têm-se que se tornarem rotinas nas empresas e no governo.

Manter os sistemas atualizados é essencial na integralização desses recursos. A conformidade com as normas regulatórias na proteção dos dados também é importante. Igualmente, as empresas devem se lembrar das ameaças internas de funcionários descontentes ou mal-intencionados.

O risco que as empresas correm por serem detentoras de tantos dados pessoais de seus

clientes tornou-se uma atração lucrativa para criminosos. O vazamento de dados é real, os cibercriminosos estão cada dia mais testando seu poder de penetração nas redes das grandes empresas e do governo. Esses ataques ameaçam a credibilidade e a confiança dos usuários. Além disso, o custo para ressarcir a utilização indevida dos dados é uma despesa alta. Assim, treinamentos internos e divulgação de campanhas podem ser uma maneira de amenizar esse problema.

Do ponto de vista acadêmico, esta pesquisa se justifica devido à proposta de analisar as influências dos três níveis do marketing macrossocial na adoção de comportamento digital ainda serem pouco estudadas. O levantamento das publicações sobre a temática foi realizado por meio da busca ativa nas bases de dados *Scientific Eletronic Library Online* (Scielo), Associação Nacional de Pós-Graduação e Pesquisa em Administração (Anpad), *Scientific Periodicals Eletronic Library* (Spell), *Web of Science* e Coordenação de Aperfeiçoamento de Pessoal e de Nível Superior (Capes). Utilizou-se como descritores: marketing macrossocial, marketing social, macromarketing, cibercrime e cibersegurança em português e inglês. Como se trata de um tema pouco explorado, não se restringiu a seleção quanto ao ano de publicação ou ao idioma.

Em se tratando de cada um dos descritores em língua portuguesa, apuraram-se os seguintes resultados quantitativos: 6 pesquisas sobre marketing macrossocial, 241 pesquisas sobre marketing social, 0 pesquisas sobre macromarketing, 41 pesquisas sobre cibercrimes e 52 pesquisas sobre cibersegurança.

Em se tratando de cada um dos descritores em língua inglesa, retornaram-se os seguintes resultados quantitativos: 36.060 pesquisas sobre *macro-social marketing*, 799.400 pesquisas sobre social *marketing*, 4.472 pesquisas sobre *macromarketing,* 66.873 pesquisas sobre *cybercrime* e 60.122 pesquisas sobre *cybersecurity*.

Os aspectos quantitativos desse levantamento bibliográfico estão apresentados na Tabela 1.

Tabela 1

Levantamento nas bases científicas

Descritores	Anpad	Journal Marketing	Spell	Scielo	Web of Science	Capes
Marketing Macrossocial *Macro-Social Marketing*	0 0	0 35.833	0 0	0 1	0 68	6 158
Marketing Macrossocial and Cibercrimes *Macro-Social Marketing and Cybercrime*	0 0	0 57	0 0	0 0	0 0	0 0
Marketing Macrossocial and Cibersegurança *Macro-social Marketing and Cybersecurity*	0 0	0 113	0 0	0 0	0 0	0 0
Cibercrime *Cybercrime*	0 1	0 1.165	0 0	0 49	0 652	41 65.006
Cibersegurança *Cybersecurity*	4 9	0 1.488	0 4	0 68	0 13.780	48 44.773
Macromarketing *Macromarketing*	0 17	0 1629	0 17	0 9	0 1.182	0 1.618
Macromarketing and Cibercrime *Macromarketing and Cybercrime*	0 0	0 0	0 0	0 0	0 0	0 0
Macromarketing and Cibersegurança *Macromarketing and Cybersecurity*	0 0	0 0	0 0	0 0	0 0	0 1
Marketing Social *Social Marketing*	0 976	0 348.719	0 976	0 805	0 175.849	241 272.075
Marketing Social and Cibercrime *Social Marketing and Cybercrime*	0 0	0 494	0 0	0 0	0 17	0 61
Marketing Social and Cibersegurança *Social Marketing and Cybersecurity*	0 0	0 712	0 0	0 0	0 108	1 160

Fonte: Elaborado pela autora (2023).

Espera-se que este estudo contribua com a teoria do marketing macrossocial ao explorar sobre uma temática diferente das publicadas, possibilitando ampliar o escopo de observação acerca do assunto e a aplicação das ações de marketing macrossocial capazes de colaborar na adoção de medidas de comportamentos digitalmente seguros.

Na esfera social, esta pesquisa justifica-se pela importância dada a esse problema social complexo que atinge globalmente a todos por se tratar de uma questão da segurança pública e nacional. Assim, o resultado da pesquisa pretende contribuir para os formuladores de políticas públicas, para os empresários e demais líderes/representantes da sociedade na divulgação de eventos capazes de promover o comportamento digital seguro, além de oferecer um ambiente de navegação digital de confiança aos usuários e incentivar a realização de denúncias dos cibercrimes.

Esta dissertação está estruturada em seis capítulos. No primeiro capítulo, tem-se a introdução à temática, a problematização, o objetivo geral e os objetivos específicos e a justificativa para a realização da pesquisa. No segundo capítulo, tem-se a contextualização do ambiente de estudo e o cenário dos crimes cibernéticos com subdivisões relativas à internet, à magnitude do cibercrime, à segurança de rede, às estruturas regulatórias, leis e atos. No terceiro capítulo apresenta-se o referencial teórico sobre o marketing social, o marketing macrossocial no contexto do mundo digital e as campanhas publicitárias de segurança da informação. O quarto capítulo traz a metodologia quanto ao tipo, à abordagem e ao método de pesquisa; à população e à amostra; ao método de coleta de dados e à técnica de análise de dados. No quinto capítulo, analisa-se e discute-se os resultados da pesquisa. No último capítulo, são apresentadas as considerações finais, as limitações do estudo e sugestões de novos estudos.

2 CIBERCRIMES: CONTEXTUALIZAÇÃO E CENÁRIO

Este capítulo apresenta o cenário da pesquisa, iniciando com o a discussão sobre a contextualização geral e evolução da internet, apresentando-se na sequência a magnitude do cibercrime, a segurança de rede e a estruturas regulatórias, leis e atos.

2.1 A internet: contextualização geral e evolução

O século XX sofreu uma revolução global com o advento da internet. Esse fato transformou a comunicação entre as pessoas e nas empresas, impactando diversas outras áreas. Além disso, foi o motor para o desenvolvimento de novas tecnologias (Cazelatto e Segatto, 2020).

No período de 1947 a 1991, houve o surgimento da internet por meio de pesquisas militares durante a Guerra Fria entre União Soviética e Estados Unidos que, para preservar informações sigilosas, criaram a rede *Advanced Research Projects Agency Network* (ARPAnet). A internet chegou ao Brasil, em 1988, por meio de estudantes e professores paulistanos e fluminenses. Também, ocorreu a conexão entre o Laboratório Nacional de Computação Científica do Ministério da Ciência, Tecnologia e Inovação e Comunicações com a Universidade Maryland para troca de mensagens, além da conexão ponto a ponto entre a Fundação Amparo à Pesquisa de São Paulo ao *Fermi National Acelerator Laboratory* em Chicago (Castells, 2003; M. Carvalho, 2006; TecMundo, 2018).

Em 1989, essa comunicação internacional se fortaleceu com a conexão da Universidade Federal do Rio de Janeiro com uma universidade americana e três criações marcantes foram instituídas nessa época. A primeira foi a Rede Nacional de Pesquisa para fornecimento de internet às instituições. A segunda foi o Instituto Brasileiro de Análises Sociais e Econômicas em parceria com o *Institute for Global Communications* dos Estados Unidos e outras agências criaram o Alternex para troca de mensagens e conferências eletrônicas. A terceira, foi o desenvolvimento do domínio .br para compra e para consumidores (Castells, 2003; TecMundo, 2018).

Em 1991, a internet era utilizada para transferência de arquivos e bases de dados por órgãos governamentais e instituições educacionais de pesquisa. Em 1992, implantou-se a primeira central da Rede Nacional de Pesquisa de internet interligando onze estados. Assim, tornou-se possível o primeiro evento com internet no país, a Eco 92 (Cavalcanti, 1997; M. Carvalho, 2006; NIC.br, 2014, 2022).

Em 1993, a BBS Canal Vip ofereceu conta de internet gratuita a qualquer pessoa pelo *Bullet Board System* via telefone para troca de arquivos, fóruns, chats e jogos para que a população pudesse degustar, ter ciência e realizar o marketing comercial futuro nessa área. A disputa comercial ganhou força quando, em 1995, a Embratel perdeu o monopólio do fornecimento de internet para os consumidores, apesar de continuar controlando os provedores que passaram a conceder acesso aos usuários. Nesse ano, também, outro evento importante de caráter regulador foi a criação do Comitê Gestor da Internet no Brasil (CGI.br) pela Portaria Interministerial nº147/95 (Cavalcanti, 1997; NIC.br, 2014, 2022).

Em 1996, surgem os primeiros portais privados de internet do Brasil, o Zaz e o Uol, e 851 domínios. Em 1997, acontece o início da informatização dos órgãos públicos, a permissão da entrega da declaração do imposto de renda pela internet e a divulgação dos resultados das eleições em tempo real pelo Tribunal Superior Eleitoral. Esses fatos mostram o enraizamento da tecnologia digital nas repartições públicas do país (TecMundo, 2018; NIC.br, 2014, 2022).

Em 2000, os consumidores também puderam apreciar novos provedores de internet com acesso gratuito e com conexão discada e com banda larga. A parte comercial prosperou, em 2004, com o aparecimento das redes sociais *Orkut* e *Google* e a primeira conexão móvel 3G pela Vivo. O comércio tecnológico ganhou ainda mais impulso, em 2007, com os primeiros *smartphones* e a implantação do sistema de televisão digital (TecMundo, 2018; NIC.br, 2014, 2022).

As estatísticas referentes às Tecnologias de informação e da comunicação (TICs) na Pesquisa Nacional de Amostra de Domicílios (PNAD) realizadas de 2012 a 2022 mostram o avanço da tecnologia e os movimentos de crescimento ou redução dentre os meios de comunicação. O acesso da população ao rádio, à televisão, ao telefone fixo e móvel, ao microcomputador e à internet no país requer do governo novas formulações de políticas de melhorias capazes de garantir o desenvolvimento econômico (IBGE, 2018, 2020, 2022).

A expansão das TICs trouxe eventos que estavam sem controle, sendo necessário regulamentá-la. Assim, em 2014, implantou-se o Marco Civil da Internet na tentativa de iniciar a organização do espaço cibernético. Em 2016, esse crescimento digital atingiu mais de 50% dos domicílios com internet e, em 2017, aumentou para 80% de domicílios conectados à internet pelo celular e 77% pelo computador. Outro importante acontecimento regulatório foi a proibição da limitação dos dados na internet fixa que não chegou a reprimir os provedores, pois, em 2021 houve o maior leilão do 5G que foi implantado em 2022 (Solagna, 2020).

A necessidade da organização das informações nas universidades e nos órgãos governamentais estimulou a criação dos bancos de dados com posterior demanda das redes

para compartilhamento. Entretanto, as possibilidades do uso da internet cresceram e a demanda comercial interligou os continentes (Canabarro, 2014; TecMundo, 2018; NIC.br, 2014, 2022). Assim, foi questão de tempo para que a internet chegasse aos cidadãos e estivesse presente nos domicílios que, de acordo com o *site Internet World Stats* (até julho de 2022) e o *site DataReportal* (2022), o número de usuários da internet era cerca de 67% a 69% da população mundial.

Essa expansão da internet repercutiu, também, na segurança dessas redes, expondo as vulnerabilidades dos usuários, das empresas e dos governos (Rainie, Kiesler, Kang & Madden, 2013; Olmstead & Smith, 2017; Safernet, 2023a). Assim, as denúncias permitem identificar a amplitude e o tipo de crime para se planejar estratégias de atuação. Portanto, o reconhecimento do problema é um primeiro passo na defesa do ciberespaço.

2.2 Magnitude do cibercrime

Segundo o *Internet Crime Report 2021* da *Federal Bureau of Investigation* (FBI, 2022), o número de denúncias e de perdas financeiras dos crimes cibernéticos e ataques maliciosos pela internet cresceram mais de 100% nos últimos cinco anos a nível mundial. S. Pereira (2022) corrobora com essa informação e afirma que no período da pandemia do Covid-19 houve um aumento descontrolado desses números. Esses dados revelam também o comprometimento da economia.

Esses crimes virtuais estão sendo combatidos por meio da parceria entre as organizações e órgãos governamentais de diversos países juntamente com empresas locais. Essa formação de redes de proteção mundial promove a união de esforços para garantir os direitos sociais. Entretanto, a participação da família, da escola e da comunidade, também, complementa essa proteção contra crimes praticados na web (Childhood, 2012, 2021; Areepattamannil & Khine, 2017).

Em relação aos cibercrimes mais praticados nos últimos cinco anos estão os crimes de extorsão, de roubo de identidade, de violação dos dados pessoais, de não-pagamento e não-

delivery, de ataques *phishing*[1], *vishing*[2], *smishing*[3] e *pharming*[4]. Entretanto, os crimes de extorsão, de não-pagamento e não-delivery decresceram enquanto os crimes de *phishing, vishing*, *smishing* e *pharming* aumentaram significantemente nos três últimos anos (FBI, 2022).

Quanto a essas ameaças, S. Pereira (2022) afirma que durante a pandemia covid-19 houve a proliferação de mensagens falsas em redes sociais e de ataques do tipo *phishing* que exploram a vulnerabilidade do internauta. Também, aponta que os números de cibercrimes são maiores que os apresentados pelos entes federais, pois, muitas vítimas não denunciam por não considerarem importante ou por não saberem que foram alvos ou por desacreditar na identificação e punição dos criminosos.

De acordo com o FBI (2022), os crimes virtuais ocorreram mais entre usuários a partir dos 20 anos, sendo que os idosos foram os que mais tiveram prejuízos. Também, a vulnerabilidade dos idosos com o uso da tecnologia se sustenta no fato que, para não serem excluídos da sociedade, acabam desprotegidos no espaço cibernético, pois, se vive em um mundo cada vez mais digital.

Os Estados Unidos e o Reino Unido foram os principais países de ocorrências dos crimes cibernéticos, em 2021. A explicação para tal fato reside que são países com grande poder econômico e cuja população tem forte presença digital. Assim, ataques cibernéticos são comuns como forma de identificação de vulnerabilidades, roubos de informações secretas e desestabilização econômica (FBI, 2022). S. Pereira (2022) acrescenta que os cibercrimes são facilmente aprendidos e interiorizados, não requer altos investimentos para praticá-los com um retorno positivo e não necessita estar no mesmo território fisicamente da vítima.

Além dos cincos mais praticados citados anteriormente, em 2021, teve em ordem crescente os crimes de fraude confidencial ou romance, de suporte técnico, de investimentos, de compromissos por *e-mail* comercial ou de conta de *e-mail*, de falsificação, de fraude de cartão de crédito, de emprego, outros, de terrorismo ou ameaça de violência, imobiliários ou aluguel, de simulação governamental, taxa antecipada, de pagamentos em excesso, de loteria ou sorteio ou herança, de direitos autorais ou falsificação, de *ransomware*[5], de crimes contra

[1] Ataque que tenta roubar o dinheiro ou a identidade do usuário por meio das informações pessoais reveladas pelo próprio usuário em falsos *sites* que o enganam como se fossem legítimos (CERT.br, NIC.br, CGI.br & ANPD, 2021).

[2] Golpes verbais que induzem o usuário a realizar ações que parecem ser do seu interesse, mas que terminam por roubar o dinheiro ou a identidade, ou seja, começa com *vishing* e finaliza com *phishing.* (CERT.br, NIC.br, CGI.br & ANPD, 2021).

[3] Combinação de *short message service* (SMS) e *phishing*, isto é, usa mensagens de texto para roubar o dinheiro ou a identidade do usuário (CERT.br, NIC.br, CGI.br & ANPD, 2021).

[4] Crime virtual em que o tráfego de um *site* é manipulado e informações confidenciais são roubadas (CERT.br, NIC.br, CGI.br & ANPD, 2021).

[5] *Software* malicioso que sequestra dados, bloqueando o computador do usuário para exigir resgate para

crianças, de violação dos dados pessoais, de matéria civil, de serviços de navegação, de intrusão de computadores, de *malware*[6] ou *scareware*[7] ou vírus, relacionados aos cuidados com a saúde, de reenvio e de jogos de azar (FBI, 2022). Isso demonstra como a sociedade está vulnerável e quão variadas são as possibilidades de ataques destes criminosos que estão sempre pensando em novos tipos de crimes cibernéticos.

Em se tratando dos prejuízos financeiros, as cinco maiores ocorrências de cibercrimes foram relacionadas a compromissos por *e-mail* comercial ou de conta de *e-mail*, investimentos, fraude confidencial ou romance, violação dos dados pessoais e imobiliários ou aluguel, em 2021. O fato é que o volume de dinheiro perdido ultrapassou os dez dígitos, mostrando o impacto nos diversos setores e na sociedade (FBI, 2022).

No entanto, é importante analisar a tendência desses tipos de crimes que vêm ocorrendo nos três últimos anos conforme apresentado pelo FBI (2022). Pois, desses 29 tipos de crimes identificados, 17 apresentaram redução em 2021, mas apenas em 3 tipos essa redução foi consecutiva, significando que essas estratégias de combate tiveram êxito. Contudo, serve de alerta para a necessidade de manutenção e redobrar a atuação frente ao cibercrime que tem ganhado cada vez mais espaço.

De acordo com S. Pereira (2022), a perspectiva do aumento do cibercrime é sustentada pela crescente conectividade da população. Esse fato está relacionado ao volume de dados trafegados na internet que chegará a 200 zettabytes até 2025, requerendo maiores investimentos em cibersegurança especializada para garantir proteção. Essa preocupação fundamenta-se ao constatar que o prejuízo financeiro relacionado à oito tipos de cibercrimes tiveram aumento considerável consecutivo nos três últimos anos (FBI, 2022). Assim, torna-se evidente a importância de ampliar os reforços através das parcerias e por meio da conscientização desse problema.

No Brasil, as estatísticas de cibercrimes também mostram números preocupantes. Segundo a Safernet Brasil (2023a), em 16 anos de atuação, o número de denúncias anônimas de crimes e violações contra os direitos humanos na internet superaram os seis dígitos. Essa organização levanta dados referentes aos números de páginas denunciadas, de páginas que foram removidas, de idiomas das páginas, números de domínios hospedados, números de IPs envolvidos, países e continentes envolvidos desde 2007 conforme apresentado na Tabela 2.

---

desbloqueá-lo (Kaspersky, 2023a).

[6] *Software* malicioso que infecta o computado do usuário (Kaspersky, 2023b).

[7] *Software* malicioso que lubridia o usuário por mensagens *pop-up*, induzindo a acessar sites com *malware* (Kaspersky, 2023c).

Tabela 2

Número de crimes e violações contra os direitos humanos na internet de 2007 a 2021

Ano	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	TOTAL
Nº denúncias	616.515	610.356	692.300	357.474	367.292	178.728	244.147	189.211	139.643	115.645	63.698	133.732	75.671	156.692	150.095	4.441.595
Nº páginas denunciadas	62.227	89.247	80.848	71.720	73.348	55.288	54.221	58.717	43.070	39.440	32.936	49.302	39.864	74.011	71.095	935.496
Nº páginas removidas	61.411	88.140	78.577	67.107	66.803	46.993	39.858	37.445	27.874	25.639	20.503	25.777	24.319	43.316	32.538	725.664
Idiomas das páginas	8	9	8	8	9	9	9	8	8	9	9	9	9	10	10	10
Nº domínios hospedados	2.979	4.292	6.865	10.577	9.918	8.113	7.802	7.655	6.890	7.309	7.019	7.358	8.015	9.236	8.926	86.098
Nº IPS envolvidos	1.564	2.384	3.846	5.291	7.260	6.553	6.796	6.427	4.821	4.230	6.011	7.375	7.258	8.524	9.900	89.473
Países envolvidos	42	54	6	67	73	70	69	63	63	61	66	69	65	63	68	108
Continentes envolvidos	5	4	5	5	5	5	5	5	5	5	5	6	6	6	6	6

Fonte: Safernet Brasil (2023a). Dados compilados pela autora (2023).

Verifica-se na Tabela 2 que o número de denúncias anônimas era alto no período de 2007 a 2009, tendo ocorrido uma redução a partir de 2012. Esse fato está relacionado à repercussão de pesquisadores na área da computação e do direito desenvolverem pesquisas e projetos sociais no combate à pornografia infantil no período inicial da internet no Brasil. Nessa época, havia falta de uma política capaz de atacar a prática de crimes e violações dos direitos humanos na internet que pudesse responder de modo eficiente. Assim, a articulação da Safernet Brasil com atores da sociedade civil, da indústria de internet e de instituições governamentais, tais como o Ministério Público Federal (MPF), Congresso Nacional, autoridades policiais foi fundamental para a sua consolidação como referência nacional e internacional, além de amenizar esse problema que retornou fortemente em 2020 com a pandemia Covid-19 (Safernet Brasil, 2023a).

Neste sentido, a Safernet Brasil criou um Observatório legislativo para acompanhar as atividades do Congresso Nacional nas discussões relacionadas à cibercrimes, liberdade de expressão e opinião e o direito à privacidade na internet. Essa tornou-se uma ferramenta de interação do cidadão com o Senado Federal e a Câmara dos Deputados. Assim, foi possível a aprovação em audiência pública 13/11/2008 do Projeto de Lei sobre Crimes Cibernéticos (Lei 89/2003) em forma da Lei 12.735 transformada em norma jurídica (Safernet Brasil, 2023b).

Outra parceria da Safernet Brasil importante trata-se da Petrobras. Essa parceria resultou em duas principais ações. A primeira foi a integração da Central Nacional de Denúncias com o Disque 100 da Secretaria Especial de Direitos Humanos do Governo Federal. A segunda foi o termo de cooperação oficial com o Departamento da Polícia Federal. Essas ações objetivavam o combate à pornografia infantil e à pedofilia pela internet (Safernet Brasil, 2023c).

De acordo com Clevenger, Navarro, Marcum & Higgins (2018) e Halder (2022), os criminosos procuram as suas vítimas conforme características de vulnerabilidades, tais como os idosos, jovens e crianças. Assim, existe uma relevância em se manter informado sobre o cibercrime quanto ao fenômeno, aos riscos, às vulnerabilidades, como agem esses criminosos e o perfil das vítimas que se tratando de jovens e crianças, os pais devem educar e proteger seus filhos.

Pensando nessas crianças e jovens, a Safernet Brasil fez parceria com o *Google* Brasil, permitindo o monitoramento e a triagem das denúncias de pornografia infantil no *Orkut*. Dessa forma, passou a ser possível elaborar notícias-crimes e relatórios técnicos de rastreamento que são encaminhados ao MPF para quebra de sigilo por via judicial. Enfim, essas parcerias colaboraram para revelar o panorama do cibercrime no Brasil, assim como para potencializar

as ações legais contra esse problema (Safernet Brasil, 2023d).

A Tabela 3 apresenta a tipificação dos crimes e violações contra os direitos humanos na internet de 2007 a 2021. Constata-se que os crimes da pornografia infantil, da apologia e incitação a crimes contra a vida e do racismo tiveram maiores números de denúncias anônimas, enquanto os crimes de tráfico de pessoas e de violência ou discriminação contra a mulher tiveram menores números de denúncias anônimas. Além disso, verifica-se esta ocorrência em diversos idiomas e em todos os continentes, mostrando tratar-se de um problema global. Também, o número de páginas removidas representa cerca de 80% das páginas denunciadas, mostrando a atuação severa da justiça (Safernet Brasil, 2023a).

Tabela 3

Tipos de crimes e violações contra os direitos humanos na internet de 2007 a 2021

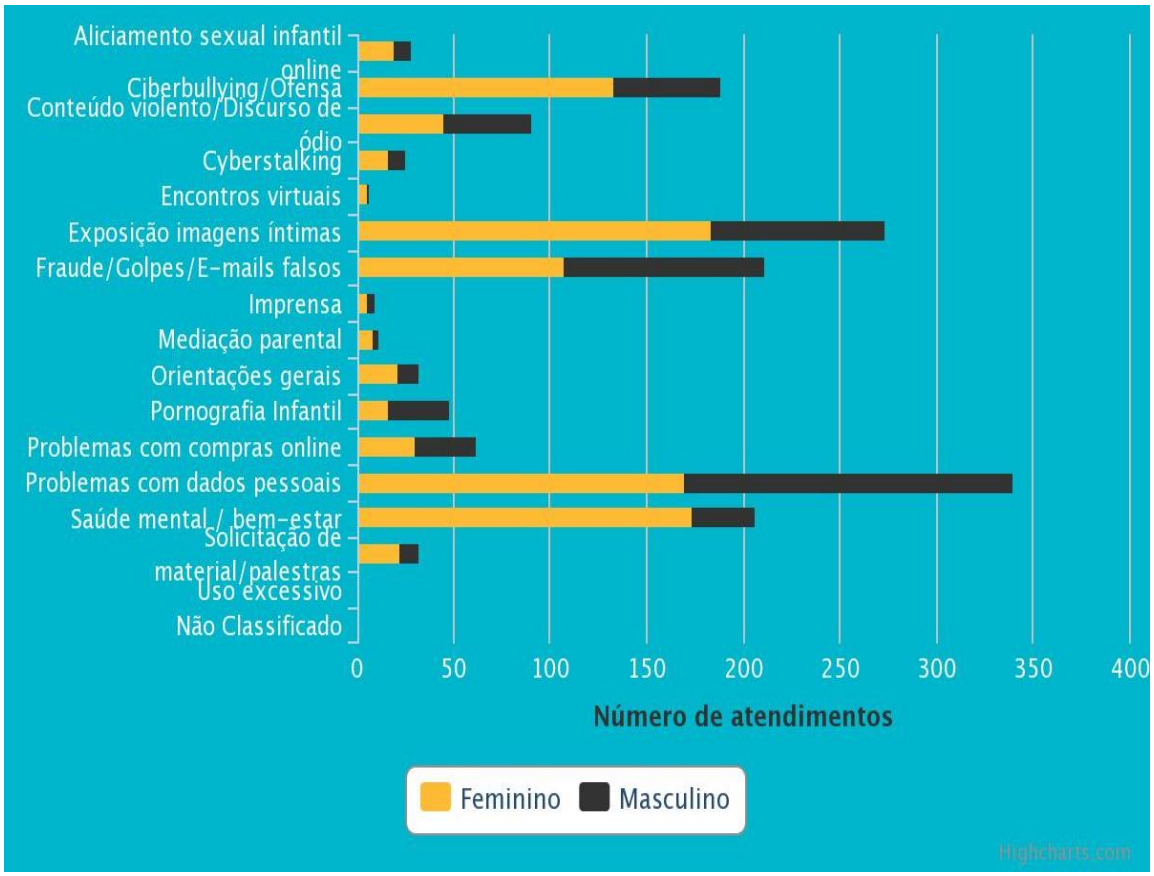
Tipificação	Maus-tratos contra animais	LGBT Fobia	Neo Nazismo	Pornografia infantil	Intolerância religiosa	Xenofobia	Racismo	Violência ou discriminação contra a mulher	Tráfico de pessoas	Apologia e incitação a crimes contra a vida	TOTAL
Nº denúncias	276.492	154.872	264.003	1.861.187	272.564	164.153	596.866	45.662	15.403	757.554	4.441.595
Nº páginas denunciadas	25.195	39.373	30.215	483.625	23.034	43.172	109.231	17.593	6.473	139.248	935.496
Nº páginas removidas	20.874	29;193	25.120	388.398	18.500	29.514	67.644	11.202	4.535	113.116	725.664
Idiomas das páginas	8	8	8	10	9	9	8	8	9	9	10
Nº domínios hospedados	1.826	2.052	1.325	64.542	1.883	1.453	6.886	2.033	1.997	9.712	86.098
Nº IPS envolvidos	3.929	4.807	2.781	72.582	3.393	3.350	13.839	3.946	2.914	14.801	89.473
Países envolvidos	47	44	40	104	36	42	63	37	51	70	108
Continentes envolvidos	5	5	5	6	5	5	5	6	5	5	6

Fonte: Safernet Brasil (2023a). Dados compilado pela autora (2023).

Outra importante análise refere-se ao número de denúncias em 2021 da população feminina ser maior que ao da população masculina conforme a Figura 2. Enquanto o número de denúncias relacionadas aos crimes com dados pessoais e fraudes, golpes, *e-mails* falsos são balanceados entre os dois sexos (Safernet Brasil, 2023a).

Figura 2

Número de denúncias por tópico em 2021

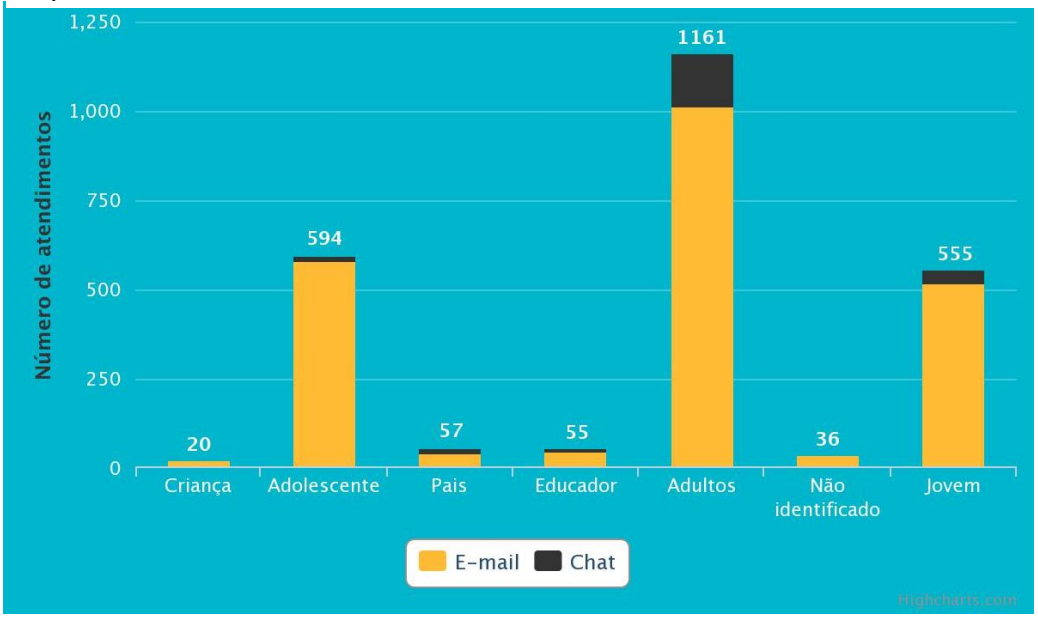


Fonte: Safernet Brasil (2023a)

Em relação ao perfil etário dos denunciantes, é maior entre a população adulta, mas a criança, o adolescente e o jovem também denunciam, de acordo com a Figura 3. Esse fato demonstra como os canais de atendimento por *e-mail* e *chat* desempenham uma alternativa para esses grupos. Além disso, o *e-mail* destacou-se como canal de atendimento preferencial (Safernet Brasil, 2023a).

Figura 3

Perfil etário dos denunciantes em 2021



Fonte: Safernet Brasil (2023a).

Quanto aos principais tipos de crimes e violações contra os direitos humanos na internet em 2021, conforme a Figura 4, os problemas com dados pessoais; a exposição de imagens íntimas; as fraudes, golpes, *e-mails* falsos; a saúde mental e bem-estar; *cyberbulling* e ofensa foram denunciados. Esses crimes mostram o impacto social provocado pela pandemia Covid-19 (Safernet Brasil, 2023a).

Figura 4

Principais tipos de crimes e violações contra os direitos na internet em 2021

Fonte: Safernet Brasil (2023a).

Portanto, volta-se a atenção para a segurança no ciberespaço que, segundo Gibson (1984), é onde acontece a articulação da informação de modo virtual por meio de uma rede de computadores.

2.3 Segurança de rede

O aumento do uso da internet e da rede de computadores tem exigido nova arquitetura de segurança de rede para proteção dos ativos, o que gera valor para as organizações corporativas e do sistema de informação contra ameaças ou atividades que possam interromper, danificar, explorar ou restringir o acesso à rede. Por isso, a implementação de uma medida isolada não garante a proteção, sendo necessária uma adoção abrangente da rede capaz de prever, proteger, monitorar, analisar, detectar e responder diante da identificação de intrusos (Garfinkel, 1997).

A segurança da rede é fundamental contra ameaças, sendo necessária a adoção de medidas preventivas. Deve ser instituída no ambiente organizacional, ampliando a segurança da rede por meio de elementos direcionados. Assim, segundo Azevedo (2010), cinco princípios auxiliam na identificação de vulnerabilidades na rede de computadores:

a) confidencialidade: somente usuários autorizados podem acessar, usar ou copiar informações dentro da organização mediante autenticação;
b) integridade: a informação não pode ser modificada, excluída ou corrompida sem autorização por meio da autenticação;
c) disponibilidade: proteção dos sistemas de informação ou redes de dados sensíveis são disponibilizados quando solicitados pelos usuários;
d) não-repúdio: serviço de validação da integridade de uma assinatura digital transmitida do ponto de origem ao seu destino e
e) autenticação: uso de credenciais cadastradas para obter acesso aos recursos organizacionais por intervenção de um servidor de autenticação.

Sistemas de arquivos, dados e informações sensíveis devem ser protegidos independentemente do tamanho da organização. Além disso, a segurança de rede traz benefícios como o aumento de lucros, a produtividade aprimorada, a conformidade aprimorada e a confiança dos clientes. Entretanto, os desafios na segurança de rede devem ser tratados, pois as ameaças evoluem e se modificam diariamente e a falta de habilidades de segurança de

rede compromete a defesa contra ataques. Deve-se considerar, nesse aspecto, que os ambientes se tornam evolutivamente mais complexos, o que amplia, em contrapartida, as dificuldades em se proporcionar um ambiente seguro (EC-*Council*, 2021).

Desse modo, são utilizadas técnicas de defesa de segurança da rede com abordagem preventiva, reativa, retrospectiva e proativa. A primeira previne ataques mediante mecanismos de controle de acesso, tais como os *firewalles*[8]. Além dos mecanismos de controle de admissão, tais como *Implement a network access control* (NAC) e *Network access protection* (NAP). Também, compreende os aplicativos criptográficos, tais como *Internet Protocol Security* (IPSec) e *Secure Sockets Layer* (SSL), assim como as técnicas biométricas, tais como a fala, digital e reconhecimento facial. A segunda refere-se ao monitoramento de segurança, como *Intrusion Detection and Prevention System* (IDS/IPS), SIMS e TRS, em caso de falha da primeira. A terceira corresponde aos mecanismos de detecção de falhas, técnicas forenses de segurança e mecanismos de análise *post-mortem*, isto é, pós-morte ou após o ocorrido. Por último, incluem-se medidas de avaliação de riscos futuros e inteligência de ameaças (EC-*Council*, 2021).

O controle da segurança de rede pode permitir ou impedir o acesso aos recursos organizacionais de acordo com o gerenciamento da identidade. Assim, os controles de segurança administrativos garantem a autorização e a autenticação de todos os níveis organizacionais, segurando a proteção da rede. Isso inclui a conformidade da estrutura regulatória, política de segurança, monitoramento de funcionários, classificação das informações, separação de deveres, princípio dos privilégios mínimos, conscientização e treinamento de segurança (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021).

Além disso, controles de segurança física diminuem a probabilidade de ataques e riscos dentro da organização. Assim, esses controles de segurança física podem ser preventivos, de dissuasão e de detecção, enquanto os controles de segurança técnica restringem o acesso aos recursos da organização que incluem o controle de acesso ao sistema e à rede, a autenticação e a autorização, a criptografia e os protocolos, os dispositivos de segurança de rede e a auditoria (EC-*Council*, 2021).

Neste contexto, os protocolos de segurança de rede garantem a integridade dos dados que trafegam na rede de uma organização. Entre os protocolos tem-se o *Remote Access Dial-In User Service* (RADIUS), o *Terminal Access Controller Access Control System Plus*

[8] Segundo a CISCO (2022), trata-se de um dispositivo de segurança da rede destinado ao monitoramento do tráfego de rede de entrada e saída, permitindo ou bloqueando determinados tráfegos conforme as regras de segurança.

(TACACS+), o *Kerberos*, o *Pretty Good Privacy* (PGP), S/MIME, o *HyperText Transfer Protocol Secure* (HTTPS), o *Transport Layer Security* (TLS), o SSL e o IPSec. O controle de acesso e a utilização de técnicas criptográficas promovem a segurança das mensagens na rede. Assim, a proteção da rede de computadores depende dos dispositivos ativos, passivos e preventivos existentes (EC-*Council*, 2021).

2.4 Estruturas regulatórias, leis e atos

As estruturas regulatórias, leis e atos desenvolvidos visam melhorar a proteção e aprimorar os processos, propiciando melhores práticas organizacionais. Desta forma, o atendimento à conformidade regulatória evita que dados organizacionais sejam violados. Portanto, a cibersegurança deve ser implementada por meio de procedimentos, práticas, diretrizes, padrões, políticas e estruturas regulatórias Senac (2021).

Além disso, a organização que cumpre os requisitos de conformidade com a estrutura regulatória tem vantagens sobre seus concorrentes, pois tem melhoria na segurança cibernética ao atender os requisitos básicos. Ainda, as perdas são minimizadas, uma vez que os dados não são violados, há redução de custos de reparo, multas e despesas advocatícias. Assim, a confiança aumenta com a crença que as informações estão seguras e o maior controle inibe erros, acessos não autorizados, ou danos aos dados (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021; Senac, 2021).

Neste sentido, o primeiro passo é a realização de uma autoavaliação organizacional com a finalidade de determinar os melhores marcos regulatórios que se adequam ao perfil corporativo que considera o tamanho, sua complexidade, crimes cibernéticos e ameaças. Em seguida, deve-se analisar e interpretar as informações coletadas. O próximo passo consiste em identificar as inconformidades para poder determinar como regularizar e quais riscos possíveis de violações. Para isso, classifica-se a ordem dos requisitos de conformidades como importantes e centrais e importantes, mas incidental. Depois, estabelecem-se as políticas, procedimentos e controles de segurança adequados (Senac, 2021).

Diante disso, é importante abordar mais sobre a política de segurança da informação a princípio com base na Norma ISO e ABNT.

2.4.1 Normas ISO e ABNT

A área da TI das organizações segue normas internacionais que ampliam a segurança

da informação, pois atestam o tratamento da informação e asseguram uma conexão com novos mercados e certificações. Para isso, a *Internacional Organization for Standardization* (ISO), organização que possui 167 países membros, compartilha conhecimento, desenvolve e publica normas acordadas internacionalmente por especialistas. Assim, são definidos padrões que descrevem a melhor maneira de se fazer algo de relevante para o mercado, ou que forneça soluções para desafios globais. No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) é o membro representativo do país na ISO. Por isso, as normas brasileiras (NBR) são as recomendações de padrão ouro para as organizações nacionais (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021).

De acordo com Senac (2021), entre as principais normativas publicadas para a segurança da informação têm-se a ISO/IEC 27.001 e a ISO/IEC 27.002 que foram revisadas e adequadas pela ABNT como as normas - NBR ISO 27001:2006 e NBR ISO 27002:2007. A primeira trata de atividades para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) com finalidade de certificação e reconhecimento internacional, sendo necessário:

a) criação de um plano de tratamento de riscos;
b) alocação de recursos;
c) seleção e implementação de controles de segurança;
d) treinamento e educação;
e) gerenciamento das operações;
f) gerenciamento dos recursos e
g) gerenciamento dos incidentes de segurança.

A NBR ISO 27002:2007 fornece suporte a definição de controles organizacionais, reunindo um conjunto de boas práticas para gerenciamento de ativos, gerenciamento de operações e gerenciamento de continuidade do negócio. Assim, cada organização deve selecionar quais controles são melhores para seu negócio. Entretanto, apesar de não serem obrigatórios, esses irão garantir as certificações para novos mercados, sendo, pois, uma decisão estratégica para a organização na proteção do sistema de informação (Senac, 2021).

Desse modo, as políticas de segurança ultrapassam as fronteiras das empresas, rompendo-se fronteiras no mundo. Pois, os países estão hiperconectados, sendo necessário o estabelecimento de suas regras e seus limites no espaço cibernético.

2.4.2 Políticas de segurança

Segundo Barbosa, Silva, Oliveira, Jesus e Miranda (2021), a lei do ciberespaço compreende regulamentações que abrangem a segurança na internet e outros dispositivos de comunicação *online*. Assim, o acesso e o uso da internet, a privacidade e a confidencialidade das informações organizacionais, sejam governamentais ou privadas, estão sob esta proteção legal.

Além disso, cada país tem suas regulamentações da internet, conforme o Quadro 1, que mostra uma preocupação crescente com a proteção dos dados, pois, no decorrer do tempo os países precisaram criar novas legislações para se adequar aos novos avanços. Foi representada no Quadro 1 a jurisdição do ciberespaço de 14 países. Verifica-se que a preocupação em estabelecer uma regulamentação não é recente, mas a criação de legislações se ampliou nos últimos anos em alguns países com a evolução da internet EC-*Council* (2021).

Essa regulamentação em gestão dos dados existia, mas ganhou força com os acontecimentos do caso de *Cambridge Analytica* quanto às eleições dos Estados Unidos com a coleta de informações de forma errada nas redes sociais do *Facebook*, do *Likedin* e do *Instagram*. No Brasil, foram criadas novas leis cibernéticas em acordo com a política internacional, para garantir o mercado econômico mundial e não incorrer em violações que possam gerar penalidades conforme exige o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021).

Dessa forma, pretende-se estabelecer segurança jurídica efetiva à proteção de dados pessoais na transferência internacional de dados. Também, o Cadastro Positivo, que é um histórico do comportamento de crédito do consumidor, e a intenção da entrada na Organização de Cooperação de Desenvolvimento Econômico (OCDE) colaboraram para os avanços na segurança dos dados para se equiparar e negociar com empresas internacionais (Perroti, 2022).

As regulamentações empregadas nos cibercrimes no Brasil evoluíram com os acontecimentos. O Código Penal vigente foi criado em 1940, e vem sendo usado, pois alguns dos cibercrimes correspondem a crimes que estão inclusos nessa legislação e passaram a ser aplicados no meio digital, tais como o estelionato e a pedofilia. Também, a Constituição Federal presente desde 1988, em seu artigo 5º, garante que são invioláveis, a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente da violação. (Spiri, 2020; Perroti, 2022).

Quadro 1

Diversas leis cibernéticas em diferentes países

Países			
Austrália	**Brasil**	**Singapura**	**Hong Kong**
Lei de Direitos Autorais de 1968	Código penal	Lei de uso indevido de computador	Art. 139 Lei Fundamental
Lei de Patentes de 1990	Constituição Federal	**Coreia do Sul**	**Índia**
Lei de Marcas Registradas de 1995	Código de Defesa do Consumidor	Lei de Direitos Autorais Nº3916	Lei da Tecnologia da Informação
Lei de Crimes Cibernéticos de 2001	Lei de Acesso à Informação (Lei 12.527/2011)	Lei de Proteção de Desenho Industrial	Lei de Direitos Autorais de 1957
Alemanha	Lei Caroline Dickman (Lei 12.737/2012)	**Estados Unidos**	Lei de Marcas Registradas de 1999
Seção 202a., 303a. Espionagem de Dados	Marco Civil da Internet (Lei 12.965/2014)	Seção 107 da lei de Direitos autorais	Lei de Patentes de 1999
Seção 303b. Sabotagem de Computador	Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018)	Lei da limitação de responsabilidade por violação de direitos autorais on-line	**Itália**
África do Sul	Decreto 8.771/2016 sobre padrões de segurança para o tratamento dos dados	Lei Lanham (Marca Registrada)	Art. 615 Código Penal
Lei de Marcas Nº127 de 1957	**Canadá**	Lei de Vigilância de Inteligência Estrangeira	**Reino Unido**
Lei de Direitos Autorais de 1978	Lei de Marcas Registradas	Lei Federal de Dissuasão de roubo de identidade e Assunção	Lei de uso indevido de computador de 1990
	Seção 342.1 do Código Penal Canadense	Lei da Privacidade de 1974	Lei de Marcas Registradas de 1994
	Lei de Direitos Autorais de 1985	Lei de Segurança de Computadores de 1987	Lei de Regulamentação dos Poderes de Investigação de 2000
	China	Lei Nacional de Proteção de infraestrutura de Informação de 1996	Lei dos Direitos Autorais e Marcas Registradas 2002
	Lei de Direitos Autorais da República Popular da China de 2001	Lei de uso indevido de computador	Regulamento de Privacidade e Comunicações de 2003
	Lei de Marcas Registradas da República Popular da China de 2001		Lei de Comunicações de 2003

Fonte: EC-*Council* (2021). Elaborado, traduzido e adaptado pela autora (2023).

Nesse contexto das legislações brasileiras aplicadas nos cibercrimes, tem-se o Código de Defesa do Consumidor instituído em 1990. Por meio desse há proteção da base de dados dos clientes no sistema comercial quanto ao sigilo e confidencialidade. Também, a Lei de acesso à informação (Lei 12.527/2011) quanto à guarda das informações pelo ente governamental (Spiri, 2020; Perroti, 2022).

No entanto, alguns acontecimentos provocaram reações no nível jurídico, tais como o caso da Lei Carolina Dickman (Lei 12.737/2012) quanto ao vazamento de informações de dispositivos móveis. Também, o Marco Civil da Internet (Lei 12.965/2014) cujos princípios trouxeram uma regulação básica quanto ao uso das informações por provedores de tecnologia. Mas a Lei de Proteção Geral dos Dados (LGPD - Lei 13.709/2018) elucidou e organizou a proteção dos dados (Spiri, 2020; Perroti, 2022).

A LGPD objetiva a regulamentação, a transparência e o controle dos dados entre o Brasil e os países estrangeiros que coletam informações de seus residentes, tendo vigência a partir de agosto de 2020. De acordo com a LGPD, dados pessoais referem-se às informações acerca da pessoa natural, tais como a identidade, CPF, geolocalização, entre outros. Dados pessoais sensíveis dizem respeito as informações raciais, étnicas, dados referentes à saúde, dados biométricos, etc. Assim, a LGP cuida de como os dados são tratados e como as empresas lidam com os vazamentos dos dados (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021; Perroti, 2022).

Pela LGP, para a coleta de informação e o processamento de dados pessoais, é necessário determinar, de forma clara, pelo menos uma base legal adotada pela empresa, seja o interesse vital do indivíduo, para a conformidade com obrigações legais, a necessidade contratual, o interesse legítimo do controlador de dados, entre outras. Por isso, foram estabelecidos dez princípios: a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas. Mas existem ainda muitas dúvidas sobre a proteção das bases de dados, uma vez que essa legislação é ampla (Perroti, 2022).

Entretanto, a LGPD prevê sanções e multas 2% sobre o faturamento anual até 50 milhões de reais nas inconformidades relacionadas à gestão de dados. É necessário reportar imediatamente à Autoridade Nacional quaisquer violações dos dados. Assim, os direitos do indivíduo devem ser respeitados. Entre esses pode-se citar o direito de acesso irrestrito e transparência, de retificação para correção dos dados, ao esquecimento com extinção de uma base de dados, à limitação de certas informações, à portabilidade para outra operadora e à oposição à determinada informação (Perroti, 2022).

Nesse sentido, as organizações devem estabelecer políticas de segurança mediante a elaboração de planos, processos, procedimentos padrões e diretrizes, protegendo as informações e integrando o programa de gerenciamento da informação. Assim, devem ser descritos os controles de segurança que constituem a infraestrutura de segurança da organização. Também, informar como trabalhar precavido com dados sensíveis ou confidenciais (Senac, 2021; Smahel, 2020).

De acordo com EC-*Council* (2021), as políticas de segurança objetivam:

a) diminuir ou excluir a responsabilidade legal de funcionários ou terceiros;
b) preservar informações confidenciais e proprietárias contra roubo, uso indevido, divulgação não autorizada ou alteração e,
c) evitar o desperdício de recursos de computação. (traduzido pela autora)

Desse modo, as organizações resguardam legalmente a rede e os sistemas de informações e a sua exposição não autorizada, além de mitigar riscos, monitorar e controlar o tráfego de dados, aprimorar o desempenho e reduzir o tempo de inatividade da rede, diminuir os custos e possibilitar a gestão efetiva. Para isso, a política de segurança deve ser clara e concisa, adequada à realidade da organização, viável de ser executada economicamente, de fácil entendimento e aplicação, consistentes, favoráveis ao empregador e empregado, discriminar áreas de responsabilidades, ser exequível por lei e estar em conformidade com a jurisdição local (Barbosa, Silva, Oliveira, Jesus & Miranda, 2021).

Contudo, a organização deve treinar os funcionários e usuários para conseguir manter a governança segura da rede e dos sistemas de informação, uma vez que esses podem ampliar a exposição ao risco, sendo primordial a divulgação das políticas de segurança de TI para conscientização do público de interesse (EC-*Council*, 2021).

2.4.3 Treinamento de segurança de rede

Os treinamentos dos funcionários são primordiais na segurança da rede e dos sistemas de informação, uma vez que são o principal ativo da organização, pois suas ações podem abrir portas para um ataque. Assim, o funcionário deve estar preparado para se defender e defender a organização, saber o que fazer diante uma ameaça, identificar dados sensíveis e confidenciais, estar familiarizado acerca da política de senha e uso de autenticação de dois fatores, assim como as consequências das violações da política de segurança. Neste contexto, os treinamentos

dos funcionários podem ser do tipo em sala de aula ou *online*, discussão em mesa-redonda, *site* de conscientização de segurança, dicas, curtas-metragens, seminários, simulação de treinamento, práticas, palestras, estudos de caso, discussões e atividades em grupo, entre outros. O acesso à rede por funcionários recém-admitidos somente deve ser concedido após treinamento ou lhe ser fornecido acesso limitado até a conclusão do treinamento (EC-*Council*, 2021).

Outra importante abordagem a ser treinada com os funcionários se refere às técnicas de ataques de engenharia social, pois, esses intrusos podem empregar técnicas de representação por meio de ligações telefônicas, de alteração de senhas nas quais o invasor se passa por autoridade solicitando modificação do nome de usuário e senha; uso de conversa relaxante para construir relacionamento com o funcionário; usando nome da autoridade para conseguir acesso a algo; se apresenta como um novo funcionário para percorrer o ambiente organizacional; envio de links maliciosos por *e-mail*; acesso à lixeira dos computadores para obtenção de informações; etc. Por isso, é relevante classificar as informações em altamente secretas, secretas, confidenciais, restritas e não classificadas, correlacionando-as com a permissão de acesso do funcionário e usuário (EC-*Council*, 2021).

Portanto, novos problemas sociais surgiram com o advento da internet, tendo no marketing macrossocial área de atuação capaz de contribuir na mudança comportamental adequada dos usuários da internet.

3 REFERENCIAL TEÓRICO

Nesta seção são abordados o marketing social e o marketing macrossocial quanto à esfera social, ao pensamento sistêmico, aos estudos desenvolvidos e as campanhas de marketing macrossocial.

3.1 Marketing social

Os princípios de responsabilidade social estiveram presentes em diversas civilizações antigas. Entre alguns desses pode-se citar, no Egito, há 3.000 a.C. o desenvolvimento do código moral fundamentado na justiça social para promover a ajuda mútua entre o povo egípcio. Na Índia, no período de 274 a.C. a 232 a.C., a preocupação com o meio ambiente na construção de poços e plantio de árvores. Na Espanha, em 1526 d.C., a propositura do censo espanhol na melhoria das atividades de caridade. Sendo que o marketing social e a responsabilidade aparecem unidos pelo mesmo sentido (Pagliano, Faria, Lago, Cruz & Silva, 1999).

Em 1952, Wiebe vinha procurando entender como vender essas campanhas sociais para alcançar o sucesso nas campanhas de produtos. Foram analisados quatro estudos de campanhas sociais com a finalidade de descobrir quais condições ou características estavam relacionadas ao sucesso ou ao fracasso. A conclusão foi que as campanhas sociais que tinham condições ou características parecidas com as campanhas de produtos tinham maiores chances de sucesso. Porém, foram identificadas limitações na prática do marketing social, uma vez que costumam ser conduzidas de modo não-mercadológico (Kotler & Zaltman, 1971).

Outros estudiosos como de Jonh K. Gal, Joe MeGinniss e Vance Packard concordavam que era possível vender qualquer coisa. Essas limitações e a falta de compreensão trouxeram desconfiança acerca do marketing social (Kotler & Zaltman, 1971). Assim, na segunda metade da década de 1960, ocorre uma modificação de paradigma na teoria e aplicação do marketing em relação às diversas mudanças sociais da época (Shaw & Tamilia, 2001)).

Nesse novo cenário, há um processo expansionista estrutural e conceitual do marketing abrangendo áreas que extrapolavam sua tradicional perspectiva econômica como, por exemplo, a religião, a política, as questões sociais, dentre outras (Barakat, Lara & Gosling, 2011).

Segundo Kotler e Zaltman (1971), o marketing social significa “a concepção, implementação e controle de programas calculados para influenciar a aceitabilidade das ideias sociais e envolvendo considerações de planejamento de produto, preço, comunicação,

distribuição e pesquisa de marketing". Para isso, emprega-se o uso de princípios e técnicas do marketing na influência de determinado grupo-alvo para modificar um comportamento em benefício de indivíduos, grupos ou da sociedade, visando melhorar a qualidade de vida (Kotler & Lee, 2011).

No Brasil, esse movimento iniciou-se com o marketing social a partir da Associação dos Dirigentes Cristãos de Empresas (ADCE) em defesa do bem-estar da comunidade, na década de 1960. A proporção acendeu com a campanha 'Faz Balanço Social' do sociólogo Hebert Sousa, conhecido como Betinho, em 1997. Depois disso, houve uma tendência da participação empresarial nas causas sociais, visto que o retorno era positivo. Assim, muitas empresas brasileiras investem no marketing social como forma de atrair clientes por meio de questões sociais, tais como a Azaleia, a Sadia, a Fundação Bradesco, o Boticário, a Natura, entre outras (Pagliano, Faria, Lago, Cruz & Silva, 1999).

A sociedade dita quais comportamentos são permitidos, proibidos ou obrigatórios. As normas sociais influenciam o comportamento dos indivíduos. Entretanto, se os membros de um grupo compreenderem as regras e padrões que dirigem e ou limitam um comportamento social, não é necessária a força da lei. Essa influência está presente na escolha alimentar, na placa do hotel comunicando que hóspedes não devem usar mais de uma vez a mesma toalha, nas campanhas de marketing e políticas voltadas para a economia de energia, acatar os *recalls* de produtos, pagamento dos impostos, evitar a poluição do meio ambiente, fumar, ingerir álcool ou drogas (Melnyk, Carrillat & Melnyk, 2022).

O marketing e os formuladores de políticas das normas sociais devem favorecer os comportamentos socialmente aceitos ou desencorajar os prejudiciais. Algumas normas sociais podem ter efeitos positivos, como não dirigir alcoolizado. Mas outras normas sociais podem ter efeito inverso, como as referentes à economia de energia (Melnyk, Carrillat & Melnyk, 2022).

De acordo com a urbanista e arquiteta Wandarti (2019), a sociedade estabelece princípios e padrões que estimulam o indivíduo. As crenças culturais, religiosas, os diferentes aspectos sociais e econômicos criam expectativas sociais. Essas podem ser expectativas empíricas da convicção do indivíduo em relação ao que outras pessoas do seu meio fazem. Também podem ser expectativas normativas que dizem respeito ao que as outras pessoas pensam em como o indivíduo deve se comportar, assim como podem ser princípios normativos pessoais que o indivíduo presume que ele ou seu grupo onde vive deve agir.

A comunidade onde vive o indivíduo influencia a credibilidade entre os indivíduos. As

opiniões dos integrantes da comunidade podem persuadir a adoção ou não de determinadas práticas. Entender como a rede comunitária se forma determina quem serão os indivíduos impactados e como serão afetados pela mudança. A qualidade de vida da comunidade pode ser alterada por meio de campanhas de conscientização, elaboração de leis ou intervenções urbanas em prol da sociedade (Wandarti, 2019).

Essa evolução da teoria de marketing social permite compreender a nova visão para o marketing macrossocial, conforme apresentado a seguir.

3.2 Marketing macrossocial

De acordo com Kennedy (2020), o marketing macrossocial é uma abordagem para resolver problemas sociais complexos e multifacetados, ou seja, quando se mostra difícil definir o problema exato, seus fatores contribuintes e caminhos para uma solução. Esse tipo de problema decorre da natureza interconectada das partes envolvidas e, se não solucionado, pode produzir um efeito cascata negativo de consequências intencionais e não intencionais.

O indivíduo nem sempre pode estar no controle completo do seu comportamento. Então, por meio de uma abordagem holística e sistêmica mostra-se facilitado o direcionamento de caminhos para a solução desses problemas nos quais o indivíduo está inserido, considerando-se o seu contexto social. Portanto, torna-se importante, após a definição do problema, a identificação das partes envolvidas e os potenciais efeitos cascata, possibilitando a implementação de mudanças em nível macro, simultaneamente (Kennedy & Parsons, 2014).

Segundo Kennedy (2020), o termo marketing macrossocial foi introduzido por Domegan, ensejando o desenvolvimento e aplicações teóricas de nível sistêmico e metodológico para o tema, tal como a teoria da perspectiva multinível (MLP), a ecologia comportamental, a teoria institucional, a teoria do mecanismo, ação, estrutura (MAS) (Layton, 2015) por meio do marketing social em nível macro para compreender o marketing dos sistemas sociais (SSM) (Domegan & Layton, 2015).

3.2.1 Esfera social

Em 2010, Collins, Tapp e Presley aplicaram a teoria dos sistemas com uma visão holística em estudos sobre problemas complexos e multifacetados. Dessa forma, incluíram a esfera social para abranger o contexto ou o sistema no qual o indivíduo habita ao longo da vida, uma vez que o ambiente o influencia (Kennedy, 2020).

A abordagem do marketing macrossocial compreende três níveis sociais que atuam em um *continuum* com as intervenções de modo integrado entre todos eles, conforme o Quadro 2 (May & Previte, 2016; Kennedy, 2020). O nível *downstream* se refere ao nível individual. Esse nível sofre a influência do nível *midstream* que é representado por grupos de líderes sociais, empresas, escolas e amigos, sendo influenciados pelo nível *upstream*. Esse nível está relacionado às atividades políticas e governamentais (Hastings, 2007; Kennedy, 2020).

Quadro 2

Níveis do sistema

Nível	Influenciadores do Indivíduo
Downstream	Família Amigos
Midstream	Escola Igreja Comunidade Local de trabalho
Upstream	Políticos Legais Econômicos
Cultura e crenças	

Fonte: Kennedy (2020). Elaborado pela autora (2023).

Assim, os pesquisadores coletaram informações com perguntas específicas, de acordo com cada nível e aspectos que devem ser influenciados. Para isso, usaram métodos de pesquisa e teorias capazes de transformar comportamentos desejados (positivos) ou obstruindo-os (negativos) conforme os estudos apresentados adiante. Além disso, sugeriram parcerias com organizações em diversos níveis do sistema, como garantia para mudanças de longo prazo, pois as camadas estariam interrelacionadas e entrelaçadas interagindo nos subsistemas. Consequentemente, se obteria um efeito cascata de intervenções influenciadoras (Kennedy, 2020).

O estudo de Gregson, Foerster, Orr, Jones, Benedict, Clarke, Hersey, Lewis e Zotz (2001) propôs um Modelo Sociológico sobre intervenções de educação nutricional e iniciativas do marketing social, sugerindo indicadores e medidas dos dados. Para tanto, apontaram cinco esferas de influências em seu modelo dentro do sistema: a estrutura social, política e sistemas; a comunidade; a institucional / organizacional; a interpessoal e a individual. O Quadro 3

apresenta exemplos de teorias, indicadores e construtos por esfera de influência do Modelo Sociológico de Gregson, Foerster, Orr, Jones, Benedict, Clarke, Hersey, Lewis e Zotz (2001).

Quadro 3

Exemplos de teorias, indicadores e construtos por esfera de influência do Modelo Sociológico

Esfera de Influência	Exemplos de Teorias	Indicadores e/ou Constructos
Estrutura social, política e sistemas	Processo de opinião pública	Transações individuais (contextos situacionais, realidade percebida, opiniões individuais), transações coletivas (opinião coletiva, consciência mútua, emergente, contexto e papéis), legitimação e transações políticas (papel político de opinião coletiva, vínculos com o governo) e a convergência desses setores.
	Processo de mudança política	Divulgação e disseminação de materiais para formuladores de políticas, *gatekeepers* e constituintes; elaboração de documentos de política; adoção de políticas; outras etapas intermediárias relevantes.
Comunidade	Teoria da mudança da iniciativa de mudança de projeto	Formação de grupos consultivos, treinamento comunitário, organizações comunitárias, oportunidades de alavancagem, convocação e educação das partes interessadas, educação pública
	Componentes do marketing social	Anúncios de serviço público, publicidade (cobertura de notícias gratuita), promoções, desenvolvimento comunitário.
	Parcerias	Grau de colaboração, tempo de parceria, relação fiscal.
	Organização comunitária	Empoderamento, competência da comunidade, participação e relevância, seleção de questões.
Instituições e organizações	Componentes do marketing social	Publicidade, publicidade e promoções específicas da organização.
	Difusão da inovação	Vantagem relativa, compatibilidade, complexidade.
	Mudança organizacional	Definição do problema, início da ação, implementação da mudança, institucionalização da mudança.
Interpessoal	Componentes apropriados do marketing social	Vendas pessoais, empoderamento do consumidor.
	Teoria cognitiva social	Capacidade comportamental, expectativas, autoeficácia, aprendizagem observacional, reforço.
Individual	Modelo trans teórico	Pré-contemplação, decisão, ação, manutenção.
	Modelo de crença em saúde	Suscetibilidade percebida, gravidade percebida, benefícios percebidos, barreiras percebidas, dicas para ação.

Fonte: Gregson, Foerster, Orr, Jones, Benedict, Clarke, Hersey, Lewis e Zotz (2001). Traduzido pela autora (2023).

Também, Dressler-Hawke e Veer (2006) estudaram a estratégia de marketing social segundo o Modelo Multinível / Multimídia de Mudança Social para promoção da mudança

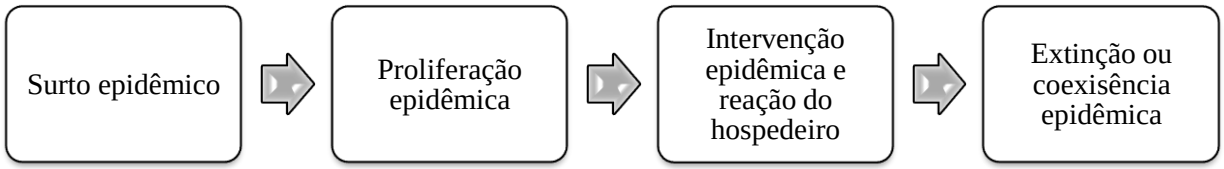
social por meio dos princípios da comunicação integrada de marketing e o Modelo Ecológico Comportamental. A comunicação integrada de marketing compreende as diversas plataformas de mídia e instrumentos capazes de comunicar uma mensagem desejada, enquanto o Modelo Ecológico Comportamental, com origem nas teorias sociocognitivas, propõe que o comportamento sofra níveis de influência individual, local, comunitário e sociocultural, sendo de natureza multifacetada. Portanto, cria-se uma sinergia na comunicação dessa associação obtida pela integração horizontal dos vários tipos de mídias e uma integração vertical desde o nível nacional ao individual. Pois, a mensagem deve ser direcionada para todos os níveis para resultar em uma adoção efetiva da mudança social total.

O comportamento saudável do indivíduo é influenciado por fatores ambientais que devem ser abordados nos estudos de marketing social que tem como proposta a mudança na saúde da população. Assim, a recomendação é juntar os níveis *upstream* e *downstream* para mudanças efetivas. Então, destaca-se a importância de se considerar a responsabilidade individual e o contexto socioambiental em que se está inserido (Dressler-Hawke & Veer, 2006).

Também, não se deve esquecer o ciclo de vida epidêmico de consumo de produtos que prejudicam a saúde com comportamentos indesejados. Pois, o marketing comercial e os fatores socioeconômicos instigam o comportamento perverso do indivíduo com repercussão na saúde da população. Portanto, ocorre o ciclo epidêmico do comportamento de consumo conforme Figura 5, isto é, períodos com campanhas que aumentam o consumo de certos produtos prejudiciais e depois ocorre a redução no consumo devido às intervenções mais intensas ou aprimoradas (Kennedy, 2020).

Figura 5

Ciclo epidêmico do comportamento de consumo conforme Kennedy (2020)



Fonte: Elaborado pela autora (2023).

3.2.2 Pensamento sistêmico

O marketing social é a abordagem de mudanças comportamentais individuais necessárias ao bem-estar do indivíduo que permeiam os problemas sociais. Esse pensamento

sistêmico por meio do marketing social iniciou-se em 1950 até começo de 1970 quando se introduziu sistemas em marketing, enquanto no período de 1970 a 1990foi inserido o pensamento sistêmico nos estudos de marketing social. A partir de 1990, houve uma integração de marketing social e ciência de sistemas. Sendo sistema entendido como o conjunto "de estruturas, atores, comportamentos, motivações, valores, atividades e ações que possuem características sociais, culturais, políticas e psicológicas" (Domegan, McHugh, Devaney, Duane, Hogan, Broome, Layton, Joyce, Mazzonetto & Piwowarczyk, 2016)

Os estudos passaram a aplicar o pensamento sistêmico para abordar o contexto social mais amplo ao invés de focar no indivíduo. Pois, os fatores que desencadeiam os problemas complexos podem escapar do controle do indivíduo, exigindo-se ações simultâneas em vários níveis do sistema, tais como o problema da obesidade. Então, os estudos deixaram de focar nas intervenções para se concentrar na causa do problema (Kennedy, 2020).

Conforme Kennedy (2020), o emprego do gerenciamento interativo (IM - Warfield, 1974) costuma ser utilizado para tratar sobre a interação entre as partes do sistema, as conexões, os caminhos e o que trabalhar. No caso *fast fashion*, onde um padrão de produção e consumo são rápidos, foi utilizada a combinação da teoria MAS e a teoria institucional para explicar o processo de mudança em nível macro:

a) normas de tarefa econômica: definem expectativas e limites de comportamento para empresas e profissionais de marketing e
b) normas institucionais culturais e morais: fornecem sistemas de significado, significado simbólico e regras constitutivas.

De acordo com Domegan (2008), Kennedy e Parsons (2012), ações estratégicas como intervenções de marketing social podem ser usadas para influenciar e mudar as normas para mitigar um problema perverso. Então, recomenda-se que sejam usadas em vários níveis por um longo período, com a finalidade de ocorrer as modificações nas normas gradualmente e substituir microestruturas que perpetuam esse problema.

Assim, aconteceu no Canadá, em nível governamental, no caso das campanhas antifumo de 1985 a 2009. De acordo com Kennedy e Parsons (2012), para alcançar a mudança de comportamento social foram realizadas diversas intervenções simultaneamente nos níveis micro (individual), meso (organizacional) e macro (estrutural), inclusive com auxílio positivo da engenharia social. Algumas medidas tomadas foram aumentar os impostos dos produtos de

tabaco, limitar locais de exibição no varejo e impedimento da propaganda e promoção que impactaram a cadeia logística. Portanto, o marketing

> [...] tem um papel na criação de motivação social para a mudança, bem como na promoção da flexibilidade social, criando imagens desejáveis de mudança, mudança de atitude e desenvolvimento de habilidades individuais, que contribuem para a mudança em nível macro. [...] Os profissionais de marketing social precisam entender os fatores estruturais e ambientais que contribuem para o comportamento problemático e se concentrar nos implementadores e controladores de intervenções estratégicas em toda a sociedade. [...] A eliminação de todos os fatores que permitem comportamentos problemáticos cria um contexto ambiental onde é fácil para os consumidores mudarem o comportamento e manterem essa mudança. (Kennedy & Parsons, 2012).

Entretanto, as mudanças comportamentais sociais gerais são difíceis de serem alcançadas por meio de alterações nas políticas. Esse fato está relacionado às limitações com as micro ações dos atores individuais. Isto é, podem envolver aspectos da aceitabilidade, conscientização ou acessibilidade, dependendo da camada da população, demonstrando a relevância de se considerar o ambiente social e cultural do sistema. Para isso, torna-se necessário a descentralização da responsabilidade e do poder, além da participação colaborativa (Jagadale & Kemper, 2022).

O marketing macrossocial objetiva conectar os três níveis *upstream*, *midstream* e *downstream* nas abordagens das deformidades sistêmicas. Pois, entende-se que o processo de institucionalização das normas, quando se refere às mudanças de crenças e atitudes, necessitam de longo prazo, porque essas normas não devem ser contraditórias e incoerentes para a população. Assim, a aplicação de intervenções pode envolver, de acordo com o nível, regulamentos, legislação, tributação, mobilização da comunidade, educação, pesquisa, etc., a fim de trazer uma mudança sistêmica holística (Jagadale & Kemper, 2022).

Com relação à metodologia de pesquisa para o nível macro e o marketing social de sistemas foram propostos diversos métodos em estudos. Domegan, McHugh, Devaney, Duane, Hogan, Broome, Layton, Joyce, Mazzonetto e Piwowarczyk (2016) estudaram a utilização de *software* de gerenciamento interativo para mapear barreiras estruturais à mudança comportamental e como superá-las. Duane, Domegan, Mchugh, e Devaney, (2016) mapearam complexas teias e cadeias relacionadas ao sistema que dificultam a mudança do

comportamento, sendo identificadas as principais áreas de intervenções que serviram para organizar estratégias.

Mas outros aspectos metodológicos também foram estudados. Kennedy, Kapitan, Bajaj, Bakonyi e Sands (2017) identificaram os atores causadores de problemas perversos, a estrutura do sistema e pontos de intervenção para entender a dinâmica total do sistema e áreas de mudanças. Domegan, Mchugh, Biroscak, Bryant, e Calis (2017) estudaram a modelagem causal não linear no mapeamento cognitivo difuso, inteligência coletiva e a modelagem de dinâmica de sistemas para mapeamento de dinâmica de problemas perversos. McHugh, Domegan e Duane (2018) empregaram um método participativo visando mapear os atores envolvidos no sistema. Além disso, propõem seu envolvimento em programas de pesquisa de mudança macro e sistêmica, que inclui a adesão aos sete protocolos, enquanto Kennedy (2017) usou uma metodologia em quatro etapas: compreensão da situação, modelagem do sistema, debater o modelo e agir.

As pesquisas de marketing macrossocial têm proporcionado novas abordagens em benefício da sociedade, abordando problemas complexos e multifacetados mediante o envolvimento nos três níveis requeridos das organizações "boa cidadania corporativa, orientação para *stakeholders* e sustentabilidade socioambiental". Além disso, a responsabilização social responsável promove a participação da comunidade. Tudo isso demonstra o engajamento construtivo e a necessidade do desenvolvimento de mais pesquisas de marketing social em nível macro (Kennedy & Smith 2022).

3.3 Marketing macrossocial no contexto do mundo digital

Em relação aos avanços tecnológicos da internet, o marketing macrossocial pode contribuir para a superação dos obstáculos decorrentes da falta da nova alfabetização em multimídias e da falta de acesso às tecnologias construindo um letramento digital capaz de desenvolver habilidades em usar as ferramentas digitais (Carretero, Vuorukari & Punie, 2017; National Center for Education Statisics[9], 2021; Wicht, Reder & Lechner, 2021; Kalmus, Opermann & Tikerperi, 2022; Mascheroni & Cino, 2022; Ponte, S. Batista & R. Baptista, 2022; V. Silva, 2015; Waechter, Stuhlpfarrer, Böttcher, Bernhardt & Kadera, 2022). Além disso, o papel do marketing macrossocial em direção às transformações digitais pode acontecer pelo

[9] por meio do *Programme for the Internacional Assessement of Adult Competencies* (PIAAC) promovido pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

desenvolvimento dessa nova alfabetização exigida e pela nova modelagem dos mercados e sistemas de marketing capazes de seduzir as pessoas para práticas participativas. Portanto, o marketing macrossocial nos próximos anos desempenhará importante função para melhorar as condições da humanidade, pois as pessoas estão, cada vez mais, procurando participar das novas experiências que o mercado tecnológico tem oferecido (Fýrat & Vicdan, 2008).

De acordo com Fýrat e Vicdan (2008), o mercado determina a vida das pessoas conforme as necessidades da economia de mercado para sua expansão. Diante disso, o surgimento da internet criou, não somente a economia digital, bem como os recursos culturais, a mão de obra técnica necessária, a mão de obra afetiva que proporciona novas experiências ou modifica as já existentes, além da materialização da inteligência coletiva. Desse modo, com a internet, houve um processo de valorização dessa cadeia cultural, técnica e afetiva. Além disso, a internet tornou o indivíduo um tolo passivo por meio das práticas de mercado, e aqueles ativos acabam não sendo remunerados com a lógica capitalista, mas pela troca de prazer e aprendizado mútuo.

Jenkins (2008) corrobora afirmando que os consumidores internautas desempenham papeis de valor e ameaça para as empresas mídias corporativas devido à sua participação na divulgação de conteúdos como uma forma de mercantilizar e comercializar. Entretanto, revela que esse internauta que navega, compra, divulga, etc. pode não ser alfabetizado digitalmente. A participação social tem seus benefícios que precisam vencer à restrição a essa alfabetização que se coloca como um modo de controle por diferentes setores da sociedade.

Torna-se necessário superar esses novos desafios que permeiam essas complexas interações advindas do surgimento da internet quanto ao capital e ao trabalho, aos recursos de alocação, a reconfiguração do mercado e dos sistemas de comercialização. Assim, o marketing macrossocial pode ajudar nessas questões em que a pessoa não é somente consumidor, mas um ser capaz de criar novos modos de vida que não sejam estipulados pelas práticas de mercado. Também auxiliam o desenvolvimento dessa nova alfabetização exigida, no intuito de tornar as pessoas participantes plenas nessas interações, assim como, nessa remodelagem do mercado e do marketing, na construção de novos modos de vida e experiências (Fýrat & Vicdan, 2008).

Segundo Fýrat e Vicdan (2008), pela internet é possível a participação das pessoas por meio das diversas mídias existentes, tais como *weblogs*, fóruns de discussão, *Indymedia, Alternet, Google, YouTube*. Além disso, as pessoas que têm acesso e recursos ajudam as pessoas que não os têm. Também, há uma tendência das pessoas quererem produzir produtos que tornam a experiência prazerosa para outras pessoas, como navegar por diferentes

experiências de vida. Então, a internet disponibilizou todas as ferramentas para as pessoas participarem de forma ativa ou passiva dessa transformação digital.

Essa interação social gerou dados que produziram inúmeras informações acessíveis as quais vão além da capacidade de processamento e do controle do fluxo das informações. Entretanto, o indivíduo poder acessar este volume de informações não significa que saibam o que fazer com informações para lidar com os problemas advindos do uso da internet. É um processo de aprendizado que envolve "compartilhar, implantar, confiar, avaliar, questionar e trabalhar o conhecimento coletivo" (Jenkins, 2008).

A transformação provocada pela internet foi essa ruptura de limites geográficos na construção do social. O mundo globalizado permitiu formações híbridas e formas de fluxo e mobilidade determinadas pelas tecnologias que surgem. Então, a sociedade assume tanto o papel de produtor como de consumidor, assumindo múltiplas experiências seja na criação de materiais para consumo ou na construção de modos de vida, experiências e significados (Fýrat & Vicdan, 2008).

Para Fýrat e Vicdan (2008) é certo que o uso das novas tecnologias e seus recursos promoveu o engajamento participativo das pessoas, apesar de existirem muitas sem acesso e recursos, seja por distinção de classe, pobreza e/ou isolamento. Pois, o marketing tem como limitação a produção de formas para capacitar pessoas a dividir com outras a organização de suas vidas. Essa abordagem social vem sendo estudada pelo marketing macrossocial na medida que existem cada vez menos unidades consumidoras nesse novo mercado tecnológico e um sistema de comunidade de pessoas que participam da criação e operação dos processos de experiências e modos de vida para estarem no controle.

A tecnologia propicia diferentes formas de controle, tais como as redes sociais promovem uma comunicação pessoal, participativa e convencedor. Essa comunicação tem o poder de influenciar por propagar facilmente entre os internautas e estabelecer um canal bidirecional com as empresas. Deve-se atentar ao tipo de informação divulgada para não se transmitir informações erradas ou até mesmo restringir conforme a conveniência de marketing gerando um problema (Lima, Fiorentini, Costa, Yamamuro, Schiavoni, Fernandes, Coutinho, Barcellos, Aranha, Busarello, Lindenberg, Cavalcanti, Meira & Fontoura, 2009).

Outro ponto importante é que os processos das tecnologias digitais são complexos quanto ao dilema corpo-mente no que diz respeito à presença e ausência corpórea. Assim, o processo de experiências deve ser considerado em diferentes momentos e diferentes contextos com a finalidade de fornecer as ferramentas adequadas para tratar os fenômenos

contemporâneos. Para isso, o marketing macrossocial propõe processos em que os participantes experimentam uma variedade de diversos equilíbrios. Em se tratando das novas tecnologias, o participante vivencia uma multiplicidade de "eus" em uma diversidade de modos de viver e ser, como vias alternativas com seus significados. Assim, o participante não se prende à uma única forma de experiência de vida (Fýrat & Vicdan, 2008).

Do mesmo modo, o processo da alfabetização passou por uma expansão no século XX por meio do livro escrito, do cinema, da televisão e do rádio e o textual superado pelo visual com o advento da internet. Nesse sentido, a tendência será a exploração dos demais sentidos pelas tecnologias. Isso leva à uma questão social que diz respeito às habilidades exigidas no mundo e às que a pessoa já possui, demonstrando a necessidade de composições multineares e multissensoriais para se comunicar. Logo, o marketing macrossocial precisa desenvolver condições para uma nova alfabetização se propagar entre as pessoas, na tentativa de capacitar as pessoas analfabetas digitais de se comprometerem com a organização de suas vidas (Fýrat & Vicdan, 2008).

O marketing macrossocial envolve ações estratégicas, como as intervenções, para influenciar e mudar as normas e para mitigar um problema perverso. Entretanto, essas ações devem ocorrer nos diferentes níveis de modo consistente e simultâneo (Jagadale & Kemper, 2022).

No nível *downstream* é possível a adoção de medidas para o indivíduo se proteger no comércio eletrônico, *internet banking*, redes sociais e nos dispositivos móveis. No que se refere ao comércio eletrônico, é comum golpes com *sites* falsos (*phishing*), *sites* fraudulentos, *sites* de leilão e vendas de produtos que não são entregues ou o uso de dados pessoais e financeiros para outros fins. Então, o indivíduo corre riscos de o produto não ser entregue, chegar com atraso, danificado, ilícito ou em desacordo com o especificado, além da dificuldade de contatar a loja, ter os dados pessoais e financeiros obtidos de forma ilegal por comerciantes, ou serem roubados ou repassados sem autorização para outras empresas (Velho, 2016; Steinberg, 2020; CERT.br, NIC.br, CGI.br & ANPD, 2021).

Em relação ao *internet banking*, os cibercriminosos têm dificuldades para fraudar os servidores das instituições bancárias. Contudo, empregam a engenharia social, alegando necessidade de atualização cadastral ou módulos de proteção para se evitar a suspensão de serviços e acesso, ou oferecendo campanhas de lançamento de produtos, etc. Também, disponibilizam aplicativos capazes de coletar dados, aproveitam das vulnerabilidades dos dispositivos para a instalação de códigos maliciosos, roubam dados sem criptografia na rede,

entre outros métodos. Então, os indivíduos estão expostos a riscos de perdas financeiras, violação do sigilo bancário, invasão da privacidade, participação em fraudes (Velho, 2016; Steinberg, 2020; CERT.br, NIC.br, CGI.br & ANPD, 2021).

Quanto às medidas de segurança nas redes sociais, essas precisam ser redobradas, pois, as informações se propagam rapidamente, atingindo grande quantidade de pessoas de diversas faixas etárias, além de não haver controle sobre as informações divulgadas e serem difíceis de serem excluídas, os indivíduos correm riscos de furto de identidade, de invasão de perfil, do acesso a conteúdos impróprios ou ofensivos, de danos à imagem e à reputação, do contato de pessoas mal-intencionadas que podem passar mensagens maliciosas (Velho, 2016; Soares, Araújo & Souza, 2020; Steinberg, 2020; Martins, 2021; CERT.br, NIC.br, CGI.br & ANPD, 2021).

Em referência aos dispositivos móveis, esses se tornaram os preferidos da população, porque podem ser levados em locais que frequenta, permitem o armazenamento de dados pessoais e profissionais e permanecer conectado. Contudo, apresentam os mesmos riscos dos computadores, tais como vazamento de informações, maior possibilidade de perda e furto, invasão da privacidade, instalação de aplicativos maliciosos e propagação de mensagens com códigos maliciosos (Velho, 2016; Steinberg, 2020; CERT.br, NIC.br, CGI.br & ANPD, 2021).

No nível *midstream* (grupos de referências), o indivíduo sofre influências de familiares, igrejas, escolas e organizações. Diante disso, a orientação aos professores e pais sobre os perigos presentes na internet deve ser por meio da informação, conhecendo os riscos que os alunos e filhos estão expostos para se prevenirem de ameaças e ataques. Então, a participação da escola e da família é essencial, no intuito, de se a usar a internet com segurança, aproveitando as oportunidades e inovações tecnológicas que surgem, mas os riscos são reais. (Unicef, 2013; Areepattamannil & Khine, 2017; CERT.br, NIC.br, CGI.br & ANPD, 2021)

Cabe ressaltar que o uso excessivo da internet põe em risco a saúde física e psicológica do indivíduo, seja adulto ou criança. É importante para os professores, pais e familiares próximos perceberem se está ocorrendo prejuízos na vida estudantil, profissional e social dos filhos. Além de poder ocorrer acesso a conteúdos impróprios e falsos, é recomendado o uso de filtros dessas informações e senso crítico, conforme a idade e a maturidade dos filhos. Informações na internet são divulgadas e se espalham rapidamente, sendo difíceis de serem excluídas (Maria Joserlane Xavier, Figueiredo, Aldo Xavier, Neres & Lavôr, 2018; Cardoso, 2020; Safernet Brasil, 2022a).

Por esses motivos, as participações dos grupos de referência têm papel significativo,

uma vez que a criança e o adolescente podem ser influenciados na adoção de comportamentos seguros. Neste sentido, em 2011, o escritor de grandes obras infantis, Ziraldo, também se engajou nessa causa social, publicando a cartilha ‘A internet segura do menino Maluquinho’. A obra traz dicas de segurança cibernética, com livre distribuição pela internet pela página do Ministério Público do Paraná.

Portanto, torna-se fundamental observar o comportamento em casa ou na escola, reforçando os cuidados que se deve ter com pessoas não conhecidas, além de ensinar noções de privacidade, cuidados com *ciberbulling*, estabelecer regras e auxiliar na proteção das contas de acesso (Castillejos Lópes, Torres Gastelú & Lagunes Domínguez, 2016; Safernet Brasil, 2022a).

No nível *upstream* é primordial a divulgação de campanhas publicitárias sobre medidas de segurança para prevenir ciberataques, principalmente, em momentos em que a sociedade pode estar exposta. Em períodos de comemorações festivas ou de campanhas eleitorais há muita veiculação de mídias pela internet que aumentam o tráfego de dados e o número de falsas informações. Assim, pretende-se inibir as notícias falsas e o compartilhamento delas (Safernet Brasil, 2021). Outra campanha idealizada pelo governo foi a “Proteja seus dados” na intenção da conscientização de proteção de dados dos consumidores para identificar e evitar tentativas de golpes pela internet. Nessa campanha houve enfoque aos cibercrimes e a LGPD (Brasil, 2021).

A mitigação dos ciberataques consiste na realização de amplas campanhas educativas pelo governo, assim como a promulgação e implementação de instrumentos legais efetivos para a proteção dos dados. A sociedade não pode se tornar vítima de *crackers*, sendo responsabilidade de todos os níveis contribuir para que os crimes cibernéticos sejam reduzidos (Santana & Oliveira, 2006; Axier & Rainie, 2019).

3.4 Campanhas publicitárias sobre segurança da informação

Em 1999, foi criado na União Europeia (UE) o Programa *Safer Internet* que evoluiu para o Programa *Safer Internet Plus* em 2005, tendo a finalidade de propiciar a divulgação de conhecimentos sobre o uso ético e seguro da internet e novas tecnologias. Esse programa tem escopo amplo, envolvendo diversos atores das áreas da tecnologia da informação, das operadoras de telefonia, de ONGs do bem-estar infantil, entre outros. Sua atuação abrange quatro vertentes que compreendem o combate ao conteúdo ilegal, a sensibilização dos perigos

da internet, o conteúdo indesejado e nocivo e a promoção de um ambiente mais seguro. A intenção é integrar a sociedade com denúncias dos cidadãos e consumidores aos órgãos apropriados (European Free Trade Association - EFTA, 2022).

Além disso, o Programa *Safer Internet Plus* da Comissão Europeia atinge uma dimensão transnacional por meio da rede *Insafe* entre os países para disseminação das melhores práticas alcançando fronteiras mundiais. Ações de conscientização dos perigos direcionadas aos pais, professores e crianças são realizadas pelas organizações multiplicadoras e por canais eletrônicos para fortalecer e mitigar esse problema (EFTA, 2022).

Também, o programa atua com ferramentas para filtragem dos conteúdos indesejados, com o financiamento de projetos na área e com o suporte para divulgação das melhores práticas. Isso foi possível pelo estabelecimento de novos códigos de condutas, como medidas de autorregulação em que indústria, organizações e formuladores de políticas possam debater sobre a segurança na internet (EFTA, 2022).

No Brasil, a organização da Campanha do Dia Internet Segura está sob a responsabilidade da Safernet Brasil, do Ministério Público Federal em São Paulo e do Comitê Gestor da Internet Brasileira com a colaboração de outras instituições interessadas. A proposta desses eventos é a responsabilidade compartilhada entre governos, educadores, pais, ONGs, veículos de mídia, indústria e outros atores relevantes na proteção dos direitos dos cidadãos no que se refere ao uso das novas tecnologias. Os organizadores acreditam que a parceria entre esses atores é fundamental para garantir o uso positivo dessas novas tecnologias, bem como reduzir os riscos decorrentes de comportamentos perigosos ou abusivos (Safernet, [n.d.]).

Esse projeto promove campanhas anuais desde 2009, no Brasil, com eventos que tem grande repercussão nacional e internacional conforme mostra a Tabela 4. O número de participantes tem aumentado assim como as atividades e as parcerias, constatando que a mensagem tenha sido transmitida (Safernet, 2022b).

A 15ª Edição do Dia da Internet Segura no Brasil, no dia 07 de fevereiro de 2023, aconteceu em São Paulo de forma presencial gratuita, sendo transmitido ao vivo pelo *Youtube* e *Facebook*. O tema foi "Unidos para uma Internet Mais Positiva". Na agenda do evento havia especialistas nacionais e internacionais, tal como na palestra "Crescendo no mundo digital", apresentada por Jessica Taylor Piotrowski da Universidade de Amsterdam (Safernet, 2023e).

Também, foram debatidos três painéis. O primeiro sobre Tecnologias emergentes e os desafios na proteção *online*. Participaram desse painel Kruakae Pothong da LSE – 5 *Rights – Digital Future Commission*; Lilian Kariuki - *Executive Director of Watoto Watch Network* –

SIC Kenya e Verity McIntosh da *University of the West of England Bristol,* tendo como moderadora a Cristine Hoepers, Gerente Geral da CERT.br (Safernet, 2023e).

O segundo painel foi sobre Cidadania, segurança e bem-estar digital nos currículos da Educação Básica. Participaram desse painel Kelly Mendoza da VP Programas de educação *Common Sense* (USA), Martin Felipe Cáceres Murrie – Diretor Executivo do *Centro de Innovación Enlaces* – Min. Educação Chile, Mariana Cartaxo – Diretora do Programa de Acesso Digital – Embaixada Britânica em Brasília e Rodrigo Nejm – Diretor de Educação da Safernet Brasil, tendo como moderador Alexandre Barbosa – Gerente do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – CETIC.br (Safernet, 2023e).

O último painel foi sobre Novos desafios para a segurança digital. Participaram desse painel Giovanna Ventre da *Google* Brasil, Taís Niffinegger – Gerente de Bem-Estar LATAM Meta, Dario Durigan – Políticas Públicas do *WhatsApp* no Brasil, Priscilla Silva Laterça – Gerente de Políticas Públicas de Segurança do *TikTok* e Bruno Faria Aguieiras – *Business Information Security Officer*, Vivo (Telefônica Brasil), tendo como moderadora Juliana Cunha – Diretora de Projetos Especiais Safernet Brasil (Safernet, 2023e).

Tabela 4

Campanhas do Dia da Internet Segura no período de 2009 a 2021 (continua)

Ano	2009	2010	2011	2012	2013	2014	2015
Data	10/02	09/02	08/02	07/02	05/02	11/02	10/02
Tema	Segurança na rede	Pense antes de postar	Estar online é mais que um jogo	Conectando gerações	Direitos e deveres online	Construindo juntos	Faça sua parte
Participantes	+1.380	+1.590	+3.340	+6.220	+7.020	+21.842	+73.430
Atividades	13	13	54	61	65	152	105
Instituições	13	18	39	61	65	110	82
UFS	4	6	15	20	23	27	27

Tabela 4

Campanhas do Dia da Internet Segura no período de 2009 a 2021 (concluso)

Ano	2016	2017	2018	2019	2020	2021	2022
Data	09/02	07/02	06/02	05/02	05/02	09/02	08/02
Tema	Vamos criar uma internet melhor	Seja a mudança	Crie, conecte e compartilhe respeito	Juntos por uma internet mais positiva	Juntos por uma internet mais positiva	Unidos para uma internet mais positiva	Unidos para uma internet mais positiva
Participantes	+253.700	+69.643	+73.650	+44.000	+45.527	+95.824	+166.660
Atividades	71	127	89	122	108	51	35
Instituições	114	84	50	63	50	23	37
UFS	16	18	19	22	17	14	18

Fonte: Safernet (2023e). Elaborado pela autora (2023a).

As atividades incluíram o lançamento e a divulgação de materiais como cartilhas, vídeos e dados pela CERT.br/NIC.br. O evento ocorreu durante toda a semana.

Além das campanhas publicitárias, as ações educativas à respeito do tema também são disseminadas por meio de cartilhas digitais produzidas pelo governo brasileiro e parcerias, conforme exemplos apresentados no Quadro 4.

Quadro 4

Cartilhas educativas sobre cibercrimes (continua)

Ano	Título	Produtores	Link
2011	Guia para o uso responsável da internet 4.0	CDI GVT	www.internet responsavel.com.br
2008 2009 2010 2011 2012 2013	Safer dicas em quadrinhos	CNPG Governo Federal MPF Petrobras Polícia Federal SaferNet Brasil	
2015	Diálogo Virtual 2.0 Preocupado com o que acontece na internet quer conversar?	cgi.br MPF nic.br PFDC Safernet Unicef WeProtect	www.safernet.org.br/cartilha
2017	Guia para Pais do Instagram	Safernet Brasil	
2012	Navegar com segurança: por uma infância conectada e livre de violência sexual.	Childhood Instituto	www.childhood.org.br
n.d.	Como os seus cliques são rastreados na internet	Safernet Brasil	www.safernet.org.br/cartilha

Quadro 4

Cartilhas educativas sobre cibercrimes (concluso)

Ano	Título	Produtores	Link
2009	Segurança em redes sociais: recomendações gerais	CAIS RNP Ministério da Educação Ministério da Ciência e Tecnologia	www.safernet.org.br/cartilha
2011	A internet segura do menino maluquinho	Abrinq F-Secure Secretaria da Educação do Governo de São Paulo TV Cultura Pinto (2009)	https://www.colegiosete.com.br/escoladigitalsegura/cartilhas/cartilha_internet_segura_maluquinho.pdf
2020	Cartilha de segurança cibernética: prevenção e orientações contra crimes cibernéticos	Tribunal de Justiça de Santa Catarina	https://www.tjsc.jus.br/documents/66294/2623449/cartilha+segurança+cibernetica
2022	Prevenção contra invasões e crimes informáticos	Tribunal de Justiça de Minas Gerais	https://canalcienciascriminais.com.br/wp-content/uploads/2020/01/cartilha_cr.pdf

Fonte: Elaborada pela autora (2023).

As cartilhas abordam o uso da internet de modo seguro numa linguagem acessível, desde o público infantil e adolescente ao adulto. Também, em algumas cartilhas são encontradas atividades recreativas sobre o assunto. Além disso, procuram conscientizar sobre como agir diante de situações que põem em risco a integridade do internauta e disponibilizam links dos canais de denúncias.

No capítulo que segue são descritos os procedimentos metodológicos adotados nessa pesquisa.

4 METODOLOGIA

Nesta seção apresenta-se o percurso metodológico adotado para atingir os objetivos da pesquisa, considerando: tipo, abordagem e método de pesquisa; população e amostra; técnicas de coleta de dados e técnicas de análise dos dados.

4.1 Tipo, abordagem e método de pesquisa

As pesquisas descritivas têm por finalidade descrever as características de uma determinada população ou fenômeno ou o estabelecer relações entre variáveis (Gil, 2008; Pereira, 2016). Cervo e Bervian (2007) afirmam que os pesquisadores em uma pesquisa descritiva podem observar e analisar fatos, fenômenos e variáveis sem manipulá-los. Assim, esta pesquisa é do tipo descritiva porque descreve o fenômeno da adoção de comportamento digital seguro de um grupo de usuários da internet. Além disso, essa visa descobrir a existência de associações entre as variáveis coletadas.

Quanto à abordagem quantitativa, Terence e Escrivão Filho (2006) afirmam que é possível realizar deduções por meio de testes de teorias e hipóteses, comprovação, interpretação e predição, no intuito de mensurar, analisar ou descrever as relações causais existentes entre as variáveis pesquisadas. Também, na pesquisa quantitativa, levantam-se dados estatísticos por meio da coleta de dados e análise das variáveis, permitindo explicar o comportamento estudado (Gil, 2008; Perovano, 2016). Assim, esta pesquisa se estrutura sob a perspectiva da abordagem quantitativa por essas razões.

Este estudo utiliza o método de pesquisa de *survey*, empregado comumente em ciências sociais para entender uma população maior que a selecionada, podendo ser associado com outros métodos (Babbie, 2001). Dessa maneira, espera-se desenvolver proposições gerais sobre a adoção de comportamento digital seguro entre usuários de internet.

Além disso, é possível explicar fenômenos mediante testes rigorosos e complexos, pois, envolve várias variáveis correlacionadas. Assim, torna-se viável um modelo lógico de causa e efeito (Babbie, 2001). Por isso, serão analisados um grande número de casos para que se possa replicar entre vários subconjuntos da amostra. Isto é, se detectada alguma correlação entre duas variáveis da pesquisa, consegue-se determinar facilmente se esta relação ocorre igualmente entre os subgrupos da amostra. Desse modo, robustece-se a certeza da correlação representativa do fenômeno geral na sociedade, permitindo ser testada e retestada por outros pesquisadores.

Segundo Babbie (2001), a pesquisa survey tem disponível um grande número de

variáveis para compreender o fenômeno. Uma vez que são quantificáveis e processadas por programas computacionais, constroem-se diversos modelos explicativos e seleciona-se o que se adequa melhor aos objetivos da pesquisa.

A seguir são apresentadas a população e amostra da pesquisa.

4.2 População e amostra

Conforme Colauto e Beuren (2009), uma população compreende um conjunto de elementos com número de características em comum, podendo ser constituída por indivíduos, organizações, entre outros. Nesta pesquisa, a população foi composta de indivíduos com idade acima de 18 anos e que utilizam a internet pelo menos duas vezes por semana.

Quanto à amostra, diz respeito ao subconjunto da população selecionada submetida à alguma aplicação, sendo por meio de métodos amostrais probabilísticos ou não probabilísticos (Malhotra, 2012). Colauto e Beuren (2009) afirmam que a amostragem probabilística apresenta representatividade e tratamento estatístico, enquanto a amostragem não probabilística utiliza-se de critérios exclusivos na definição da amostra de modo subjetivo pelo pesquisador. Assim, nesse tipo de amostragem não se tem como prever o erro amostral que impossibilita a generalização dos resultados.

Neste estudo, a amostra foi de caráter não probabilístico, compreendendo essa os indivíduos que perfazem os critérios estabelecidos e se dispuseram a responder ao questionário aplicado. A amostra foi composta por 294 (duzentos e noventa e quatro) indivíduos. Hair, Babin, Money e Samouel (2005) postulam o mínimo de cinco questionários por variável analisada e o ideal o mais próximo de dez por questão em escala *likert*. Considerando que o instrumento de coleta de dados apresenta 37 questões em escala *likert*, a amostra atingiu 7,94 questionários por variável analisada, conferindo segurança à análise estática.

A seguir são apresentadas as técnicas de coleta da pesquisa.

4.3 Técnicas de coleta

Em relação ao questionário, segundo Gil (2008), esse é composto de questões para investigar informações a serem estudadas de determinadas pessoas. Assim, nesta pesquisa foi utilizado um questionário estruturado, disponível no Apêndice A, para obter informações relevantes aos cibercrimes. É constituído por uma apresentação da pesquisa e pelo Termo de Consentimento Livre e Esclarecido com informações sobre a finalidade, os objetivos da

pesquisa, o anonimato, o sigilo e como serão utilizados os dados coletados.

A elaboração do questionário se fundamentou na literatura sobre a temática e nos questionários da Comissão Europeia[10] (European Commission, 2022) e do *site* da *Ikanos.eus*. (2022). Foram criadas 72 variáveis compondo o questionário, sendo 7 variáveis para análise do perfil sociodemográfico do usuário, 26 variáveis descritivas sobre a área da segurança e 37 variáveis referente aos quatros construtos *downstream*, *midstream*, *upstream* e segurança apresentados no APÊNDICE B. O questionário apresenta três perguntas excludentes, referindo-se à concordância em participar da pesquisa, ter 18 anos de idade ou mais e acessar no mínimo duas vezes por semana a internet.

Também, Hair, Black, Babin, Anderson e Tatham (2009) recomendam que o pesquisador retire os casos ou as variáveis que apresentarem alto valor de dados faltantes da pesquisa. Assim, todas as questões desta pesquisa foram elaboradas como obrigatórias no *Google Forms*, isto é, o participante não poderia passar para a pergunta seguinte sem responder à pergunta atual. Essa medida garantiu maior aproveitamento dos dados coletados.

As questões dos quatros construtos contêm variáveis em escala *likert* com variação de 1 a 5 pontos, sendo: (1) Discorda totalmente; (2) Discorda parcialmente; (3) Neutro – Não concorda e nem discorda; (4) Concorda parcialmente e (5) Concorda totalmente. As questões com as variáveis na escala *likert* permite indicar o grau de concordância do participante acerca das variáveis (Virgillito, 2010). A aplicação de um instrumento de pesquisa com escala *likert* permite que o respondente possa indicar seu grau de concordância a respeito de determinada variável da forma mais clara e objetiva possível (Virgillito, 2010).

Esse questionário estruturado foi aplicado à amostra de usuário por meio da ferramenta digital do *Google forms*. O pré-teste foi realizado enviando-se para a base de contatos da pesquisadora o *link* desse questionário após uma abordagem direta com os participantes. Como não houve necessidade de alterações no pré-teste, todos os dados coletados nessa fase foram aproveitados para a etapa seguinte da pesquisa.

A maior parte dos dados foi coletada de forma presencial pela pesquisadora (82%). Foram abordadas 440 pessoas, sendo que 299 aceitaram responder ao questionário. Para a coleta foi utilizado um *tablet* de 10 polegadas exclusivo para a pesquisa que permitiu melhor visualização do questionário do participante de qualquer idade. Também, foi usada a internet particular da pesquisadora como meio de acesso ao questionário no *Google forms* para garantir

[10] Foi fundada em 1958 para defender os interesses da comunidade europeia, tendo entre as suas diversas funções propor legislação, gerir e aplicar políticas.

segurança aos dados coletados.

Para a coleta de dados de forma presencial foi escolhida o Terminal Rodoviário Governador Israel Pinheiro em Belo Horizonte, durante os dias dia 08 de dezembro de 2022 a 29 de janeiro de 2023. A escolha do *locus* de coleta de dados considerou que a Rodoviária, por contemplar grande trânsito de pessoas de distintas origens, pudesse levar a uma amostra mais representativa da população, que não seria acessível por outros métodos de coleta de dados. A Direção da Rodoviária autorizou a coleta dos dados para a pesquisa.

A seguir são apresentadas as técnicas de análise dos dados da pesquisa.

4.4 Técnicas de análise dos dados

Para a análise dos 294 questionários coletados procedeu-se com o tratamento dos dados *outliers*, a análise descritiva das variáveis e a análise multivariada dos dados, conforme exposto a seguir.

4.4.1 *Outliers*

A primeira etapa da análise de dado foi sobre o tratamento dos dados que compõem a amostra. Assim, inicialmente foram identificados os dados atípicos – *outliers* – da amostra. Esses dados foram aqueles em que os entrevistados apresentam casos excepcionais em comparação com os outros elementos da amostra. Como os principais cálculos dessa dissertação envolvem a utilização de técnicas estatísticas de análise multivariadas, optou-se por identificar os *outliers* multivariados.

Por conseguinte, o primeiro passo desse processo consistiu em calcular o valor da Distância D^2 de Mahalanobis para cada registro da amostra. Além disso, foi necessário calcular o valor do Teste do Qui-Quadrado com o parâmetro de significância de 0,001. O número de graus de liberdade a serem usados foi o mesmo número de itens paramétricos a serem usados nos cálculos utilizando as técnicas de estatística multivariada.

A quantidade dos indicadores paramétricos desta dissertação foi de 37 itens, os quais representam os quatro construtos já definidos anteriormente. Por conseguinte, o resultado do teste do Qui-Quadrado foi de 69,35. Assim, para todos aqueles registros que apresentarem o seu valor Distância D^2 de Mahalanobis acima de 69,35 foram classificados como sendo *outliers* multivariados.

A Tabela 5 mostra os valores da Distância D^2 de Mahalanobis para todos os registros

da amostra.

Tabela 5

Elementos da Amostra e a Distância D^2 de Mahalanobis (continua)

Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2
1	67,03451	75	17,32030	149	24,01983	223	25,50674
2	44,17957	76	56,37511	150	52,41265	224	36,09148
3	10,89344	77	19,21907	151	35,95454	225	19,43778
4	53,77632	78	37,42252	152	28,27332	226	40,63054
5	*71,72034*	79	34,76613	153	32,32251	227	53,09768
6	39,59734	80	22,68729	154	26,66959	228	18,63501
7	28,26099	81	33,44321	155	44,10302	229	34,54288
8	*75,54456*	82	*69,93369*	156	17,87311	230	60,71895
9	10,64219	83	25,56618	157	26,15675	231	9,82828
10	23,50603	84	9,24006	158	30,34120	232	*80,11810*
11	22,23677	85	24,56005	159	27,60726	233	38,07151
12	38,70510	86	36,09496	160	53,35759	234	33,63534
13	26,08390	87	59,12942	161	19,81701	235	27,26164
14	38,73040	88	53,03674	162	18,30170	236	21,87758
15	62,93971	89	*70,07074*	163	18,65133	237	39,54527
16	15,19810	90	49,40067	164	17,06723	238	15,72618
17	40,56599	91	49,10191	165	40,90023	239	58,50726
18	30,16042	92	45,74211	166	30,75050	240	11,99940
19	20,04054	93	31,05751	167	34,55559	241	24,58683
20	28,78864	94	*72,33717*	168	50,61502	242	14,96905
21	47,83086	95	*75,65050*	169	15,69626	243	17,32814
22	56,04711	96	49,49582	170	17,07090	244	25,43022
23	47,03483	97	*80,28946*	171	33,93612	245	34,39405
24	38,95713	98	62,68651	172	9,44129	246	28,23061
25	24,30325	99	38,44074	173	28,94228	247	28,80412
26	24,50192	100	45,97703	174	32,57109	248	39,27687
27	42,07196	101	*76,39386*	175	34,92211	249	34,98743
28	24,52822	102	24,08612	176	22,05458	250	24,61201
29	27,34146	103	21,31307	177	33,64031	251	*90,37085*
30	40,45374	104	26,85124	178	28,62696	252	18,77068
31	11,13631	105	35,19455	179	28,83350	253	69,18571
32	17,95309	106	48,16183	180	36,40431	254	36,69021
33	13,96960	107	34,53987	181	15,53662	255	38,25136
34	17,30252	108	53,52288	182	17,52957	256	50,54768
35	37,70463	109	22,07194	183	22,17651	257	30,88890
36	37,11137	110	29,76366	184	51,50156	258	13,20623
37	13,26995	111	8,20147	185	22,11865	259	53,77877
38	34,45650	112	49,89238	186	41,51505	260	*82,26809*
39	59,45264	113	42,65927	187	41,00447	261	51,10209
40	34,18371	114	25,94954	188	24,70118	262	23,21487
41	42,84874	115	30,22685	189	15,79976	263	47,79121
42	60,98851	116	19,02130	190	23,53465	264	43,30523
43	23,99274	117	35,23662	191	31,47005	265	37,94396
44	39,79021	118	*79,41593*	192	34,53409	266	*84,12545*
45	17,80865	119	21,74126	193	27,42145	267	61,92211
46	33,79675	120	57,21797	194	23,47125	268	31,30840

Tabela 5

Elementos da Amostra e a Distância D^2 de Mahalanobis (concluso)

Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2	Elemento da Amostra	Valor do Teste do X^2
47	25,60850	121	39,67361	195	32,30259	269	29,19319
48	49,09377	122	42,89567	196	27,93645	270	21,87195
49	20,02973	123	25,95137	197	*90,31233*	271	41,72223
50	30,64775	124	27,54339	198	22,97883	272	51,75601
51	20,89003	125	31,92892	199	37,35539	273	22,13303
52	41,42662	126	42,14364	200	*81,63517*	274	67,04911
53	18,30711	127	23,49328	201	41,86963	275	13,67179
54	*75,24866*	128	37,35783	202	52,80166	276	37,05217
55	29,02437	129	27,81129	203	30,35322	277	10,19228
56	*78,97851*	130	61,06534	204	59,41910	278	26,36286
57	66,30087	131	49,96078	205	47,07756	279	18,22092
58	46,94228	132	29,09070	206	61,94198	280	46,21301
59	46,67004	133	29,82577	207	21,95646	281	18,68824
60	14,00861	134	17,70584	208	44,32748	282	30,18322
61	41,70692	135	42,59366	209	27,65459	283	27,36886
62	27,90938	136	*79,84728*	210	27,43397	284	21,67062
63	32,96280	137	28,99696	211	21,57660	285	26,73742
64	18,39348	138	25,52543	212	46,99709	286	20,07788
65	43,51330	139	31,39937	213	35,23214	287	*98,65317*
66	52,95671	140	24,71520	214	35,79498	288	35,51653
67	25,02931	141	33,60419	215	21,90231	289	21,42443
68	57,57026	142	23,64019	216	21,70399	290	60,02116
69	39,69289	143	23,58019	217	38,02696	291	32,71149
70	*77,18352*	144	33,77543	218	31,52531	292	55,46510
71	40,21554	145	17,11115	219	27,97875	293	54,90500
72	19,72228	146	51,57462	220	*71,63860*	294	14,38763
73	36,77291	147	38,40188	221	45,00458		
74	*111,30258*	148	39,10294	222	29,91330		

Fonte: Dados da pesquisa (2023).

A partir da observação da Tabela 5 verificou-se que os seguintes elementos podem ser classificados como *outliers* multivariados, os quais foram sublinhados e em itálico: 5, 8, 54, 56, 70, 74, 82, 89, 94, 95, 97, 101, 118, 136, 197, 200, 220, 232, 251, 260, 266 e 287. Esses 22 elementos da amostra foram descartados, o que traz como consequência a diminuição do número de observações de 294 para 272 casos.

A seguir é apresentada a metodologia aplicada à normalidade da amostra da pesquisa.

4.4.2 Normalidade

Como no formulário para a coleta de dados não existia a possibilidade de o respondente deixar alguma questão em branco, não houve a necessidade de se preocupar com os dados faltantes. Assim, a próxima etapa da análise de dados foi referente à verificação da normalidade da amostra.

Para esta dissertação, o exame da normalidade da amostra ocorreu por meio da aplicação do Teste de *Kolmogorov-Smirnov* (K-S). Assim, todas as variáveis que foram usadas para representar os construtos que formavam o modelo hipotético a ser testado foram examinados em termos da sua normalidade, ou não. O Teste K-S foi adotado, pois a amostra era formada por mais de 50 observações (Pestana & Gageiro, 2000).

A seguir é apresentada a metodologia aplicada para o *Common Method Bias* (CBM).

4.4.3 *Common Method Bias*

Outro aspecto avaliado em relação ao conjunto de dados da pesquisa foi o exame sobre a ocorrência do *Common Method Bias* (CMB), ou não. O CMB nada mais é que um viés que ocorre nas respostas preenchidas, quando o mesmo entrevistado é o responsável por responder questões relacionadas às crenças, percepções, atitudes e, no mesmo instrumento de coleta de dados, esse entrevistado responde a aspectos relacionados à sua intenção comportamental ou comportamento realizado (autorrelatado).

Nesse caso pode ocorrer um incremento da variância explicada dos construtos e das relações entre eles, por meio de uma maior padronização das respostas sobre os indicadores que representam esses construtos. Por conseguinte, construtos podem apresentar valores para a validade convergente inflados, ou ainda os valores das cargas fatoriais e das comunalidades dos indicadores também podem ser maiores que na realidade, como também as relações entre os construtos que são representadas por meio de hipóteses, que podem ser um incremento indevido.

Para que os problemas com a CMB possam ser eliminados ou minimizados, os responsáveis pela pesquisa devem usar técnicas de pesquisas que sejam eficientes contra a ocorrência do CMB. Essas técnicas incluem orientações para o preenchimento do questionário, a ordem das questões apresentadas para os entrevistados, mistura dos indicadores dos construtos ao longo do questionário, entre outras possibilidades.

Além disso, o pesquisador também pode realizar testes estatísticos para averiguar a ocorrência ou não do *Common Method Bias*. Neste estudo o *Harman's Single-Factor Test* foi o procedimento escolhido. Ressalta-se que esse é o teste mais utilizado para verificar a existência do CMB (Fuller, Simmering, Atinc, Atinc & Babin, 2016).

O *Harman's Single-Factor Test* é basicamente um teste no qual o pesquisador realiza uma análise fatorial exploratória, inserindo na análise todos os indicadores de todos os construtos presentes no modelo hipotético a ser testado. Além disso, essa análise fatorial

exploratória é parametrizada para que ela, ao seu final, gere somente um fator. Esse único fator deve apresentar um valor de até 50% para o indicador da variância explicada. Assim, pode-se afirmar que o *Common Method Bias* não é um aspecto preocupante em relação aos dados coletados (Fuller, Simmering, Atinc, Atinc & Babin, 2016; P. Podsakoff, MacKenzie, Lee & N. Podsakoff, 2003).

A seguir é apresentada a metodologia aplicada para as características da amostra.

4.4.4 Características da amostra

Para análise das características da amostra foram realizados os cálculos da frequência absoluta e da frequência relativa.

A seguir é apresentada a metodologia aplicada na análise descritiva da amostra.

4.4.5 Estatística descritiva

A próxima etapa da análise de dados diz respeito à análise descritiva dos resultados obtidos por meio da análise de frequências.

Essa análise é importante para o conhecimento acerca da percepção dos respondentes acerca dos comportamentos de prevenção e de risco ao usar a internet, principalmente em relação aos seus dados e informações pessoais. Além disso, também são analisados os indicadores de cada um dos construtos usados nesta dissertação.

Dessa forma, além da média de cada construto e de cada indicador, é possível também identificar o padrão de respostas de cada uma das opções de respostas disponíveis para os respondentes.

Nesta pesquisa especificamente foram analisados alguns comportamentos que os respondentes apresentavam ou não. Posteriormente, foram detalhados os 4 construtos presentes no modelo testado nesta dissertação.

A seguir é apresentada a metodologia aplicada na análise da unidimensionalidade.

4.4.6 Unidimensionalidade

Para que o modelo hipotético possa ser testado, é necessário garantir que os construtos que formam esse modelo sejam unidimensionais, ou seja, que sejam formados por somente uma dimensão ou fator. Para que isso possa ser verificado, é necessária a realização da técnica de análise estatística multivariada, conhecida como análise fatorial exploratória (AFE), técnica

adequada para esse tipo de verificação – além de outros usos - em relação aos construtos.

Inicialmente, é preciso considerar que três pressupostos devam ser satisfeitos para que os resultados obtidos sejam classificados como válidos. Assim, é preciso que o Teste de Esfericidade de Bartlett seja realizado e que o resultado seja menor que 0,05 (Malhotra, Nunan & Birks, 2017; Morgan & Griego, 1998).

Outro teste que precisa ser efetuado é o Teste de *Kaiser-Meyer-Olkin* (KMO), o qual apresenta como resultado a Medida de Adequacidade da Amostra (MSA). O valor de referência para este teste é de no mínimo 0,700. Contudo, em situações nas quais novas escalas estão sendo desenvolvidas, valores de pelo menos 0,600 também são considerados adequados (Hair, Black, Babin, Anderson e Tatham (2009).

Outro pressuposto é sobre o nível de correlação que deve existir entre os indicadores que formam cada um dos construtos. Mais especificamente, os indicadores devem apresentar um alto nível de correlação entre si, de forma que elas sejam iguais ou superiores a 0,300. Preferencialmente, todos os indicadores devem ser correlacionados entre si (Hair, Black, Babin, Anderson & Tatham, 2009).

Ao realizar a análise fatorial exploratória, o pesquisador possui uma série de métodos de extração dos fatores. Nesta dissertação, como o objetivo é o de identificar somente se cada um dos construtos é formado por somente um fator – isso é equivalente a tentar gerar um índice ou indexador –, o método adequado é o de fatoração pelos componentes principais (Hair, Black, Babin, Anderson & Tatham, 2009).

Outro aspecto a ser salientado é sobre a escolha do método de rotação. Isso ocorre quando o construto apresenta mais de um fator. Para facilitar o processo de visualização por parte dos pesquisadores, caso isso ocorra, o método de rotação ortogonal do método varimax será utilizado.

A seguir é apresentada a metodologia aplicada na análise da confiabilidade.

4.4.7 Confiabilidade

Após ter a confirmação sobre a unidimensionalidade dos construtos que formam o modelo hipotético, é necessário verificar se as escalas usadas para mensurar esses construtos são confiáveis, ou seja, se os resultados alcançados a partir da aplicação da escala são distintos para respondentes que possuem opiniões ou percepções diferentes acerca de um determinado comportamento, assunto ou objeto. Por conseguinte, a escala utilizada para medir um construto deve ser capaz de representar as diferenças apresentadas entre os respondentes ao longo do

tempo e sobre o tema que está sendo avaliado.

Neste estudo, optou-se por utilizar o indicador do *Alpha de Cronbach* (AC) para avaliar a confiabilidade de cada uma das escalas usadas. O valor do *Alpha de Cronbach* varia entre 0 e 1 e quanto maior o valor, maior é o nível de confiabilidade da escala (Malhotra, Nunan & Birks, 2017).

Em relação aos valores de referência, o valor mínimo aceitável deve ser de 0,700, sendo que nas situações em que a escala esteja em desenvolvimento e ainda em testes, os valores de até 0,600 também podem ser considerados aceitáveis (Pestana & Gageiro 2000; Hair, Black, Babin, Anderson & Tatham, 2009; Morgan & Griego, 1998).

A seguir é apresentada a metodologia aplicada na análise da validade convergente.

4.4.8 Validade convergente

Após a verificação da confiabilidade de cada uma das escalas utilizadas para medir os construtos que formam o modelo hipotético a ser testado, o passo seguinte da análise de dados refere-se à averiguação da validade convergente de todos os construtos.

Assim, além do construto ser unidimensional e da escala usada para medi-lo ser confiável, é necessário que o construto apresente a validade convergente. Isso significa que os indicadores usados para medir os construtos, realmente possuam relações consistentes entre si, de tal forma que os pesquisadores tenham a certeza de que esses indicadores representam uma única concepção ou essência.

Para que isto seja possível, os indicadores relacionados a um construto devem possuir altos valores das cargas fatoriais em relação ao construto. Assim, pode-se considerar que o construto realmente pode ser representado pelo grupo de indicadores (Hair, Black, Babin, Anderson & Tatham, 2009; Malhotra, Nunan & Birks, 2017; Bagozzi, Yi & Phillips, 1991).

Para que o exame da existência ou não da validade convergente para cada um dos construtos é necessário calcular o valor da variância média extraída (AVE) e o valor da confiabilidade composta (CC).

A variância média extraída - como apresentado em seu nome – representa a média da variância que todos os indicadores em conjunto são capazes de explicar em relação à variância do construto. Para calcular esse valor é necessário calcular o valor da carga fatorial de cada um dos indicadores em relação ao construto, elevar esse valor ao quadrado – representando a variância – e somar cada um deles. Ao final, o pesquisador deve dividir esse valor da soma ao quadrado das cargas fatoriais de cada um dos indicadores pelo número de indicadores.

O valor de referência para a variância média extraída é de pelo menos 0,500. Assim, tem-se a garantia que o conjunto de indicadores é capaz de explicar mais da metade da variância do construto como um todo. Em suma, a variância explicada será sempre maior que a variância não explicada (Hair, Black, Babin, Anderson & Tatham, 2009).

No caso da confiabilidade composta, esse parâmetro representa a consistência interna dos indicadores que constituem o construto. Para calcular a confiabilidade composta, além do valor da carga fatorial de cada um dos indicadores, também é considerado o valor do erro de mensuração de todos eles. O valor considerado como adequado para a confiabilidade composta é de 0,700 ou superior (Hair, Black, Babin, Anderson & Tatham, 2009).

A seguir é apresentada a metodologia aplicada na análise da validade discriminante.

4.4.9 Validade discriminante

O próximo tópico da análise de dados é referente à verificação da validade discriminante entre os construtos que formam o modelo hipotético.

Mais especificamente, além de todas as verificações já efetuadas – relativas à unidimensionalidade dos construtos, à confiabilidade das escalas utilizadas, à validade convergente de cada um dos construtos – é preciso também garantir que os construtos sejam distintos entre si, ou seja, que eles não sejam redundantes e que realmente representem conceitos distintos. Isso é averiguado por meio da verificação da validade discriminante.

Assim, uma situação positiva para que exista a validade discriminante é a que os valores das AVEs – variância média extraída – seja o mais alto possível e que os valores das correlações entre os construtos sejam os mais baixos possíveis (Hair, Black, Babin, Anderson & Tatham, 2009; Kline, 2005; Malhotra, Nunan & Birks, 2017; Bagozzi, Yi & Phillips, 1991).

A maneira escolhida para o exame da ocorrência ou não da validade discriminante ocorre inicialmente por meio do cálculo dos valores das correlações entre todos os construtos. O valor da correlação entre os pares de todos os construtos presentes no modelo hipotético deve ser menor que os dois valores das AVEs dos construtos que formam o par. Caso isso ocorre, então existe a validade discriminante entre o par de construtos. Assim, quanto menor for o valor da correlação entre os construtos e quanto maior for o valor da AVE dos construtos, maior a possibilidade da existência da validade discriminante (Hair, Black, Babin, Anderson & Tatham, 2009).

Outro aspecto a ser considerado é que o valor da correlação entre um par de construtos não deve exceder o valor de 0,85. Assim, mesmo que os valores das AVEs dos dois construtos

sejam superiores ao valor da correlação entre eles, haverá violação da validade discriminante, caso o valor dessa correlação seja superior a 0,85, pois é considerado um valor muito alto para representar dois construtos conceitualmente diferentes (Anderson & Gerbing, 1988).

O valor das AVEs de cada construto a ser considerado nesta etapa da validade discriminante já foi calculado na etapa de verificação da validade convergente. Para tal, foram realizadas modelagens de equações estruturais para cada um dos construtos.

A seguir é apresentada a metodologia aplicada na análise da validade nomológica.

4.4.10 Validade nomológica

A última etapa da análise de dados é efetivamente realizar o teste da validade nomológica do modelo hipotético, a qual examina se as relações de causa e efeito presentes na cadeia nomológica representada pelos construtos, apresenta relações estatisticamente significativas e com o mesmo sentido descrito nas definições das hipóteses (Malhotra, Nunan & Birks, 2017).

Para realizar a averiguação da validade nomológica do modelo é necessário usar a técnica estatística multivariada denominada modelagem de equações estruturais (SEM), a qual é capaz de realizar simultaneamente o cálculo de diversas regressões lineares representando a cadeia nomológica, bem como também diversas análises fatoriais. Dessa forma o pesquisador é capaz de testar e validar modelos hipotéticos, os quais em algumas situações representam uma sequência de causa e efeito por meio de um conjunto de hipóteses. Antes da SEM, o pesquisador precisava realizar individualmente as análises fatoriais, bem como um conjunto de regressões lineares.

A partir da modelagem de equações estruturais, o pesquisador pode verificar se as relações entre os construtos definidas no modelo hipotético são estatisticamente significativas. Dessa forma, o pesquisador tem a capacidade de verificar a ocorrência da validade nomológica ou não (Hair, Black, Babin, Anderson & Tatham, 2009; Kline, 2005).

Em relação à modelagem de equações estruturais, uma das decisões a serem tomadas é sobre a escolha do método de estimação a ser utilizado. No caso dessa dissertação escolheu-se o método de estimação *Maximum Likelihood* (ML), o qual é robusto em relação à violação da normalidade e também é adequado para os cálculos usando variáveis paramétricas ou não-categóricas (Hair, Black, Babin, Anderson & Tatham, 2009).

5 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Para a análise dos 294 questionários coletados procedeu-se à análise descritiva das variáveis e a análise multivariada dos dados.

5.1 Normalidade

Inicialmente, para análise dos dados realiza-se a verificação da normalidade da amostra, em relação às todas as variáveis paramétricas – numéricas – que fazem parte dos construtos pesquisado. Conforme exposto na Metodologia, nesta pesquisa é aplicado o Teste de *Kolmogorov-Smirnov* (K-S) com essa finalidade.

Para o Teste de K-S, a Tabela 6 apresenta os resultados alcançados.

Tabela 6

Resultados do teste de Kolmogorov-Smirnov (continua)

Código	Questão	Estatística	Sig.
Dow1	Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital.	0,209	0,000
Dow2	Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger.	0,189	0,000
Dow3	Utilizo palavras-passes diferentes para fazer *login* em dispositivos da escola ou do trabalho ou de *lanhouse*.	0,206	0,000
Dow4	Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais.	0,158	0,000
Dow5	Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	0,175	0,000
Dow6	Desconfio de mensagens recebidas de desconhecidos.	0,413	0,000
Dow7	Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas.	0,188	0,000
Dow8	Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos.	0,281	0,000
Dow9	Antes de abrir mensagem ou documentos que recebo pelo *WhatsApp* ou *e-mail* verifico a confiabilidade da informação.	0,281	0,000
Dow10	A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital.	0,283	0,000

Tabela 6

Resultados do teste de Kolmogorov-Smirnov (continua)

Código	Questão	Estatística	Sig.
Dow11	Tomo precauções para que meus dados não sejam roubados digitalmente.	0,248	0,000
Mid1	Os pais acompanham seus filhos enquanto esses utilizam a internet.	0,229	0,000
Mid2	As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus *sites.*	0,331	0,000
Mid3	A escola é responsável pela educação digital de seus alunos.	0,200	0,000
Mid4	As empresas monitoram os comportamentos suspeitos em seus *sites.*	0,196	0,000
Mid5	As pessoas sabem denunciar crimes cibernéticos.	0,229	0,000
Mid6	As empresas são as principais responsáveis por um ambiente digital seguro.	0,217	0,000
Mid7	As pessoas, em geral, deixam suas senhas salvas nos sites de compras, para facilitar acessos futuros.	0,253	0,000
Mid8	As empresas usam os dados pessoais de seus clientes com transparência.	0,153	0,000
Ups1	A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet.	0,160	0,000
Ups2	O governo brasileiro promove leis para um ambiente seguro da internet.	0,164	0,000
Ups3	Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.	0,247	0,000
Ups4	É fácil denunciar um crime cibernético.	0,179	0,000
Ups5	O governo é o principal responsável por um ambiente digital seguro.	0,151	0,000
Ups6	O governo promove campanhas sobre segurança na internet.	0,179	0,000
Ups7	O governo oferece recursos educativos digitais para a segurança na internet.	0,179	0,000
Ups8	Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.	0,277	0,000
Seg1	Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital.	0,179	0,000
Seg2	As pessoas tomam precauções quando utilizam um Wi-Fi público.	0,221	0,000

Tabela 6

Resultados do teste de Kolmogorov-Smirnov (concluso)

Código	Questão	Estatística	Sig.
Seg3	Em geral, as pessoas utilizam palavras-passes diferentes para fazer login em dispositivos diferentes do seu pessoal.	0,192	0,000
Seg4	As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	0,238	0,000
Seg5	As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.	0,285	0,000
Seg6	As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.	0,171	0,000
Seg7	Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.	0,222	0,000
Seg8	As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.	0,192	0,000
Seg9	As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.	0,168	0,000
Seg10	Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente.	0,194	0,000

Fonte: Dados da pesquisa (2023)

A partir dos dados apresentados na Tabela 6 foi possível concluir que a amostra não possui distribuição normal em virtude que todos os indicadores testados possuem um p-valor igual a 0.000. Isso mostra a rejeição da hipótese Ho, a qual preconiza que o indicador segue uma distribuição normal. Isso ocorreu para todas as variáveis testadas.

Por conseguinte, é necessário considerar que todas as técnicas de estatística multivariadas devem ser robustas em relação às características de violação da normalidade da amostra.

A seguir apresenta-se a análise do *Common Method Bias* (CMB).

5.2 *Common Method Bias*

Esta seção refere-se à ocorrência do CMB ou não. O resultado apurado para a variância explicada com a análise fatorial gerando um único fator foi de 27,73%. Assim, o CMB não foi um aspecto preocupante em relação à amostra utilizada.

A seguir apresenta-se a caracterização da amostra.

5.3 Características da amostra

Esta seção refere-se à descrição das características da amostra. Assim, foram apresentadas as principais características demográficas dos respondentes que compõem a amostra da pesquisa.

A amostra é composta na maioria dos respondentes do gênero masculino – mais de 54% -, as mulheres representam 43,8% e 1,8% preferiu não responder.

Em relação à faixa etária, o maior grupo de respondentes possui entre 26 e 40 anos com 41,9% de todos os entrevistados. Os outros dois grupos apresentam resultados muito similares com 27,9% para quem tem entre 18 anos e 25 anos e de 27,6% para os indivíduos com idade entre 41 e 60 anos. O grupo com idade acima de 60 anos representa 2,6% da amostra.

Do total de respondentes desta pesquisa 11,4% afirmam não trabalharem e não ter renda e 10,7% não trabalham e são estudantes. Nesse sentido, ressalta-se que a maioria (30,5%) dos respondentes estão na faixa de renda mensal entre 1.401 reais e 8.400 reais, 25,7% possuem renda na faixa de 4.201 reais até 8.400 reais, 12,1% da amostra recebem até 1.400 reais, 8,1% possuem renda na faixa de 8.401 reais até 14.000 reais, 0,7% possuem renda de 14.001 reais até 28.000 reais e 0,7% possuem renda acima de 28.000 reais.

Também, 97,8% da amostra possui internet em casa e majoritariamente reside em Minas Gerais (mais de 77% de todos os respondentes).

No caso da escolaridade da amostra, o maior grupo é formado por aqueles que estão fazendo um curso superior e por aqueles que já terminaram – 39,0%. Em seguida por aqueles com o ensino médio completo ou incompleto representados por 27,2% de todos os entrevistados, 18,4% da amostra com pós-graduação *latu sensu* ou MBA, 8,8% possuem mestrado ou doutorado e 6,6% têm ensino fundamental completo ou incompleto.

Sobre o maior nível de escolaridade das pessoas que moram com o respondente, os valores dos resultados mudam um pouco, mas os dois grupos principais de respondentes continuam sendo formados por aqueles com o ensino superior concluído ou em incompleto (28,7%) em conjunto com aqueles que já terminaram o ensino médio ou que também estavam incompletos (23,9%). Em seguida por 15,1% da amostra com pós-graduação latu sensu ou MBA, 5% com mestrado ou doutorado e 9,2% têm ensino fundamental completo ou incompleto. Ressalta-se que para essa questão, 17,6% das pessoas moram sozinhas, o que diminui o valor absoluto e relativo das opções de escolaridade possíveis.

A seguir apresenta-se a análise descritiva dos resultados.

5.4 Estatística descritiva

Esta seção refere-se à estatística descritiva da amostra. Os resultados são mostrados pela Tabela 7 a seguir.

Tabela 7

Percepções sobre o uso de informações oriundas da internet (continua)

Comportamento	Opções	Frequência	Percentagem
Frequência com que usa os dispositivos com internet	Nunca	0	0%
	Pelo menos uma vez por semana	0	0%
	Duas a quatro vezes por semana	7	2,6%
	A maior parte dos dias	41	15,1%
	Todos os dias	224	82,4%
	TOTAL GERAL	**272**	**100,00%**
Sabe quando suspeitar das informações que encontra.	Sempre	69	25,4%
	Quase sempre	145	53,3%
	Às vezes	56	20,6%
	Nunca	2	,7%
	TOTAL GERAL	**272**	**100,00%**
Consegue identificar se uma fonte de informação é confiável	Sempre	52	19,1%
	Quase sempre	151	55,5%
	Às vezes	64	23,5%
	Nunca	5	1,8%
	TOTAL GERAL	**272**	**100,00%**
Descarta informações indesejadas adequadamente	Sempre	141	51,8%
	Quase sempre	70	25,7%
	Às vezes	55	20,2%
	Nunca	6	2,2%
	TOTAL GERAL	**272**	**100,00%**
É capaz de comparar informações de diferentes sites, de acordo com sua utilidade	Sempre	109	40,1%
	Quase sempre	87	32,0%
	Às vezes	67	24,6%
	Nunca	9	3,3%
	TOTAL GERAL	**272**	**100,00%**
Participa de sites que publicam informações que lhe interessam para o seu trabalho ou hobbies	Sempre	128	47,1%
	Quase sempre	66	24,3%
	Às vezes	66	24,3%
	Nunca	24	8,8%
	TOTAL GERAL	**272**	**100,00%**

Tabela 7

Percepções sobre o uso de informações oriundas da internet (concluso)

Comportamento	Opções	Frequência	Percentagem
Ensino outras pessoas a avaliar criticamente as informações que elas acessam	Sempre	50	18,4%
	Quase sempre	66	24,3%
	Às vezes	122	44,9%
	Nunca	34	12,5%
	TOTAL GERAL	**272**	**100,00%**

Fonte: Dados da pesquisa (2023).

Em relação às percepções sobre o uso das informações oriundas da internet, verifica-se que 97,5% dos respondentes usam os dispositivos com internet todos os dias ou então a maior parte dos dias. Isso significa um alto uso da internet e que ela está presente na vida das pessoas conforme, também, aos resultados da Unicef (2013) que 69% dos adolescentes pesquisados informaram acessar a internet todos os dias.

Os dados apresentados nesta dissertação vão ao encontro de Cazelatto e Segatto (2020) que afirmam que as tecnologias disponíveis ao uso particular conectadas à internet se tornaram um instrumento imprescindível à vida de uma grande parcela da população mundial. Com a evolução da internet, a mobilidade permitiu que as rotinas das pessoas se conectassem ao mundo virtual para resolução instantânea das suas necessidades e para lazer.

Este resultado encontrado corrobora, também, o Relatório Global de Estatísticas de 2022 do site *DataReportal* que afirma que 67,1% da população mundial usam um celular, tendo crescido mais de 1,8% no ano passado. Também, informa que 62,5% da população total do mundo usam a internet, tendo crescido mais de 4% no ano passado. Além de mostrar que 58,4% da população total do mundo usam as mídias sociais, tendo crescido mais de 10% nos últimos doze meses.

Em relação ao crescimento dos internautas, esse número mais que dobrou nos últimos dez anos. Quanto ao tempo navegando, em geral no mundo, o usuário gasta quase 7h na internet e os brasileiros gastam 10h diariamente na internet (DataReportal, 2022). Esses fados reforçam o resultado desta pesquisa.

No caso dos comportamentos de prevenção e de cuidado sobre as informações oriundas da internet, constatou-se que a grande maioria das pessoas – quase 80% - avaliou que sempre ou quase sempre sabiam quando suspeitar das informações que encontravam, bem como conseguiam descartar as informações indesejadas de forma adequada. Esse resultado foi parecido com a percepção sobre se as pessoas conseguiam identificar se uma fonte de

informação era confiável, na qual mais de 74% consideravam que isso era possível sempre, ou quase sempre.

Em relação à capacidade de navegação na internet quanto a verificar se as informações encontradas são verdadeiras, de acordo com Smahel (2020), os resultados obtidos em 19 países europeus com respondentes entre 9 a 16 anos, mostram que 16% (Suíça) a 43% (Lituânia) sentem confiantes, 18% (Alemanha) a 39% (Estônia, Finlândia, Noruega) sentem um pouco de confiança e, de 30% (Finlândia) a 64% (Espanha) não sentem confiança ou não sabem informar.

Não obstante, nesta dissertação os resultados apresentaram-se melhores quanto à capacidade de identificar se a informação é confiável. Segundo Smahel (2020), essa habilidade de navegação e confiabilidade na precisão da informação *online* é importante para o uso da internet para educação, cidadania e participação.

Entretanto, Cardoso (2020) afirma que pelas redes sociais é possível falsear a realidade, dificultando ao indivíduo perceber a verdade nas informações disponibilizadas na internet. Também, as reais informações podem ser ignoradas, mesmo que se tenha acesso a elas, ou se escolha a que lhe é mais confortável.

Conforme as estatísticas apresentadas na revisão de literatura pela Safernet (2023a) sobre a magnitude do cibercrime, o número de ocorrências cresceu no Brasil, assim como novos tipos de ataques. Essa confiança nas informações encontradas pode ser questionada diante dos demais indicadores apresentados quanto à proeficiência digital.

Outro aspecto a ser destacado foi que mais de 70% dos respondentes acreditavam que sempre, ou quase sempre, eram capazes de comparar informações de diferentes sites, de acordo com sua utilidade. Apesar desses comportamentos, a maioria das pessoas não ensinava outras pessoas a avaliar criticamente as informações que elas acessavam. A maioria das respostas foram para as opções “somente às vezes” ou “nunca”.

Sobre a participação em sites que publicavam informações que lhe interessavam para o seu trabalho ou *hobbies*, novamente pouco mais de 48% dos respondentes apresentaram esse tipo de comportamento de às vezes ou quase sempre. Nesse caso, mais de 47% dos entrevistados faziam isso sempre.

A literacia digital está relacionada com as habilidades em usar as ferramentas digitais. De acordo com o *Programme for the Internacional Assessement of Adult Competencies* – PIAAC (National Center for Education Statisics, 2021), o nível de literacia está relacionado à idade. Europeus acima dos 45 anos entrevistados apresentaram média menor do nível de literacia quando comparados com indivíduos mais jovens.

Outra associação encontrada na pesquisa do PIAAC foi com o nível escolar. Quanto maior o tempo de estudo, maior o nível de proeficiência digital. Também, há correlação entre o nível de literacia e a propensão para a participação educativa, formativa e social. Quanto maior o nível de proeficiência digital, maior o nível de confiança para participação em atividades educativas, formativas e sociais.

Os resultados encontrados nesta pesquisa contrariam parcialmente ao PIAAC que já foi aplicada em mais de trinta países. Nesta dissertação, cerca de 66% dos respondentes estão abaixo dos 45 anos e têm ensino médio ou superior completo ou incompleto. Entretanto, grande parte respondeu que não ensinavam outras pessoas a avaliar criticamente as informações que elas acessavam ou não publicavam em sites informações que lhes interessavam para o seu trabalho ou *hobbies*, ou seja, uma não participação educativa, formativa e social.

Pode-se afirmar que esses resultados estão associados à um nível de proeficiência digital baixo ou intermediário. A avaliação da literacia digital compreende oito níveis, sendo dois para cada nível básico, intermediário, avançado e altamente especializado. As atividades que envolvem orientar outros e adaptar-se a outros estão no nível acima do nível intermediário (Carretero, Vuorukari & Punie, 2017).

Além disso, os resultados mostraram que conseguem executar atividades complexas como suspeitar de informações, identificar uma informação não confiável e comparar informações. Parecem atividades simples, mas, conforme as estatísticas apresentadas na revisão de literatura, os crimes de extorsão, de roubo de identidade, de violação dos dados pessoais, de não-pagamento e não-*delivery*, de ataques *phishing* , *vishing*, *smishing* e *pharming* (FBI, 2022) são os mais praticados. Esses crimes estão todos relacionados à não prática dessas atividades.

Outro ponto analisado nesta dissertação versa sobre o meio de como os respondentes adquiriram os seus atuais conhecimentos sobre tecnologias de informação e de comunicação.

A Tabela 8 a seguir mostra esses resultados obtidos.

Tabela 8

Meio de como os respondentes adquiriram os seus atuais conhecimentos sobre tecnologias de informação e de comunicação

Comportamento	Frequência	Percentagem
Tenho habilidades de TI muito básicas	97	30,70%
Sou autodidata (recursos disponíveis na web, experiência prática…)	121	38,22%
Em serviços públicos abertos de formação (telecentros)	29	9,20%
Nos centros públicos de formação profissional não regulamentados	10	3,20%
Em centros de treinamento privados	59	18,67%
TOTAL GERAL[1]	**316**	**100,00%**

Nota: para estas questões, o respondente podia marcar mais de uma opção. Por isso, o valor total de respostas é de 316 respostas e não de 272 que corresponde ao tamanho da amostra usada na dissertação.
Fonte: Dados da pesquisa (2023).

As duas opções de respostas, que representaram quase 70% da escolha do total de respondentes, indicaram que as pessoas consideram, em grande número, que estudaram e aprenderam sozinhas sobre informática e segurança na web. Todavia, quase 1/3 dos respondentes consideraram que as suas habilidades em tecnologia da informação eram muito básicas.

De acordo com Wicht, Reder e Lechner (2021), os resultados em duas pesquisas alemãs do *National Educational Panel Study* (NEPS) e PIAAC mostraram que as habilidades de TIC nos adultos estão relacionadas ao "aprender fazendo em casa e no trabalho". Além disso, esses autores afirmam que a habilidade de alfabetização está fortemente relacionada às habilidades na aquisição e no sucesso com as TIC. Esses dados sustentam o resultado obtido nesta dissertação.

Em relação ao compartilhamento de informações e de conteúdo digital com outras pessoas, o comportamento dos respondentes pode ser visto na Tabela 9.

Tabela 9

Compartilhamento de informações e de conteúdo digital

Comportamento	Opções	Frequência	Percentagem
Usa *e-mail* para compartilhar conteúdo digital: documentos, fotos, vídeos, etc.	Sim	173	63,6%
	Não	99	36,4%
TOTAL GERAL		**272**	**100,00%**
Usa ferramentas online para compartilhar esses conteúdos: *Google Drive, Scribd, Slide share, Instagram…*	Sim	229	84,2%
	Não	43	15,8%
TOTAL GERAL		**272**	**100,00%**
Participa de redes sociais e fóruns *online* para compartilhar conhecimento	Sim	185	68,0%
	Não	87	32,0%
TOTAL GERAL		**272**	**100,00%**
Tem um canal no qual publico meus conteúdos e recebo comentários dos leitores	Sim	59	21,7%
	Não	213	78,3%
TOTAL GERAL		**272**	**100,00%**
Através da internet, colabora com outras pessoas da sua área educacional ou profissional (minha rede pessoal de aprendizagem ou PLN)	Sim	115	42,3%
	Não	157	57,7%
TOTAL GERAL		**272**	**100,00%**
Encorajo e ensino outras pessoas a usar ferramentas digitais para trocar informações e conteúdo	Sim	153	56,3%
	Não	119	43,8%
TOTAL GERAL		**272**	**100,00%**

Fonte: Dados da pesquisa (2023).

Ao analisar a Tabela 9, é possível verificar que os respondentes apresentam um alto nível de compartilhamento de informações pela internet. Mais especificamente, a grande maioria dos entrevistados utiliza ferramentas *online* para compartilhar os seus conteúdos: *Google Drive, Scribd, Slide share, Instagram*…, além de participar de redes sociais e fóruns *online* para compartilhar conhecimento. A maioria dos indivíduos também usa e-mail para compartilhar conteúdo digital: documentos, fotos, vídeos, etc. e incentiva outras pessoas a usar ferramentas digitais para trocar informações e conteúdo.

Todavia, a maioria dos respondentes não tem um canal no qual se publicam seus conteúdos e recebem comentários dos leitores e, também, a maioria não colabora com outras pessoas da sua área educacional ou profissional. A explicação para esse resultado pode ser fruto que a maioria dos respondentes utiliza o compartilhamento de informações pela internet para lazer e entretenimento.

Os resultados encontrados são similares aos encontrados na literatura. De acordo com a Unicef (2013) quanto às ferramentas mais usadas, 59% dos adolescentes pesquisados utilizavam *e-mail* e 84% as redes sociais. Também, 66% disponibilizavam fotos na internet.

Segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD) do Instituto Brasileiro de Geografia e Estatística (IBGE, 2018, 2020, 2022), no período de 2016 a 2021, o percentual variou de 69,3 a 62 entre os entrevistados que usam o *e-mail* para compartilhar informações e 94,2 a 94,9 usam algum aplicativo diferente de e-mail para enviar ou receber mensagens de texto, voz ou imagens. Também, de acordo com a pesquisa do Instituto de Computação da UFMT (Soares, Araújo & Souza, 2020) sobre conscientização e sensibilização sobre os riscos na *web*, 60,2% raramente postam alguma coisa nas redes sociais.

Essas pesquisas do IBGE (2018, 2020, 2022) e da UFMT (Soares, Araújo & Souza,2020) reforçam os resultados apresentados nesta pesquisa, mostrando uma tendência do uso de aplicativos tanto para atividades de lazer como para disseminação de notícias, enquanto ocorre o desuso do e-mail para enviar e receber mensagens formais na sociedade.

Quanto ao uso dos dispositivos digitais os resultados estão na Tabela 10.

Tabela 10

Uso dos dispositivos digitais

Comportamento	Opções	Frequência	Percentagem
Usa antivírus e faz atualizações	Sim	220	80,9%
	Não	52	19,1%
TOTAL GERAL		**272**	**100,00%**
É cauteloso ao receber mensagens cujo remetente ou anexo não conhece (SPAM)	Sim	249	91,5%
	Não	23	8,5%
TOTAL GERAL		**272**	**100,00%**
Usa senhas diferentes para seus dispositivos e serviços digitais e as modifica periodicamente	Sim	172	63,2%
	Não	100	36,8%
TOTAL GERAL		**272**	**100,00%**
Troca periodicamente a chave da rede Wi-Fi da sua casa	Sim	68	25,0%
	Não	204	75,0%
TOTAL GERAL		**272**	**100,00%**
Ajudo pessoas próximas a mim a evitar riscos de segurança com os dispositivos	Sim	175	64,3%
	Não	97	35,7%
TOTAL GERAL		**272**	**100,00%**

Fonte: Dados da pesquisa (2023).

Sobre o uso dos dispositivos digitais, a pesquisa mostrou que a grande maioria dos respondentes apresentava um comportamento cauteloso e preventivo. Somente o aspecto relacionado a trocar a senha da rede Wi-Fi da sua residência apresentou um baixo nível de ocorrência. A causa desse fenômeno pode ser de interesse para os gestores da área de Tecnologia da Informação (TI). Assim, novas pesquisas que busquem conhecer as suas causas podem ensejar mudanças nos dispositivos atuais, bem como o conteúdo a ser difundido entre os indivíduos para uma melhor orientação sobre o comportamento de trocar a senha do seu Wi-Fi residencial.

Os resultados da dissertação corroboram os estudos de Castillejos Lópes, Torres Gastelú e Lagunes Domínguez (2016) que, investigando a segurança digital entre jovens, encontraram que 77% possuem antivírus instalado que executam e atualizam regularmente, 69% utilizam senhas diferentes para acessar dispositivos e serviços digitais, além de realizarem a troca das senhas periodicamente. Esses mecanismos básicos de proteção são inegáveis na segurança da informação (Hall, 2016).

Também, resultados similares aos da Unicef (2013) apontam que 46% dos adolescentes responderam não adicionar desconhecidos em seu perfil, 51% utilizaram ferramentas de bloqueio de pessoas nas redes sociais, tendo 30% bloqueado para evitar acesso à informação, mostrando que têm o hábito de serem cautelosos.

A Tabela 11 mostra os resultados sobre a percepção dos respondentes em relação aos seus dados quando usa a internet.

Tabela 11

Sobre os dados na internet (continua)

Comportamento	Opções	Frequência	Percentagem
Sabe que os seus meus dados podem ser usados por outras pessoas	Sim	244	89,7%
	Não	28	10,3%
TOTAL GERAL		**272**	**100,00%**
Conhece o perigo de ser substituído na internet (roubo de identidade, chantagem, ...)	Sim	250	91,9%
	Não	22	8,1%
TOTAL GERAL		**272**	**100,00%**
Toma extremas precauções antes de fornecer informações pessoais pela internet (DN, endereço, idade, telefone, dados bancários / cartões de crédito, fotos pessoais, ...)	Sim	228	83,8%
	Não	44	16,2%
TOTAL GERAL		**272**	**100,00%**

Tabela 11

Sobre os dados na internet (concluso)

Comportamento	Opções	Frequência	Percentagem
Sabe que o Regulamento Geral de Proteção de Dados (GDPR) existe para proteger dados pessoais na internet	Sim	171	62,9%
	Não	101	37,1%
TOTAL GERAL		**272**	**100,00%**
Sabe quando uma página usada tem um certificado de segurança	Sim	178	65,4%
	Não	94	34,6%
TOTAL GERAL		**272**	**100,00%**
Saberia identificar páginas da *web* ou mensagens de *e-mail* com as quais pode ser enganado	Sim	193	71,0%
	Não	79	29,0%
TOTAL GERAL		**272**	**100,00%**
Participa de atividades para promover hábitos de proteção e privacidade	Sim	72	26,5%
	Não	200	73,5%
TOTAL GERAL		**272**	**100,00%**

Fonte: Dados da pesquisa (2023).

Sobre o comportamento preventivo e cauteloso dos internautas, a grande maioria em sua autoavaliação conhecia os perigos de navegar pela internet, sabia identificar esses perigos, além de tomar precauções sobre o fornecimento de informações pessoais. A exceção foi a participação em atividades para promover hábitos de proteção e privacidade. Assim, verificou-se que as pessoas tinham conhecimento e sabiam agir caso precisassem, mas não participavam de eventos para promover esses hábitos "tecnologicamente saudáveis".

Também, quanto à utilização dos dados pessoais por terceiros, esta dissertação obteve resultados similares ao estudo de Castillejos Lópes, Torres Gastelú e Lagunes Domínguez (2016) em que 90% dos jovens responderam ter conhecimento e levam em consideração os perigos e consequências de alguém na internet usar sua identidade digital.

Além disso, quanto às precauções antes de fornecer informações pessoais pela internet, os resultados são parecidos Castillejos Lópes, Torres Gastelú e Lagunes Domínguez (2016), pois grande maioria respondeu que toma extremas precauções.

Entretanto, resultados contrários a esta dissertação foram obtidos por Axier e Rainie que publicaram pesquisa na *Pew Research Center* (2019), tendo que 49% dos americanos dizem ter pouco ou 14% nenhum conhecimento sobre as regulamentações cibernéticas quanto à proteção dos dados.

O próximo passo da análise de dados, utilizando-se as técnicas descritivas univariadas,

foi a apresentação da frequência e do valor da média de cada um dos indicadores e dos seus respectivos construtos.

O primeiro dos quatro construtos a ser explorado foi a prática de *downstream* pelos respondentes. Os resultados foram exibidos na Tabela 12.

Tabela 12

Prática de downstream (continua)

Indicadores	Opções	Frequência	Percentagem
Sempre utiliza antivírus para verificar se há alguma ameaça em seu dispositivo digital	1	26	9,6%
	2	33	12,1%
	3	48	17,6%
	4	67	24,6%
	5	98	36,0%
MÉDIA INDICADOR		**3,65**	
TOTAL GERAL		**272**	**100,00%**
Quando utiliza Wi-Fi de locais públicos utiliza uma rede virtual pessoal (VPN) para se proteger	1	82	30,1%
	2	33	12,1%
	3	56	20,6%
	4	38	14,0%
	5	63	23,2%
MÉDIA INDICADOR		**2,88**	
TOTAL GERAL		**272**	**100,00%**
Utiliza palavras-passes diferentes para fazer *login* em dispositivos da escola ou do trabalho ou de *lanhouse*	1	64	23,5%
	2	27	9,9%
	3	47	17,3%
	4	41	15,1%
	5	93	34,2%
MÉDIA INDICADOR		**3,26**	
TOTAL GERAL		**272**	**100,00%**
Sabe propor novas ideias e processos para garantir a proteção de tecnologias digitais	1	69	25,4%
	2	41	15,1%
	3	76	27,9%
	4	41	15,1%
	5	45	16,5%
MÉDIA INDICADOR		**2,82**	
TOTAL GERAL		**272**	**100,00%**
Sabe onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais	1	76	27,9%
	2	39	14,3%
	3	44	16,2%
	4	47	17,3%
	5	66	24,3%
MÉDIA INDICADOR		**2,96**	
TOTAL GERAL		**272**	**100,00%**
Desconfia de mensagens recebidas de desconhecidos	1	15	5,5%
	2	4	1,5%
	3	20	7,4%
	4	38	14,0%
	5	195	71,7%
MÉDIA INDICADOR		**4,45**	
TOTAL GERAL		**272**	**100,00%**

Tabela 12

Prática de downstream (concluso)

Indicadores	Opções	Frequência	Percentagem
Sabe proteger seus dispositivos móveis do ataque de pessoas maliciosas	1	34	12,5%
	2	30	11,0%
	3	67	24,6%
	4	70	25,7%
	5	71	26,1%
MÉDIA INDICADOR		**3,42**	
TOTAL GERAL		**272**	**100,00%**
Suas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos	1	14	5,1%
	2	25	9,2%
	3	36	13,2%
	4	64	23,5%
	5	133	48,9%
MÉDIA INDICADOR		**4,02**	
TOTAL GERAL		**272**	**100,00%**
Antes de abrir mensagem ou documentos que recebe pelo *WhatsApp* ou *e-mail* verifica a confiabilidade da informação	1	29	10,7%
	2	24	8,8%
	3	36	13,2%
	4	51	18,8%
	5	132	48,5%
MÉDIA INDICADOR		**3,86**	
TOTAL GERAL		**272**	**100,00%**
A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital	1	19	7,0%
	2	17	6,3%
	3	44	16,2%
	4	58	21,3%
	5	134	49,3%
MÉDIA INDICADOR		**4,00**	
TOTAL GERAL		**272**	**100,00%**
Toma precauções para que seus dados não sejam roubados digitalmente	1	20	7,4%
	2	11	4,0%
	3	38	14,0%
	4	84	30,9%
	5	119	43,8%
MÉDIA INDICADOR		**4,00**	
TOTAL GERAL		**272**	**100,00%**
MÉDIA CONSTRUTO		**3,57**	

Nota: As âncoras utilizadas foram “1” para “Discordo Totalmente” e “5” para “Concordo Totalmente”.

Fonte: Dados da pesquisa (2023).

Em relação às práticas de *downstream*, os resultados mostraram que, em geral, a maioria dos respondentes agia de alguma forma para prevenir possíveis problemas de segurança. Isso se refletiu na média desse construto que foi de 3,57 pontos – com a escala variando de um a cinco pontos.

Outro ponto destacado foi que para os onze itens, a opção cinco que representa o maior nível de concordância com a afirmativa, foi a mais escolhida pelos respondentes, com exceção dos indicadores “quando utiliza Wi-Fi de locais públicos utiliza uma rede virtual pessoal (VPN)

para se proteger", "sabe propor novas ideias e processos para garantir a proteção de tecnologias digitais" e "sabe onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais". Isso significou que, dos onze indicadores desse construto, em oito deles a opção cinco foi a mais assinalada.

Os quatro indicadores que apresentaram o maior nível de concordância foram "desconfia de mensagens recebidas de desconhecidos", "suas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos", "a pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital" e "Toma precauções para que seus dados não sejam roubados digitalmente". Esse fato influenciou nos altos valores das médias desses indicadores, com 4,41, 4,02, 4,00 e 4,00 pontos, respectivamente. Além disso, as respostas assinaladas para as opções quatro e cinco, representaram mais de 70% para esses quatro indicadores.

Isso significa que as pessoas, em tese, eram desconfiadas e acreditavam que elas eram as responsáveis pela sua própria segurança – o que provavelmente reforça o seu nível de responsabilidade e de desconfiança, bem como outras atividades como escolher senhas adequadas – e buscavam criar senhas difíceis de serem descobertas pelos criminosos.

O alto percentual para o indicador contraria o estudo de Martins (2021) em que apenas 14% dos respondentes conferem a autenticidade das informações e 42,85% não conferem.

De outro lado, os já citados indicadores "quando utiliza Wi-Fi de locais públicos utiliza uma rede virtual pessoal (VPN) para se proteger", "sabe propor novas ideias e processos para garantir a proteção de tecnologias digitais" e "sabe onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais" foram aqueles que apresentaram os menores valores de média – 2,88, 2,82 e 2,96 respectivamente. Cabe ressaltar que esses valores médios foram abaixo do valor de três, ponto central da escala – mediana – entre um e cinco, o que significou um nível maior de discordância que de concordância pelos respondentes.

Isso significa que talvez faltou informação para essas pessoas saber como fazer as denúncias, além de utilizar as suas redes VPN em locais públicos. Nesse caso pode ser um problema de como fazer ou talvez essas pessoas nem sabiam desse tipo de risco. Por fim, houve ainda a auto percepção das pessoas sobre a sua incapacidade ou falta de vontade em propor soluções para melhorar a proteção das tecnologias digitais.

Os resultados obtidos nesta dissertação, quanto à proteção virtual são parcialmente semelhantes aos 4 estudos da *ySKILLS* realizados por Ponte, S. Batista e R. Baptista (2022) em Portugal com 1.017 adolescentes, por Kalmus, Opermann e Tikerperi (2022) na Estônia com 1.249 adolescentes, por Waechter, Stuhlpfarrer, Böttcher, Bernhardt e Kadera (2022) na

Alemanha com 1.086 adolescentes e por Mascheroni e Cino (2022) na Itália com 965 adolescentes. Esses apresentaram os seguintes resultados: 57% a 78% sabem bloquear *pop-ups* e anúncios indesejados, 60% a 68% sabem identificar se a informação *online* é verdadeira, 57 a 69% sabem avaliar se um *website* é de confiança, 53% a 74% sabem usar navegação privada, 72% a 95% sabem desligar a geolocalização nos dispositivos móveis, 73% a 83% sabem reportar conteúdos negativos sobre ele ou grupos a que pertence, 71% a 85% sabem reconhecer quando alguém está sendo alvo de *cyberbulling*, 60% a 91% sabem mudar a definição de privacidade, 94% a 98% sabem proteger um dispositivo com PIN, impressão digital e reconhecimento facial.

A prática de *midstream* foi o segundo construto a ser avaliado. Os valores alcançados foram mostrados pela Tabela 13.

Tabela 13

Prática de Midstream (continua)

Indicadores	Opções	Frequência	Percentagem
Os pais acompanham seus filhos enquanto esses utilizam a internet.	1	40	14,7%
	2	40	14,7%
	3	48	17,6%
	4	41	15,1%
	5	103	37,9%
MÉDIA INDICADOR		**3,47**	
TOTAL GERAL		**272**	**100,00%**
As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus *sites*.	1	9	3,3%
	2	15	5,5%
	3	35	12,9%
	4	58	21,3%
	5	155	57,0%
MÉDIA INDICADOR		**4,23**	
TOTAL GERAL		**272**	**100,00%**
A escola é responsável pela educação digital de seus alunos.	1	24	8,8%
	2	24	8,8%
	3	63	23,2%
	4	72	26,5%
	5	89	32,7%
MÉDIA INDICADOR		**3,65**	
TOTAL GERAL		**272**	**100,00%**
As empresas monitoram os comportamentos suspeitos em seus *sites.*	1	24	8,8%
	2	30	11,0%
	3	78	28,7%
	4	51	18,8%
	5	89	32,7%
MÉDIA INDICADOR		**3,56**	
TOTAL GERAL		**272**	**100,00%**

Tabela 13

Prática de Midstream (concluso)

Indicadores	Opções	Frequência	Percentagem
As pessoas sabem denunciar crimes cibernéticos.	1	96	35,3%
	2	78	28,7%
	3	46	16,9%
	4	26	9,6%
	5	26	9,6%
MÉDIA INDICADOR		**2,29**	
TOTAL GERAL		**272**	**100,00%**
As empresas são as principais responsáveis por um ambiente digital seguro.	1	22	8,1%
	2	23	8,5%
	3	68	25,0%
	4	58	21,3%
	5	101	37,1%
MÉDIA INDICADOR		**3,71**	
TOTAL GERAL		**272**	**100,00%**
As pessoas, em geral, deixam suas senhas salvas nos *sites* de compras, para facilitar acessos futuros.	1	34	12,5%
	2	18	6,6%
	3	30	11,0%
	4	73	26,8%
	5	117	43,0%
MÉDIA INDICADOR		**3,81**	
TOTAL GERAL		**272**	**100,00%**
As empresas usam os dados pessoais de seus clientes com transparência.	1	65	23,9%
	2	48	17,6%
	3	82	30,1%
	4	35	12,9%
	5	42	15,4%
MÉDIA INDICADOR		**2,78**	
TOTAL GERAL		**272**	**100,00%**
MÉDIA CONSTRUTO		**3,44**	

Nota: As âncoras utilizadas foram “1” para “Discordo Totalmente” e “5” para “Concordo Totalmente”.

Fonte: Dados da pesquisa (2023).

Em relação às práticas de *midstream*, os valores presentes na Tabela 13 mostraram que a grande maioria dos respondentes concorda com o conteúdo dos indicadores que formam o construto. Isso também foi possível de ser verificado pelo valor da média geral que foi de 3,44 pontos. Outro ponto que reforça essa conclusão foi que a opção cinco, que representa o maior nível de concordância pelos respondentes foi a mais escolhida para seis dos oito indicadores.

Quanto aos pais acompanharem seus filhos enquanto esses utilizam a internet, os resultados foram semelhantes (52%) ao da Unicef (2013) que 54% dos adolescentes responderam sim, terem controle pelos pais e 77% recorreriam aos pais caso sofressem algum tipo de violência virtual.

Em relação à escola ser responsável pela educação digital de seus alunos, Areepattamannil e Khine (2017) na pesquisa sobre características comportamentais e

motivacionais relacionadas à TIC com 56.209 jovens de 13 a 16 anos em 20 países revelou que a aprendizagem de tarefas de TIC na escola e o uso de TIC durante as aulas contribuíram positivamente na frequência para comunicação social. Também, Ilomäki e Rantanen (2007) mostraram que os usos de TIC nas aulas promovem o desenvolvimento de habilidades e aprimoram o conhecimento de TIC entre adolescentes. Além disso, constataram que a percepção de competência em TIC está ligada ao seu envolvimento social às TIC. Esses resultados dessas pesquisas revelam a importância da escola nesta era digital de interações sociais virtuais.

Analisando-se os itens que apresentaram o maior nível de concordância ("as empresas são responsáveis pela segurança da informação das pessoas que utilizam seus sites" com 4,23 pontos; "as pessoas, em geral, deixam suas senhas salvas nos sites de compras, para facilitar acessos futuros" com 3,81 pontos; e "as empresas são as principais responsáveis por um ambiente digital seguro" com 3,71 pontos) verificou-se que as pessoas - além de si próprias como ocorreu com o construto *downstream* – também consideraram que as empresas eram as responsáveis por um ambiente informacional seguro e protegido na internet. Isso também se refletiu na percepção dos consumidores quando eles deixam as suas senhas salvas em *sites* de compras. Quem controla esse ambiente são as empresas.

Os dois indicadores que mostraram discordância por parte dos respondentes – com média abaixo de três – foram "as pessoas sabem denunciar crimes cibernéticos" com média de 2,29 pontos e "as empresas usam os dados pessoais de seus clientes com transparência" com 2,78 pontos. No primeiro caso, o resultado foi coerente com o obtido para o construto *downstream*, para o qual o indicador onde as pessoas podem denunciar crimes cibernéticos, apresentou um maior nível de discordância.

Para o segundo indicador, as pessoas consideraram que falta transparência por parte das empresas sobre a utilização dos seus dados pessoais. Há de se ressaltar que a coleta de dados ocorreu na vigência da LGPD – Lei Geral de Proteção de Dados -, o que deveria contribuir para uma percepção mais positiva por parte dos respondentes. Novamente, esse resultado é importante em termos gerenciais, haja visto que o consumidor considera que a empresa também é responsável pela segurança dos dados e informações no ambiente digital.

Esses dados corroboram estudos de V. Silva (2015) que pesquisou sobre a preocupação com a privacidade na internet no Brasil, mostrando uma forte preocupação com as informações mais sensíveis quanto à privacidade para senhas (74%), número do cartão de crédito (73%), número da agência e da conta corrente (67%), saldo bancário (64%) e gastos com cartão de crédito (63%).

V. Silva (2015) também encontrou um grau elevado de preocupação entre 60% a 71% para os construtos relacionados à coleta de dados, ao uso secundário das informações fornecidas, ao acesso indevido dos dados, ao controle adequados sobre as informações pessoais na internet, sobre as práticas dos sites relativas à privacidade das informações. Por outro lado, quando analisado o grau de confiança nas empresas que coletam as informações na internet as respostas foram mais neutras até 25% a discordo totalmente acima de 50%, mostrando uma tendência de desconfiança.

De acordo com a pesquisa de Olmstead e Smith publicada na *Pew Research Center* (2017) com 1.040 adultos em 2016 sobre segurança cibernética, a maior parte dos respondentes sofreu roubo de dados ou fraude cibercrime. Também, consideram que seus dados estão menos seguros nos últimos tempos. Além disso, não confiam na proteção de seus dados para uso indevido pelas instituições que coletam na internet.

O relatório da Unisys (2021) revela que 49% dos respondentes confiam em seu banco para alertá-los de qualquer atividade suspeita e 34% confiam na sua operadora de telefonia para não liberar suas informações pessoais sem serem notificados.

Conforme Velho, (2016), Steinberg, (2020), CERT.br, NIC.br, CGI.br e ANPD (2021), é necessário a adoção de medidas para garantir a segurança dos dados sensíveis, tanto por parte do governo e das empresas quanto do indivíduo, família e amigos. Os dados pessoais e financeiros podem tanto serem acessados de forma ilegal por comerciantes quanto serem roubados ou até mesmo repassados sem autorização para outras empresas.

O próximo construto analisado foi *upstream* e os resultados foram mostrados na Tabela 14.

Tabela 14

Prática de Upstream (continua)

Indicadores	Opções	Frequência	Percentagem
A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet	1	59	21,7%
	2	62	22,8%
	3	83	30,5%
	4	35	12,9%
	5	33	12,1%
MÉDIA INDICADOR		**2,71**	
TOTAL GERAL		**272**	**100,00%**

Tabela 14

Prática de Upstream (concluso)

Indicadores	Opções	Frequência	Percentagem
O governo brasileiro promove leis para um ambiente seguro da internet.	1	53	19,5%
	2	57	21,0%
	3	84	30,9%
	4	51	18,8%
	5	27	9,9%
MÉDIA INDICADOR		**2,79**	
TOTAL GERAL		**272**	**100,00%**
Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.	1	22	8,1%
	2	29	10,7%
	3	47	17,3%
	4	58	21,3%
	5	116	42,6%
MÉDIA INDICADOR		**3,80**	
TOTAL GERAL		**272**	**100,00%**
É fácil denunciar um crime cibernético.	1	61	22,4%
	2	73	26,8%
	3	79	29,0%
	4	33	12,1%
	5	26	9,6%
MÉDIA INDICADOR		**2,60**	
TOTAL GERAL		**272**	**100,00%**
O governo é o principal responsável por um ambiente digital seguro	1	37	13,6%
	2	42	15,4%
	3	78	28,7%
	4	58	21,3%
	5	57	21,0%
MÉDIA INDICADOR		**3,21**	
TOTAL GERAL		**272**	**100,00%**
O governo promove campanhas sobre segurança na internet.	1	79	29,0%
	2	62	22,8%
	3	61	22,4%
	4	44	16,2%
	5	26	9,6%
MÉDIA INDICADOR		**2,54**	
TOTAL GERAL		**272**	**100,00%**
O governo oferece recursos educativos digitais para a segurança na internet.	1	77	28,3%
	2	64	23,5%
	3	66	24,3%
	4	37	13,6%
	5	28	10,3%
MÉDIA INDICADOR		**2,54**	
TOTAL GERAL		**272**	**100,00%**
Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.	1	16	5,9%
	2	10	3,7%
	3	43	15,8%
	4	70	25,7%
	5	133	48,9%
MÉDIA INDICADOR		**4,08**	
TOTAL GERAL		**272**	**100,00%**
MÉDIA CONSTRUTO		**3,03**	

Nota: As âncoras utilizadas foram “1” para “Discordo Totalmente” e “5” para “Concordo Totalmente”.

Fonte: Dados da pesquisa (2023).

Em relação ao construto *upstream*, os resultados obtidos – ao contrário dos construtos anteriores - indicaram que existe uma heterogeneidade da percepção dos respondentes. Primeiramente isso pode ser observado pelo valor médio do construto que foi de 3,03 pontos, ou seja, muito próximo do valor médio "absoluto" de três.

Além disso, entre os oito indicadores desse construto, em somente dois deles a opção cinco – que representa o maior nível de concordância possível – foi a preferida dos respondentes. Isso ocorreu para os indicadores "acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país", com 4,08 pontos e "se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país", com 3,80 pontos. Isso significa que os respondentes consideraram importante o país ter uma legislação sobre segurança adequada e que os indivíduos que porventura cometam crimes, devem realmente ser punidos de acordo com essas leis.

Esses resultados corroboram com Axier e Rainie na pesquisa pela *Pew Research Center* (2019) na qual 75% dos americanos disseram ser favoráveis à mais legislações governamentais.

Um outro indicador ainda apresentou um valor acima da média "absoluta" de três, que foi "o governo é o principal responsável por um ambiente digital seguro" com o valor médio de 3,21 pontos. Assim, verificou-se que as pessoas consideraram que todos somos responsáveis por um ambiente seguro na internet, sejam as próprias pessoas, o meio econômico, além do ambiente governamental.

Os dois indicadores que apresentaram os menores níveis de concordância mostraram que os respondentes avaliaram como deficiente a ação do governo sobre o tema de segurança digital. Isso pode ser verificado a partir dos conteúdos dos indicadores "o governo promove campanhas sobre segurança na internet" e "o governo oferece recursos educativos digitais para a segurança na internet" com as médias de 2,54 pontos para ambos indicadores.

Resultados parecidos foram achados no estudo de Olmstead e Smith (2017) em relação à segurança digital promovida pelo governo, 28% dos americanos entrevistados não confiam no governo para manter seus dados privados seguros e protegidos do acesso indevido, enquanto 12% tem um nível de confiança alto no governo americano nesse aspecto.

Também, Rainie, Kiesler, Kang (2013) ao pesquisarem se as legislações existentes eram capazes de proteger os dados pessoais com 1.102 adultos com 18 anos ou mais, encontraram que cerca de 63% dos respondentes afirmaram que não e 24% que eram razoáveis.

O terceiro indicador desta dissertação com a menor média e, portanto, também, com um nível de discordância foi coerente com os dois construtos anteriores. Mais especificamente, o indicador "é fácil denunciar um crime cibernético" teve um valor médio de 2,60 pontos,

indicando a dificuldade dos respondentes em denunciar um crime cibernético. Isso pode ser consequência da sua percepção de desconhecimento sobre onde denunciar e como denunciar.

O último construto presente no modelo a ser testado e alvo da análise descritiva foi a segurança. A Tabela 15 contém os resultados alcançados.

Em relação à percepção sobre segurança, analisando-se a Tabela 15 foi possível descrever que em princípio existia um maior nível de discordância que de concordância em relação ao conteúdo dos indicadores desse construto. Foi possível perceber inicialmente que o valor da média de 2,78 pontos estava abaixo do valor médio "absoluto" de três pontos. Além disso, para seis dos dez indicadores as opções um e dois foram as mais assinaladas.

Tabela 15

Percepção sobre segurança (continua)

Indicadores	Opções	Frequência	Percentagem
Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital	1	27	9,9
	2	44	16,2
	3	61	22,4
	4	62	22,8
	5	78	28,7
MÉDIA INDICADOR		**3,44**	
TOTAL GERAL		**272**	**100,00%**
As pessoas tomam precauções quando utilizam um Wi-Fi público.	1	105	38,6
	2	73	26,8
	3	47	17,3
	4	25	9,2
	5	22	8,1
MÉDIA INDICADOR		**2,21**	
TOTAL GERAL		**272**	**100,00%**
Em geral, as pessoas utilizam palavras-passes diferentes para fazer *login* em dispositivos diferentes do seu pessoal.	1	69	25,4
	2	74	27,2
	3	68	25,0
	4	33	12,1
	5	28	10,3
MÉDIA INDICADOR		**2,55**	
TOTAL GERAL		**272**	**100,00%**
As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	1	85	31,3
	2	90	33,1
	3	51	18,8
	4	24	8,8
	5	22	8,1
MÉDIA INDICADOR		**2,29**	
TOTAL GERAL		**272**	**100,00%**

Tabela 15

Percepção sobre segurança (concluso)

Indicadores	Opções	Frequência	Percentagem
As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.	1	22	8,1
	2	15	5,5
	3	49	18,0
	4	52	19,1
	5	134	49,3
MÉDIA INDICADOR		**3,96**	
TOTAL GERAL		**272**	**100,00%**
As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.	1	44	16,2
	2	69	25,4
	3	72	26,5
	4	49	18,0
	5	38	14,0
MÉDIA INDICADOR		**2,88**	
TOTAL GERAL		**272**	**100,00%**
Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.	1	65	23,9
	2	92	33,8
	3	66	24,3
	4	30	11,0
	5	19	7,0
MÉDIA INDICADOR		**2,43**	
TOTAL GERAL		**272**	**100,00%**
As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.	1	44	16,2
	2	80	29,4
	3	73	26,8
	4	38	14,0
	5	37	13,6
MÉDIA INDICADOR		**2,79**	
TOTAL GERAL		**272**	**100,00%**
As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.	1	68	25,0
	2	64	23,5
	3	74	27,2
	4	40	14,7
	5	26	9,6
MÉDIA INDICADOR		**2,60**	
TOTAL GERAL		**272**	**100,00%**
Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente	1	56	20,6
	2	79	29,0
	3	70	25,7
	4	40	14,7
	5	27	9,9
MÉDIA INDICADOR		**2,64**	
TOTAL GERAL		**272**	**100,00%**
MÉDIA CONSTRUTO		**2,78**	

Nota: As âncoras utilizadas foram "1" para "Discordo Totalmente" e "5" para "Concordo Totalmente".

Fonte: Dados da pesquisa (2023).

Para os indicadores "as pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas", com 2,88 pontos e "as pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável", com 2,60 pontos,

a opção três – que representa a opção neutra - foi a mais assinalada, apesar dos valores médios indicarem um maior nível de desconfiança que de confiança.

Os dois indicadores que apresentam valores médios acima de três foram “as pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos” com 3,96 pontos e “em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital” com 3,44 pontos. Assim, constatou-se que os respondentes consideraram que as pessoas podiam denunciar possíveis crimes cibernéticos caso fossem vítimas, apesar da dificuldade em fazê-lo e que as pessoas em geral usavam antivírus em seus dispositivos pessoais.

Os três indicadores que têm os maiores níveis de discordância foram: “as pessoas tomam precauções quando utilizam um Wi-Fi público” com o valor médio de 2,21 pontos; “as pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais” com o valor médio de 2,29 pontos e “em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas” com 2,43 pontos.

Esse último resultado é interessante, pois, a autoavaliação das pessoas indicaram que elas sabiam se proteger e tinham conhecimento sobre as ameaças digitais, mas essa percepção mudou bastante em relação às outras pessoas. Além disso, esses resultados foram coerentes quando comparados com os outros construtos, nos quais a utilização do Wi-Fi pessoal protegido em ambiente público ou mudanças de senhas em sua rede doméstica, não eram realizadas pelas pessoas em geral. No caso do processo de denúncia, novamente os resultados mostraram que os respondentes consideraram que as pessoas em geral não sabiam onde fazer uma denúncia na ocorrência de algum crime cibernético.

Os resultados obtidos corroboram a pesquisa da Unisys (2021). A empresa de TI Unisys, mundialmente conhecida, realiza diversos serviços na solução de problemas na área de TI. Entre os serviços está a medição estatística para os governos combaterem riscos, monitorando com índices de segurança específicos. São fornecidos quatro índices: de segurança nacional e de epidemias sobre guerras ou terrorismos e desastres naturais; de segurança financeira acerca de fraudes bancárias e cumprimento de obrigações financeiras pessoais; de segurança na internet sobre operações *online*, vírus, *spam* e *hacks* e de segurança pessoal quanto à roubo de identidade e riscos físicos. Esses índices observam e analisam os eventos que se passam nos países pesquisados (11). Para isso, utiliza-se uma escala de 0 a 300 quanto ao nível de preocupação, sendo 0 nenhuma e 300 o máximo (Unisys, 2021).

No relatório da Unisys (2021) com 11.000 respondentes, sendo mil em cada país, o índice de segurança geral quanto à preocupação das pessoas sobre a segurança foi de 217 no

México, 215 na Colômbia, 192 no Brasil, 175 nos Estados Unidos, 159 na Austrália, 156 na França, 150 na Inglaterra, 140 na Nova Zelândia, 139 na Bélgica, 125 na Alemanha e 115 na Holanda. Quanto à preocupação das pessoas sobre a segurança financeira foi de 224 na Colômbia, 221 no México, 202 no Brasil, 166 nos Estados Unidos, 160 na Austrália, 155 na França, 152 na Inglaterra, 143 na Nova Zelândia, 142 na Bélgica, 115 na Alemanha e 103 na Holanda.

Esses dados mostram uma posição preocupante para os países latinos, demonstrando uma baixa confiança com a segurança financeira e pessoal. Os Estados Unidos como país desenvolvido se aproximam dos níveis de preocupação da América Latina, destacando-se a segurança na internet. Também, nos Estados Unidos e na Europa, a preocupação com a segurança financeira vem aumentando ao contrário da Bélgica que se manteve estável, tendo o governo obtido sucesso com medidas de apoio (Unisys, 2021).

A pandemia do Covid-19 serviu de alerta para a questão da segurança desconhecida para os consumidores. O índice de segurança da Unisys no mercado europeu cresceu, exceto para a França que se manteve estável. Até a Holanda sofreu nesse período com o segundo maior índice de Covid-19, com vários golpes de *hackers* e *ransomware*s que abalaram a confiança nas empresas e no governo. Entre os países desenvolvidos, a Austrália e a Nova Zelândia também apresentaram aumento na segurança da internet. O Covid-19 impactou a segurança da internet devido ao trabalho remoto e aos ataques cibernéticos, com maior intensidade nos Estados Unidos e na Holanda (Unisys, 2021).

Após a pandemia, o índice de segurança da Unisys mostra que retornou ao padrão visto antes para as quatro áreas de segurança. A preocupação com a segurança nacional e segurança pessoal caíram, tendo a atenção voltada para o mundo *online*. O relatório mostrou que os consumidores se tornaram mais conscientes dos riscos envolvidos no pagamento *online*. O percentual de preocupações foi de 60% para fraude bancária, 62% para roubo de identidade, 57% para *hackers* e vírus, 52% para desastres naturais, 51% para segurança nacional, 51% para compras *online*, 47% para obrigações financeiras e 45% para segurança pessoal (Unisys, 2021).

Além disso, o relatório da Unisys confirmou que a pandemia do Covid-19 provocou um aumento da preocupação com a segurança da internet. Esse fato pode ser explicado pelo aumento do uso da internet. A população mundial teve suas rotinas associadas ao mundo *online*, tais como compras *e-commerce*, os serviços governamentais, trabalho e o estudo remotos. Consequentemente, o compartilhamento de dados financeiros com varejistas *online* aumentou o risco de ser comprometido ou enganado. Os ataques cibernéticos cresceram exponencialmente, sendo favorecidos pelo deslocamento da população de ambientes físicos

seguros como os escritórios para ambientes virtuais mais vulnerável (Unisys, 2021).

Outro ponto desse relatório que merece importante destaque é que muitos desconhecem os riscos cibernéticos ou onde denunciá-los: 56% não estão familiarizados com ameaças do tipo *phishing* por SMS, 79% não conhecem SIM jacking e 76% não sabem onde denunciar (Unisys, 2021).

No trabalho remoto, o funcionário executa tarefas que põe em risco a empresa onde trabalha e a si próprio, abrindo anexos sem checar a fonte. Entre esses comportamentos de risco para a segurança digital, 45% dos respondentes disseram realizar *download*s ou instalar *software* não aprovados pela empresa, tendo 42% justificado que usam aplicativos pessoais ou 42% usam aplicativos que consideram melhores que os usados na empresa. Também, 38% dos respondentes afirmaram que a empresa não forneceu uma boa alternativa de ferramentas para trabalharem (Unisys, 2021).

O emprego de BYOD (dispositivos de preferência pessoal) nos ambientes de trabalho se expandiram para serviços, aplicativos, redes sociais, entrelaçando as preferências pessoais à vida profissional. Isso possibilita a entrada de vírus ou *malware* nas redes das empresas, tronando-se um grave problema. O trabalho remoto por aplicativos na modalidade em nuvem contribuíram para a disrupção digital, pois o funcionário pode trabalhar de qualquer lugar frente às mudanças do mercado. Entretanto, a complexidade aumenta com a computação na nuvem e ambientes híbridos, consequentemente, os riscos também aumentam (Unisys, 2021).

Diante disso, as empresas precisam analisar os seus ambientes de TI para mediar as lacunas e incidentes que podem expor seus clientes, parceiros e consumidores. Adquirir conhecimento específico da configuração da plataforma em nuvem e automação governada para implantação de infraestrutura são fundamentais para garantir práticas de segurança antes de se migrar para esse ambiente (Unisys, 2021).

Além disso, *software* inadequados tendem induzir o usuário a procurar melhores alternativas para conseguir produzir mais e alcançar seus objetivos. As empresas devem estar dispostas a atender as preferências e necessidades individuais de tal modo que possa garantir uma comunicação, a colaboração e ferramentas apropriadas que não coloquem em risco a segurança e aumente os custos. A transparência com as informações, a conscientização e a educação dentro das empresas são imperativas como forma de promover comportamentos seguros e conduzir a responsabilidade, amenizando muitos riscos com a mudança de cultura (Unisys, 2021).

5.5 Unidimensionalidade

Esta seção refere-se à análise da unidimensionalidade. Assim, foram apresentados os resultados para os quatros construtos da pesquisa.

Os primeiros resultados a serem analisados são referentes ao construto *downstream* – ver Tabela 16.

Tabela 16

Resultados da AFE para o construto downstream

Indicadores		Fator 1	Fator 2
Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital.		0,495	0,336
Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger.		0,728	0,116
Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais.		0,768	0,116
Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.		0,657	0,192
Desconfio de mensagens recebidas de desconhecidos.		-0,013	0,809
Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas.		0,592	0,519
Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos.		0,320	0,688
Antes de abrir mensagem ou documentos que recebo pelo *WhatsApp* ou *e-mail* verifico a confiabilidade da informação.		0,332	0,720
A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital.		0,164	0,670
Tomo precauções para que meus dados não sejam roubados digitalmente.		0,475	0,670
	KMO		0,889
	Teste de Esfericidade de Bartlett	X^2	1114,717
		df	55
		Sig.	0,000

Fonte: Dados da pesquisa (2023).

Os resultados obtidos mostram que o construto *downstream* é formado por dois fatores, ou seja, ele não é unidimensional. Assim, o próximo passo é definir para quais fatores cada um dos indicadores será alocado e também identificar nos quais ocorre um "carregamento cruzado" das cargas de um indicador em dois ou mais fatores.

A partir da matriz sofreu uma rotação pelo método Varimax para facilitar o processo de definição de cada um indicador e os seus respectivos fatores. A partir dessa análise identificou-se que o Fator 1 é formado pelos seguintes indicadores:

- Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger.
- Utilizo palavras-passes diferentes para fazer *login* em dispositivos da escola ou do trabalho ou de *lanhouse.*
- Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais.
- Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.

O Fator 2 é formado pelos seguintes indicadores:

- Desconfio de mensagens recebidas de desconhecidos.
- A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital.

Por fim, os seguintes indicadores apresentaram carga cruzada nos dois fatores. Por isso eles não serão alocados a nenhum dos dois fatores:

- Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital.
- Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas.
- Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos.
- Tomo precauções para que meus dados não sejam roubados digitalmente.
- Antes de abrir mensagem ou documentos que recebo pelo *WhatsApp* ou *e-mail* verifico a confiabilidade da informação.

Nesta dissertação utilizou-se como regra para a definição da carga cruzada os critérios usados por Vos, Galetzka, Mobach, van Hagen e Pruyn (2019) e por Pijls-Hoekstra, Groen, Galetzka e Pruyn (2017), nos quais a carga fatorial do fator principal deve ser maior que 0,600 e a carga do segundo fator com maior carga não deve ser superior a 0,300. Caso isso não ocorra, existe uma carga cruzada desses indicadores entre os dois ou mais fatores. A recomendação nesse caso é da retirada do indicador das análises de validação subsequentes.

Ao observar a composição do Fator 1, decidiu-se defini-lo como "*downstream*_cuidados_denúncias". O mesmo foi feito para o Fator 2, o qual recebeu a denominação de "*downstream*_mensagens".

O próximo passo é a realização de uma nova análise fatorial exploratória para o novo construto *downstream*_cuidados_denúncias com o intuito de verificar se ele é unidimensional e se os pressupostos da análise fatorial exploratória são atendidos.

Os resultados alcançados pela AFE estão presentes na Tabela 17 a seguir.

Tabela 17

Resultados da AFE para o construto downstream_cuidados_denúncias

Indicadores	Carga Fatorial	Comunalidade
Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger.	0,742	0,550
Utilizo palavras-passes diferentes para fazer l*ogin* em dispositivos da escola ou do trabalho ou de *lanhouse*.	0,747	0,557
Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais.	0,798	0,637
Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	0,706	0,499
KMO		0,716
Teste de Esfericidade de Bartlett	X^2	238,462
	df	6
	Sig.	0,000

Fonte: Dados da pesquisa (2023).

Ao contrário que ocorreu anteriormente, o construto *downstream*_ cuidados_denúncias é formado por somente um fator.

Os resultados presentes na Tabela 17 mostram que os valores das comunalidades e das cargas fatoriais são adequados, pois, estão acima de 0,500 e de 0,700 respectivamente. Além disso, todos os pressupostos para considerar os resultados alcançados pela análise fatorial exploratória como válidos foram satisfeitos. Todas as seis correlações existentes entre os indicadores dos construtos são estatisticamente significativas. O valor do Teste KMO é superior a 0,700, bem como o valor sig. do Teste de Esfericidade de Bartlett é igual a 0,000.

O próximo construto a ser analisado é o *downstream*_mensagens. A Tabela 18 a seguir exibe os valores gerados pela sua análise fatorial exploratória.

Tabela 18

Resultados da AFE para o construto downstream_mensagens

Indicadores		Carga Fatorial	Comunalidade
Desconfio de mensagens recebidas de desconhecidos		0,840	0,706
A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital		0,840	0,706
	KMO		0,500[1]
Teste de Esfericidade de Bartlett		X^2	50,142
		df	1
		Sig.	0,000

Nota: [1]Quando o construto é formado por somente dois indicadores, o valor *default* é de 0,500 para o KMO.

Fonte: Dados da pesquisa (2023).

No caso do construto *downstream*_mensagens, os resultados alcançados são positivos. Esse é um construto unidimensional, ou seja, é formado por somente um fator composto por três indicadores. Todos os pressupostos para considerar os resultados da análise fatorial válidos foram alcançados. A única correlação existente entre os dois indicadores é estatisticamente significativa. Além disso, o p-valor do teste de Esfericidade de Bartlett é igual a 0,000.

No caso do teste KMO o valor de 0,500 é o valor *default* para quando se tem somente dois indicadores. Ressalta-se ainda que os valores obtidos para a comunalidade e para a carga fatorial de todos os indicadores são superiores aos valores de referência de 0,500 e de 0,700 respectivamente (Hair, Black, Babin, Anderson & Tatham, 2009).

O próximo construto para o qual foi realizada uma análise fatorial exploratória é o *midstream*.

A Tabela 19 a seguir mostra os resultados alcançados para o construto *midstream*.

Tabela 19

Resultados da AFE para o construto midstream

Indicadores		Fator 1	Fator 2	Fator 3
Os pais acompanham seus filhos enquanto esses utilizam a internet.		0,706	-0,043	0,153
As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus *sites*.		0,515	0,532	-0,065
A escola é responsável pela educação digital de seus alunos.		0,696	0,140	0,074
As empresas monitoram os comportamentos suspeitos em seus sites.		0,780	0,114	0,017
As pessoas sabem denunciar crimes cibernéticos.		0,360	-0,371	0,701
As empresas são as principais responsáveis por um ambiente digital seguro.		0,637	0,232	0,286
As pessoas, em geral, deixam suas senhas salvas nos sites de compras, para facilitar acessos futuros.		0,116	0,828	0,123
As empresas usam os dados pessoais de seus clientes com transparência.		0,007	0,359	0,828
	KMO			0,760
Teste de Esfericidade de Bartlett	X^2			406,871
	df			28
	Sig.			0,000

Fonte: Dados da pesquisa (2023).

Da mesma forma que ocorreu com o construto *downstream*, o construto *midstream* também possui mais de uma dimensão. A análise fatorial exploratória gerou três fatores. Novamente, o próximo passo é definir para quais fatores cada um dos indicadores será alocado e também identificar os quais nos quais ocorre um "carregamento cruzado" das cargas de um indicador em dois ou mais fatores.

A partir da análise da matriz rotacionada identificou-se que o Fator 1 é formado pelos seguintes indicadores:

- Os pais acompanham seus filhos enquanto esses utilizam a internet.
- A escola é responsável pela educação digital de seus alunos.
- As empresas monitoram os comportamentos suspeitos em seus *sites*.
- As empresas são as principais responsáveis por um ambiente digital seguro.

O Fator 2 é formado pelos seguintes indicadores:

- As pessoas, em geral, deixam suas senhas salvas nos sites de compras, para facilitar acessos futuros.

Não foram identificados indicadores para serem alocados para o Fator 3.

Por fim, os seguintes indicadores apresentaram carga cruzada em dois ou nos três fatores. Por isso eles não serão alocados a nenhum dos três fatores:

- As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus sites.
- As pessoas sabem denunciar crimes cibernéticos.
- As empresas usam os dados pessoais de seus clientes com transparência.

Ao observar a composição do Fator 1, decidiu-se defini-lo como "*midstream*_monitoramento". O mesmo foi feito para o Fator 2, o qual recebeu a denominação de "*midstream*_senhas_salvas". Como esse construto é formado por somente um indicador, não é necessário realizar a sua análise fatorial exploratória para verificar a sua unidimensionalidade.

O próximo passo é a realização de uma nova análise fatorial exploratória para o novo construto *midstream*_monitoramento com o intuito de verificar se ele é unidimensional e se os pressupostos da análise fatorial exploratória são atendidos.

A seguir, tem-se a Tabela 20 que contém os valores da AFE apurados para o construto *midstream*_monitoramento.

Tabela 20

Resultados da AFE para o construto midstream_monitoramento

Indicadores	Carga Fatorial	Comunalidade
Os pais acompanham seus filhos enquanto esses utilizam a internet.	0,711	0,506
A escola é responsável pela educação digital de seus alunos.	0,719	0,517
As empresas monitoram os comportamentos suspeitos em seus *sites*.	0,796	0,633
As empresas são as principais responsáveis por um ambiente digital seguro.	0,735	0,540
KMO		0,700
Teste de Esfericidade de Bartlett	X^2	219,815
	df	6
	Sig.	0,000

Fonte: Dados da pesquisa (2023).

Os dados presentes na Tabela 20 mostram que o construto *midstream*_monitoramento é unidimensional sendo formado por somente um fator.

Os pressupostos para a aceitação dos resultados da análise fatorial exploratória foram satisfeitos. Todas as três correlações que existem entre os três indicadores são estatisticamente significativas. O valor do Teste de Esfericidade de Bartlett gerou um valor sig. = 0,000 e o Teste KMO foi de 0,700. No caso dos valores da comunalidade e da carga fatorial, os três indicadores apresentaram valores avaliados como adequados.

O próximo construto a ser analisado é o *upstream* cujos resultados são exibidos na Tabela 21 a seguir.

Tabela 21

Resultados da AFE para o construto upstream

Indicadores		Fator 1	Fator 2
A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet		0,651	0,192
O governo brasileiro promove leis para um ambiente seguro da internet.		0,694	0,272
Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.		0,297	0,720
É fácil denunciar um crime cibernético.		0,596	0,252
O governo é o principal responsável por um ambiente digital seguro		0,307	0,508
O governo promove campanhas sobre segurança na internet.		0,809	0,115
O governo oferece recursos educativos digitais para a segurança na internet.		0,822	0,127
Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.		0,022	0,863
	KMO		0,791
	Teste de Esfericidade de Bartlett	X^2	641,245
		df	28
		Sig.	0,000

Fonte: Dados da pesquisa (2023).

Para o construto *upstream*, a análise fatorial exploratória identificou que ele é bidimensional, pois, a AFE resultou em dois fatores. Da mesma forma que ocorreu anteriormente, o próximo passo é definir para quais fatores cada um dos indicadores será alocado e também identificar os quais nos quais ocorre um "carregamento cruzado" das cargas de um indicador em dois fatores.

A partir da análise da matriz rotacionada identificou-se que o Fator 1 é formado pelos seguintes indicadores:

- A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet.
- O governo brasileiro promove leis para um ambiente seguro da internet.
- O governo promove campanhas sobre segurança na internet.
- O governo oferece recursos educativos digitais para a segurança na internet.

O Fator 2 é formado pelos seguintes indicadores:

- Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.
- Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.

Além disso, os seguintes indicadores apresentaram carga cruzada em dois fatores. Por isso eles não serão alocados a nenhum dos dois fatores:

- É fácil denunciar um crime cibernético.
- O governo é o principal responsável por um ambiente digital seguro.

Ao observar a composição do Fator 1, decidiu-se defini-lo como "*upstream*_governo". O mesmo foi feito para o Fator 2, o qual recebeu a denominação de "*upstream*_lei". Como esse construto é formado por somente um indicador, não é necessário realizar a sua análise fatorial exploratória para verificar a sua unidimensionalidade.

O próximo passo é a realização de uma nova análise fatorial exploratória para o novo construto *upstream*_governo com o intuito de verificar se ele é unidimensional e se os pressupostos da análise fatorial exploratória são atendidos.

Em seguida são apresentados os resultados alcançados pela realização da AFE para o construto *upstream*_governo – ver Tabela 22.

Tabela 22

Resultados da AFE para o construto upstream_governo

Indicadores		Carga Fatorial	Comunalidade
A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet.		0,674	0,455
O governo brasileiro promove leis para um ambiente seguro da internet.		0,770	0,593
O governo promove campanhas sobre segurança na internet.		0,839	0,705
O governo oferece recursos educativos digitais para a segurança na internet.		0,840	0,706
	KMO		0,709
		X^2	366,647
	Teste de Esfericidade de Bartlett	**df**	6
		Sig.	0,000

Fonte: Dados da pesquisa (2023).

Os resultados obtidos mostram problemas com os valores da comunalidade e da carga fatorial com um dos cinco indicadores que formam o construto com valores menores que 0,500 e que 0,700 respectivamente. Assim, decidiu-se por retirar o indicador "a Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet" e realizar uma nova análise fatorial exploratória para o construto *upstream*_governo.

A Tabela 23 a seguir exibe os resultados alcançados.

Tabela 23

Resultados da AFE para o construto upstream_governo pós nova análise fatorial exploratória

Indicadores		Carga Fatorial	Comunalidade
O governo brasileiro promove leis para um ambiente seguro da internet.		0,747	0,558
O governo promove campanhas sobre segurança na internet.		0,884	0,782
O governo oferece recursos educativos digitais para a segurança na internet.		0,889	0,790
	KMO		0,657
		X^2	285,714
	Teste de Esfericidade de Bartlett	**df**	3
		Sig.	0,000

Fonte: Dados da pesquisa (2023).

Os resultados da análise fatorial exploratória efetuada – ver Tabela 23 – mostram que o construto *upstream*_governo pós nova análise fatorial exploratória é unidimensional, pois, possui somente um fator.

Apesar do indicador "O governo brasileiro promove leis para um ambiente seguro da internet" apresentar um valor abaixo de 0,500 para a comunalidade, a diferença de 0,003 em conjunto com o fato que o valor da sua carga fatorial é superior a 0,700 fizeram com que a pesquisadora se considera a manutenção desse indicador. Os outros indicadores também apresentaram valor para a comunalidade acima de 0,500 e para a carga fatorial de pelo menos 0,700.

Os pressupostos para a aceitação dos resultados da análise fatorial exploratória foram satisfeitos, com todas as correlações entre os indicadores estatisticamente significativas, com o valor KMO acima de 0,600 e com o p-valor do Teste de Esfericidade de Bartlett igual a 0,000.

O outro construto derivado do construto *upstream* é o *upstream*_lei, cujos resultados estão presentes na Tabela 24 a seguir.

Tabela 24

Resultados da AFE para o construto upstream_lei

Indicadores		Carga Fatorial	Comunalidade
Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.		0,848	0,718
Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.		0,848	0,718
	KMO		0,500[1]
	Teste de Esfericidade de Bartlett	X^2	57,059
		df	1
		Sig.	0,000

Nota: [1] Quando o construto é formado por somente dois indicadores, o valor *default* é de 0,500 para o KMO.

Fonte: Dados da pesquisa (2023).

Ao observar a Tabela 24 verifica-se que os resultados são adequados. Os valores para a comunalidade e para a carga fatorial são de pelo menos 0,500 e de 0,700 respectivamente. Sobre os pressupostos, é preciso ressaltar que quando o construto é formado por apenas dois indicadores, o valor do Teste KMO é sempre de 0,500 – isso é o seu valor *default.* O valor do Teste de Esfericidade de Bartlett possui um sig. com o valor de 0,000 e a única correlação

existente entre os dois indicadores desse construto é estatisticamente significativa.

O último construto a ser analisado é a segurança cujos resultados estão abaixo – ver Tabela 25.

Da mesma forma que ocorreu com todos os outros construtos, o construto segurança é composto por mais de um fator. Os resultados mostram que o fator 1 é formado pelos seguintes indicadores:

- As pessoas tomam precauções quando utilizam um Wi-Fi público.
- As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.
- As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.
- Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.
- As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.
- Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente.

Tabela 25

Resultados da AFE para o construto segurança

Indicadores	Fator 1	Fator 2
Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital	0,318	0,639
As pessoas tomam precauções quando utilizam um Wi-Fi público.	0,761	0,122
Em geral, as pessoas utilizam palavras-passes diferentes para fazer *login* em dispositivos diferentes do seu pessoal.	0,735	0,310
As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	0,764	0,141
As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.	0,055	0,884
As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.	0,685	0,184
Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.	0,823	0,062
As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.	0,724	0,309
As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.	0,749	0,232
Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente.	0,806	0,180
KMO		0,906
Teste de Esfericidade de Bartlett	X^2	1342,432
	df	45
	Sig.	0,000

Fonte: Dados da pesquisa (2023).

A partir da análise do conteúdo de cada um dos indicadores que estão contidos no Fator 1 acima, esse construto foi renomeado para “segurança_precaução” de forma a representar o significado da totalidade desses indicadores.

Os resultados mostram que o fator 2 é formado pelo seguinte indicador:

- As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.

Além disso, os seguintes indicadores apresentaram carga cruzada em dois fatores. Por isso eles não serão alocados a nenhum dos dois fatores:

- Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital.
- Em geral, as pessoas utilizam palavras-passes diferentes para fazer *login* em dispositivos diferentes do seu pessoal.
- As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.

A partir da análise do conteúdo do indicador que está contido no Fator 2 acima, esse construto foi renomeado para "segurança_poder_denunciar" de forma a representar a totalidade do seu significado. Como esse construto é formado por somente um indicador, não é necessária a execução de uma nova análise fatorial para ele, bem como os cálculos dos valores para atestar a confiabilidade da escala e da validade convergente do construto.

Assim, a próxima análise fatorial exploratória é sobre o "novo construto" segurança_precaução cujos resultados estão presentes na Tabela 26 a seguir.

Tabela 26

Resultados da AFE para o construto segurança_precaução

Indicadores	Carga Fatorial	Comunalidade
As pessoas tomam precauções quando utilizam um Wi-Fi público.	0,766	0,586
As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.	0,776	0,603
As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.	0,737	0,543
Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.	0,832	0,693
As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.	0,785	0,616
Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente	0,837	0,700
KMO		0,856
Teste de Esfericidade de Bartlett	X^2	783,589
	df	15
	Sig.	0,000

Fonte: Dados da pesquisa (2023).

Em relação à unidimensionalidade, os resultados mostram que foi gerado somente um fator. Todos os pressupostos para considerar os resultados válidos da AFE foram alcançados. O valor do Teste do KMO é superior a 0,800, bem como o teste de Esfericidade de Bartlett tem um p-valor = 0,000. Todas as quinze correlações existentes entre os seis indicadores são estatisticamente significativas.

No caso dos valores das comunalidades e das cargas fatoriais dos indicadores, todos eles apresentam valores considerados adequados, acima de 0,500 e de 0,700 respectivamente.

5.6 Confiabilidade

Esta seção refere-se à análise da confiabilidade das escalas usadas para mensurar os construtos da pesquisa.

Os resultados são apresentados por meio da Tabela 27 a seguir.

Tabela 27

Valores do Alpha de Cronbach de cada um dos construtos que formam o modelo hipotético (continua)

Construto	Indicador	AC	AC se indicador for retirado
*Downstream_* cuidado_ denúncia	Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger.	0,736	0,678
	Utilizo palavras-passes diferentes para fazer l*ogin* em dispositivos da escola ou do trabalho ou de *lanhouse.*		0,676
	Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais.		0,641
	Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.		0,707
Downstream_ mensagens	Desconfio de mensagens recebidas de desconhecidos.	0,579	n. d.
	A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital.		n. d.
Midstream_ monitoramento	Os pais acompanham seus filhos enquanto esses utilizam a internet.	0,722	0,685
	A escola é responsável pela educação digital de seus alunos.		0,679
	As empresas monitoram os comportamentos suspeitos em seus *sites.*		0,616
	As empresas são as principais responsáveis por um ambiente digital seguro.		0,662

Tabela 27

Valores do Alpha de Cronbach de cada um dos construtos que formam o modelo hipotético (concluso)

CONSTRUTO	INDICADOR	AC	AC SE INDICADOR FOR RETIRADO
Upstream_ governo	O governo brasileiro promove leis para um ambiente seguro da internet.	0,794	0,843
	O governo promove campanhas sobre segurança na internet.		0,649
	O governo oferece recursos educativos digitais para a segurança na internet.		0,639
*Upstream*_Lei	Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.	0,604	n. d.
	Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.		n. d.
Segurança_ precaução	As pessoas tomam precauções quando utilizam um Wi-Fi público.	0,878	0,862
	As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.		0,859
	As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.		0,867
	Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.		0,848
	As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.		0,858
	Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente		0,847

Nota: AC significa *Alpha de Cronbach.*
n. d. significa "não disponível". O valor do A. C. caso o item seja excluído não é calculado nesse caso, pois, caso o item seja retirado o indicador ficará com somente um indicador, o que elimina a necessidade do cálculo do valor de A. C.
Fonte: Dados da pesquisa (2023).

Ao analisar a Tabela 27 é possível verificar que as escalas usadas para mensurar os

construtos podem ser consideradas confiáveis, pois, os valores obtidos para o *Alpha de Cronbach* estão acima do valor mínimo exigido de 0,600.

A exceção fica por conta do construto *downstream*_mensagens, o qual possui um valor de 0,579 para o *Alpha de Cronbach*. Por este motivo, esse construto foi retirado das análises subsequentes.

É importante destacar ainda que somente a retirada de dois indicadores é capaz de aumentar o valor do *Alpha de Cronbach*. Contudo, ressalta-se que o objetivo não é o de alcançar o maior valor possível para o AC, e sim, alcançar valores em conjunto com a manutenção de indicadores que indiquem que a escala é confiável em relação às medidas obtidas a partir das respostas dos entrevistados. Assim, a única modificação que ocorre e que é capaz de aumentar o AC é do construto *upstream*_governo.

5.7 Validade convergente

Esta seção refere-se à análise da validade convergente de todos os construtos da pesquisa.

Os resultados obtidos para todos os construtos são exibidos na Tabela 28 a seguir.

Tabela 28

Valores alcançados para a AVE e a CC

Construtos	AVE	CC
*Downstream*_cuidado_denúncia	0,52	0,69
*Midstream*_monitoramento	0,50	0,66
Segurança_proteção	0,55	0,88
*Upstream*_governo	0,59	0,81
*Upstream*_Lei	0,44	0,61

Fonte: Dados da pesquisa (2023).

No caso dos construtos segurança_proteção e *upstream*_governo, os dados presentes na Tabela 28 mostram que eles possuem validade convergente.

Em relação ao construto *upstream*_lei, ele apresenta valores muito aquém dos valores de referência de 0,500 para a AVE e de 0,700 para a CC. Por este motivo, este construto é

retirado das etapas posteriores da análise de dados.

Sobre o construto *downstream*_cuidado_denúncia, os valores da AVE e da CC apurados foram respectivamente 0,42 e 0,74 para a AVE e para a CC. Como o valor da AVE ficou muito abaixo do mínimo recomendável optou-se por retirar o indicador que apresentou a menor carga fatorial – "quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger" – e realizar um novo cálculo da AVE e da CC.

Os resultados novamente ficaram abaixo do adequado, pois, a AVE ficou com o valor de 0,45. Retirou-se novamente o indicador que tinha a menor carga em relação ao construto – "utilizo palavras-passes diferentes para fazer login em dispositivos da escola ou do trabalho ou de *lanhouse*" – e realizou-se um novo cálculo para a AVE e para a CC.

Os valores obtidos foram de 0,52 para a AVE e de 0,69 para a CC. Nesse último caso, como o valor ficou muito próximo de 0,70, optou-se por manter o construto e prosseguir com as análises com os dois indicadores restantes: "sei propor novas ideias e processos para garantir a proteção de tecnologias digitais" e "sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais".

O mesmo ocorre com o construto *midstream*_monitoramento. Inicialmente os valores apurados para a AVE foi de apenas 0,40 e a CC de 0,73. Assim, retirou-se o indicador com o menor valor para a carga fatorial – "as empresas são as principais responsáveis por um ambiente digital seguro" – e calculou-se novamente a AVE e a CC para esse construto.

Os resultados mostram que a AVE alcançou um valor de 0,46 e a CC de 0,70. Assim, foi retirado o indicador "a escola é responsável pela educação digital de seus alunos" e novamente os valores da AVE e da CC foram apurados.

Dessa vez, a AVE exibiu um valor de 0,50 e a CC um valor de 0,66. Da mesma forma que ocorreu com o construto *downstream*_cuidado_denuncia, optou-se por manter esse construto com os dois indicadores – "os pais acompanham seus filhos enquanto esses utilizam a internet" e "as empresas monitoram os comportamentos suspeitos em seus *sites*" – e considerar o valor da CC próximo o suficiente para prosseguir com as análises.

5.8 Validade discriminante

Esta seção refere-se à análise da validade discriminante entre os construtos que formam o modelo hipotético da pesquisa.

A Tabela 29 a seguir exibe os resultados alcançados para os construtos que formam o modelo hipotético. Os valores presentes na diagonal principal dessa matriz são os valores da

raiz quadrada da AVE de cada um dos construtos. Esses valores estão em negrito.

Ressalta-se ainda que o valor da raiz quadrada da AVE atribuído aos dois construtos formados por somente um indicador (*midstream*_senhas_salvas e segurança_poder_denunciar) foi definido a partir do valor da média dos outros quatro construtos formados por mais de um indicador.

Tabela 29

Matriz de correlação entre os construtos e a diagonal principal apresentando o valor da raiz quadrada da AVE de cada um dos construtos

CONSTRUTOS	1	2	3	4	5	6
*Downstream*_cuidado_denúncia	**0,722**					
*Midstream*_monitoramento	0,405	**0,706**				
*Midstream*_senhas_salvas	0,101	0,232	**0,734**			
Segurança_poder_ denunciar	0,217	0,231	0,233	**0,734**		
Segurança_proteção	0,405	0,379	-0,037	0,283	**0,742**	
*Upstream*_governo	0,478	0,354	0,059	0,239	0,603	**0,767**

Nota: 1) É o construto *Downstream*_cuidado_denuncia.
2) É o construto *Midstream*_monitoramento.
3) É o construto *Midstream*_senhas_salvas.
4) É o construto Segurança_poder_denunciar.
5) É o construto Segurança_proteção.
6) É o construto *Upstream*_governo.
Fonte: Dados da pesquisa (2023).

Ao analisar os dados presentes na Tabela 29 é possível concluir que a validade discriminante foi alcançada para todos os construtos. A existência da validade discriminante é muito importante para o teste de modelos hipotéticos, pois, ela garante que os construtos presentes no modelo não são redundantes ou duplicados entre si, ou seja, acontecem uma vez somente. Assim, o modelo é formado por estruturas conceituais que são diversas entre si.

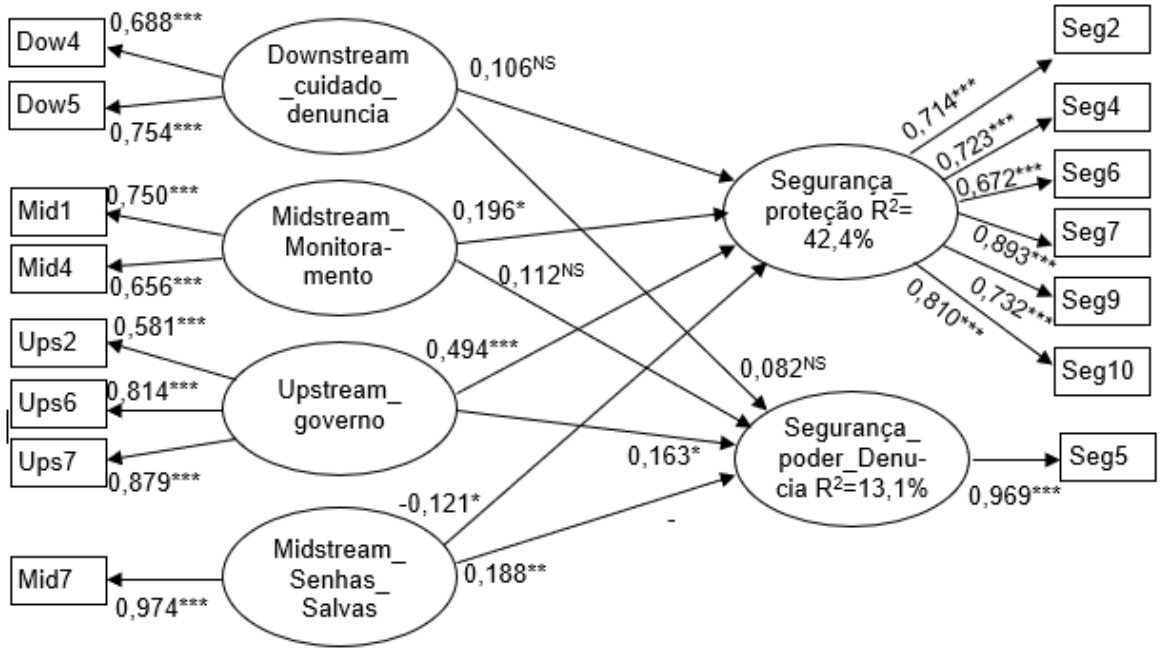
5.9 Validade nomológica

Esta seção refere-se à análise da validade nomológica do modelo hipotético da pesquisa.

A Figura 6 em conjunto com a Tabela 30 a seguir, mostram os resultados alcançados para o modelo hipotético proposto nessa dissertação.

Figura 6

Resultados obtidos para o modelo hipotético proposto



Nota: *** indica que a relação é estatisticamente significativa em nível de 0,001.
** indica que a relação é estatisticamente significativa em nível de 0,01.
* indica que a relação é estatisticamente significativa em nível de 0,05.
NS indica que a relação não é estatisticamente significativa.
Fonte: Dados da pesquisa (2023).

Os resultados expostos na Figura 6 mostra que das oito relações existentes entre os construtos, cinco delas estão estatisticamente significativas.

Além das relações, outro aspecto a ser considerado é o valor da variância explicada dos construtos endógenos do modelo, mais especificamente para a segurança_proteção e segurança_poder_denunciar.

No caso da segurança_proteção o valor encontrado para a variância explicada é de 42,4%, o qual é classificado por Hair, Hult, Ringle e Sarstedt (2014) como sendo uma capacidade explicativa mediada – R2 entre 0,25 e 0,50.

Para o construto segurança_poder_denunciar o valor da variância explicada é de 13,1%. A avaliação é que essa capacidade explicativa é classificada como pequena – até 0,25 – de acordo com os parâmetros de Hair, Hult, Ringle e Sarstedt (2014).

A partir das informações disponibilizadas é possível fazer a análise sobre as hipóteses apresentadas nessa dissertação. A descrição é exibida a seguir – ver Tabela 30.

Tabela 30

Resultado das hipóteses

Hipótese	Coeficiente de Caminho	Significância	Resultado
H1a: As ações do nível *downstream*_cuidado_denuncia influenciam a adoção de comportamentos seguros_proteção no ambiente virtual.	0,106	0,207^{NS}	Rejeitada
H1b: As ações do nível *downstream*_cuidado_denuncia influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual.	0,082	0,375^{NS}	Rejeitada
H2.1a: As ações do nível *midstream*_monitoramento influenciam a adoção de comportamentos seguros_proteção no ambiente virtual.	0,196	*	Apoiada
H2.1b: As ações do nível *midstream*_monitoramento influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual.	0,112	0,203^{NS}	Rejeitada
H2.2a: As ações do nível *midstream*_senhas_salvas influenciam a adoção de comportamentos seguros_proteção no ambiente virtual.	-0,121	*	Apoiada
H2.2b: As ações do nível *midstream*_senhas_salvas influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual.	0,188	**	Apoiada
H3a: As ações do nível *upstream*_governo influenciam a adoção de comportamentos seguros_proteção no ambiente virtual.	0,494	***	Apoiada
H3b: As ações do nível *upstream*_governo influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual.	0,163	*	Apoiada

Nota: *** indica que a relação é estatisticamente significativa em nível de 0,001.
** indica que a relação é estatisticamente significativa em nível de 0,01.
* indica que a relação é estatisticamente significativa em nível de 0,05.
NS indica que a relação não é estatisticamente significativa**.**
Fonte: Dados da pesquisa (2023).

Ao analisar a Tabela 30 verifica-se que a validade nomológica foi alcançada de forma parcial, apesar da maioria das relações se mostrar estatisticamente significativa e a maioria das hipóteses ser apoiada.

Os resultados mostram que o construto *downstream*_cuidado não influencia nenhum dos dois tipos de segurança que foram gerados a partir da análise fatorial exploratória.

Ao analisar os dados anteriores relacionados às médias dos construtos, verifica-se que esse resultado, apesar de ser diferente do que preconiza a teoria, é coerente com a percepção dos respondentes.

O construto que apresentou o maior valor para a média é o *downstream* e o construto que apresentou o menor valor para a média é a segurança. Isto explica porque as relações entre esses dois construtos – e os seus subconstrutos - não são significativas.

Isso mostra também que as pessoas percebem que se preocupam com a segurança no ambiente digital e agem de forma apropriada, mas, não percebem que as pessoas em geral também possuem as mesmas preocupações e comportamentos. Assim, verifica-se que os indivíduos possuem uma autoavaliação muito mais positiva em comparação com a sociedade em geral ou com o meio em que vivem.

A expectativa do respondente em relação ao comportamento do outro alerta para os integrantes dos níveis *midstream* e *upstream* da lacuna existente sobre a temática na sociedade. Esse resultado pode ser alinhado com a experiência da Cidade Ativa de Wandarti (2019) que relata sobre a transformação da escadaria na zona sul de São Paulo no Jardim Nakamura. A rede de referência da comunidade foi envolvida por meio da articulação com as lideranças e grupos de artistas locais a fim de passar segurança aos moradores. Também, foi coletada a opinião deles para assegurar que a transformação seria benéfica para a comunidade. O resultado foi a participação dos moradores independente da idade, da comunidade escolar, dos artistas locais do *graft*, dos comerciantes locais e do poder público nas oficinas e na execução da benfeitoria em prol do bem societário.

Também, Melnyk, Carrillat e Melnyk (2022) estudaram sobre as normas sociais e concluíram que impactam significativamente o comportamento humano. Esses autores revelaram que normas sociais têm maior influência em comportamentos socialmente aprovados em comparação com comportamentos reprovados.

Tanto a experiência de Wandarti (2019) e Melnyk, Carrillat e Melnyk (2022) servem de subsídio para como trabalhar essa lacuna da segurança do comportamental digital. O sucesso da elaboração de leis, das intervenções públicas e de outras atividades nesta área dependem da aprovação pela sociedade para correção desse comportamento. A complexidade desse problema perverso requer o envolvimento dos três níveis do marketing macrossocial, conforme mostrado na experiência da transformação da escadaria em São Paulo.

Em relação ao *midstream*, os seus resultados em geral são significativos. Todavia, ressalta-se que no caso do midstream_monitoramento, ele não afeta o construto segurança_poder_denunciar. Talvez isso ocorra porque as pessoas sabem que podem denunciar, mas não consideram que a sociedade em geral possui práticas de acompanhamento e de monitoramento das ações que ocorrem na internet.

De outro lado verifica-se que o *midstream* impacta os comportamentos de segurança. No caso do valor negativo para a relação entre *midstream*_senhas_salvas e segurança_proteção, esse fato pode ser em função de que as pessoas que deixam a senha salva para facilitar o processo de compra, não possuem o conhecimento ou o hábito de terem comportamento que

aumente o seu nível de proteção no ambiente virtual.

Por fim, as hipóteses relacionadas ao *upstream* foram apoiadas. Nesse caso, verifica-se que as ações públicas, sejam elas em termos de legislação, regras ou mesmo de comunicação são capazes de afetar o comportamento dos indivíduos – hipóteses H3a e H3b.

Ao realizar a modelagem de equações estruturais, o pesquisador deve ainda fazer um exame sobre os índices de ajuste, os quais são úteis para verificar se o modelo testado é válido.

Os índices escolhidos para essa dissertação foram o X^2/df (Qui-quadrado Normado), o valor do índice comparativo de ajuste (CFI), o valor do índice incremental de ajuste (IFI), o valor do índice de Tucker-Lewis (TLI), o valor do índice de qualidade do ajuste (GFI) e o valor da raiz do erro quadrático médio de aproximação (RMSEA), os quais são índices comumente utilizados para verificar o ajuste do modelo.

Os resultados alcançados estão presentes na Tabela 31 a seguir.

Tabela 31

Índices de ajuste do modelo proposto

Índice de ajuste	**Valor obtido**	**Valor de referência[1]**
X^2/df	2,12	>1 até 3 e para modelos mais complexos até 5
CFI	0,94	≥ 0,90
IFI	0,94	≥ 0,90
TLI	0,92	≥ 0,90
GFI	0,92	≥ 0,90
RMSEA	0,06	> 0,03 e < 0,08

Fonte: Dados da pesquisa (2023) e Hair et al. (2009).

A partir dos dados presentes na Tabela 31 conclui-se que os valores dos índices de ajuste são adequados. Esse resultado é importante, pois, ressalta a validade da versão final do modelo obtida com a retirada dos itens que não alcançaram os valores adequados para as suas características psicométricas.

6 CONSIDERAÇÕES FINAIS

A segurança e a proteção dos dados pessoais estão ameaçadas por cibercriminosos dispostos a obter algum tipo de vantagem sobre as vítimas seja como demonstração de poder, prestígio, motivação financeira e/ou ideológicas e/ou comerciais. Nesse sentido, a questão da pesquisa era como os indivíduos que acessam regularmente a internet percebem a influência dos três níveis do marketing macrossocial na adoção de comportamentos digitalmente seguros. Assim, o objetivo geral e específicos da pesquisa, a contextualização do cenário, o referencial teórico e metodológico contribuíram para a análise do modelo analítico proposto.

Teoricamente, a pesquisa explorou essa temática de comportamentos digitalmente seguros na prevenção de cibercrimes sob a perspectiva do marketing macrossocial, sendo abordado o aspecto histórico; a magnitude do cibercrime; a segurança da rede; as estruturas regulatórias, leis e atos, o marketing macrossocial no contexto do mundo digital e as campanhas publicitárias de segurança da informação.

A influência dos três níveis do marketing macrossocial foi pesquisada em um campo ainda não explorado, qual seja, na adoção de comportamentos digitalmente seguros para responder a questão da pesquisa. Foi constatada a importante influência do nível *midstream* e *upstream* diante desse problema multifacetado de segurança da informação e proteção aos dados pessoais na perspectiva dos indivíduos. Mas o nível *downstream* se dissociou dos demais nesse processo da segurança digital. Esse fato demonstrou a importância das ações educativas, formativas e sociais pelos níveis *midstream* e *upstream* para a adoção de comportamentos digitalmente seguros pelo indivíduo.

Destaca-se que as hipóteses iniciais precisaram ser modificadas. As alterações ao nível dos construtos permitiram o levantamento de oito hipóteses dos três níveis do marketing macrossocial para o construto segurança. As duas primeiras hipóteses: as ações do nível *downstream*_cuidado_denuncia influenciam a adoção de comportamentos seguros_proteção no ambiente virtual e as ações do nível *downstream*_cuidado_denuncia influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual foram rejeitadas. Foi constatado que o nível *downstream* (individual) não influencia a segurança digital.

Quanto ao nível *midstream*, das quatro hipóteses levantadas, três foram apoiadas e uma rejeitada. As ações do nível *midstream*_monitoramento influenciam a adoção de comportamentos seguros_proteção no ambiente virtual; as ações do nível *midstream*_senhas_salvas influenciam a adoção de comportamentos seguros_proteção no ambiente virtual e as ações do nível *midstream*_senhas_salvas influenciam a adoção de

comportamentos seguros_poder_denunciar no ambiente virtual foram apoiadas. As ações do nível *midstream*_monitoramento influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual foram rejeitadas. Foi constatado que o nível *midstream* (individual) exerce forte influência na segurança digital.

Quanto ao nível *upstream*, as duas hipóteses foram aceitas. As ações do nível *upstream*_governo influenciam a adoção de comportamentos seguros_proteção no ambiente virtual e as ações do nível *upstream*_governo influenciam a adoção de comportamentos seguros_poder_denunciar no ambiente virtual foram apoiadas. Foi constatado que o nível *upstream* (individual) tem alto poder de influência na segurança digital.

Para atender ao objetivo geral, o primeiro objetivo específico pretendeu identificar se as ações do nível *downstream* influenciam a adoção de comportamentos seguros no ambiente virtual. Segundo resultados da pesquisa, constatou-se que os elementos que compuseram o construto *downstream* não têm influência significativa na segurança digital. Esse resultado deve ser considerado sob a ótica de uma falsa segurança digital que o indivíduo pensa ter.

Esses elementos do construto *downstream* tratam acerca de saber propor novas ideias e processos para garantir a proteção das TICs e saber onde denunciar no caso de identificar algum crime relacionado ao uso de dispositivos digitais. Esses demonstram uma lacuna a ser trabalhada pelos níveis *midstream* e *upstream* por meio de campanhas de conscientização, podcasts, áudios, vídeos, *folders*, *e-books*, regulamentações e legislações.

Quanto ao primeiro elemento, esse está relacionado ao desenvolvimento da literacia digital que se mostrou abaixo do nível avançado. O desenvolvimento da literacia digital está relacionado à idade e aos anos de estudo conforme estudos publicados. Mas esta pesquisa obteve resultados contrários, pois apesar dos respondentes serem na maioria abaixo dos 45 anos e possuírem ensino médio e superior completo/incompleto, não eram capazes de propor novas ideias e processos para garantir a proteção das TICs.

Em relação ao segundo elemento, a conscientização sobre a segurança da informação faz parte de um engajamento maior em prol da cibersegurança. A ciência das ameaças e riscos nos ambientes de trabalho, em casa e sociais deve ser estimulada para a realização de denúncia, seja anônima ou não. Os atos suspeitos devem ser investigados pelos responsáveis e autoridades competentes. A divulgação sobre como realizar denúncias é importante para inibir a recorrência do crime. A preservação das evidências do cibercrime, tais como, *print* da tela, certidão policial, ata notorial, ofício da autoridade policial, *facebook.records* contribuem para a investigação.

Para atender ao objetivo geral, o segundo objetivo específico pretendeu identificar se

as ações do nível *midstream* influenciam a adoção de comportamentos seguros no ambiente virtual. Segundo resultados da pesquisa, constatou-se que os três elementos que compuseram o construto *midstream* têm influência significativa na segurança digital.

Esses elementos do construto *midstream* tratam acerca do acompanhamento dos pais enquanto seus filhos utilizam a internet, das empresas monitorarem os comportamentos suspeitos em seus sites e das pessoas deixarem suas senhas salvas nos *sites* de compras, para facilitar acessos futuros. Esses, também, demonstram uma lacuna a ser trabalhada pelos níveis *midstream* e *upstream.*

Quanto ao primeiro elemento, esse está relacionado aos pais acompanharem seus filhos ou utilizar filtros capazes de restringir o acesso a sites indevidos e com limite de tempo para uso da internet. Esta pesquisa obteve resultados que corroboraram com os estudos presentes na literatura. Entretanto, as ações dos níveis *midstream* e *upstream* podem elevar esse percentual para garantir uma proteção maior e menor número de cibercrimes relacionados à criança e ao adolescente.

Em relação ao segundo elemento, do monitoramento das empresas de comportamento suspeitos em seus *sites*, a infraestrutura da empresa deve ser analisada para ver se necessita de adequações capazes de detectar esses comportamentos suspeitos. O plano de contingência para situações de vazamento de dados dos clientes deve ser de conhecimento dos funcionários para reduzir o tempo de exposição das informações ou o sequestro de dados que possa deixar a empresa inoperante. Os treinamentos dos funcionários devem ser realizados e atualizados frequentemente, pois esses são um dos elos frágeis na proteção dos dados. O resultado da pesquisa indica que o nível *midstream* tem responsabilidade para garantir um ambiente seguro para seus clientes.

O terceiro elemento, versa sobre o comportamento de deixar a senha salva nos sites. Apesar da preocupação com os dados pessoais na internet o comportamento é outro, mostrando uma assimetria e um paradoxo entre a intenção e o comportamento real. Esse comportamento tem relação com o conhecimento sobre o assunto que revela uma falta de informação sobre a questão “ganho de tempo” em se deixar a senha salva, facilitando o processo da compra pela internet, além do viés cognitivo quanto ao limite no processamento das informações pelo usuário. Tais comportamentos demonstram uma lacuna a ser trabalhada pelos níveis *midstream* e *upstream* para a conscientização sobre a segurança como ferramenta capaz de modificar esse comportamento inseguro.

Para atender ao objetivo geral, o terceiro objetivo específico pretendeu identificar se as ações do nível *upstream* influenciam a adoção de comportamentos seguros no ambiente virtual.

Segundo resultados da pesquisa, constatou-se que os três elementos que compuseram o construto *upstream* têm influência significativa na segurança digital.

Esses elementos dizem a respeito do governo brasileiro promover leis e campanhas para um ambiente digital seguro e oferecer recursos educativos digitais para a segurança na internet. A pesquisa mostrou que as pessoas consideram que todos são responsáveis por um ambiente seguro na internet e querem que o governo tenha leis, realize campanhas sobre o tema e disponibilize recursos para a população.

Para atender ao objetivo geral, o último objetivo específico propôs e testou um modelo analítico capaz de avaliar a influência dos três níveis do marketing macrossocial em prol de comportamentos seguros no ambiente virtual. O modelo proposto precisou ser alterado, mas constatou-se forte influência dos níveis *midstream* e *upstream* na adoção de comportamento seguro digital pelo indivíduo.

Quanto ao construto segurança do modelo proposto, os sete elementos que compuseram o construto apresentaram valores significativos. Esses elementos tratam sobre as pessoas tomarem precauções quando utilizarem um Wi-Fi público, saber onde fazer a denúncia no caso de identificarem algum crime relacionado ao uso de dispositivos digitais, poder denunciar no caso de ter seus dispositivos tecnológicos invadidos, ter ciência dos riscos ao abrir mensagens recebidas de desconhecidos, proteger os seus dispositivos móveis do ataque de pessoas maliciosas, verificar se a fonte é confiável antes de abrir mensagens ou documentos recebidos pelo *WhatsApp* e tomar precauções para que seus dados não sejam roubados digitalmente.

A pesquisa mostrou resultados semelhantes aos de outras pesquisas. Os usuários utilizam muito a internet e avaliam que sabem como se proteger de informações suspeitas e agir, caso necessário. Essa constatação reforça que o gerenciamento da internet pelas empresas e governo deve aumentar a vigilância na busca de ameaças, pois o tempo de exposição e a quantidade de acesso são altos. O cibercriminoso tem uma probabilidade grande de encontrar uma vítima.

Portanto, os objetivos da pesquisa foram alcançados, demonstrando a importância sobre as ações do marketing macrossocial na adoção de comportamentos digitalmente seguros.

Limitações do estudo e sugestões de futuros estudos

Conforme citado anteriormente, esta dissertação abrangeu respondentes de 15 estados brasileiros, sendo cerca de 70% de Minas Gerais. Entretanto, não foi abordado nessa pesquisa se o participante era da capital ou interior do estado que residia. Pois, o aspecto macro contexto

regional pode desempenhar influência nas habilidades TICs. Essa análise multifacetada poderia explicar o uso das TICs e a relação entre as oportunidades sócio estruturais e as habilidades de TICs conforme Wicht, Reder e Lechner (2021), ficando sugerido novos estudos.

Para novos estudos, sugere-se pequisar sobre a adoção do comportamento digitalmente seguro da população vulnerável aos cibercrimes a partir de campanhas de conscientização, podcasts, áudios, vídeos, *folders*, *e-books*, regulamentações e legislações realizadas pelos níveis *midstream* e *upstream*. Outra sugestão é sobre os impactos dos investimentos entre unidades de ensino governamentais e privadas que promovem a adoção do comportamento digitalmente seguro para a prevenção do cibercrime no âmbito do marketing macrossocial. Também, estudos de como mobilizar uma comunidade para se tornar ativa em denunciar cibercrimes. Outro estudo sugerido, é analisar os fatores que influenciam a prática de cibercrimes a partir de um modelo de hipóteses para a predição de intenção a redução desses na perspectiva do marketing macrossocial. Além disso, pesquisa sobre a disponibilização de mecanismos de prevenção aos cibercrimes oferecidos ao nível *downstream* pelos níveis *upstream* e *midstream.*

REFERÊNCIAS

Alves, Joice dos Santos & Barboza, Stephanie Ingrid Souza. (2019, 2 a 5 outubro). O processo da literacia da saúde da mulher à luz do marketing social. *XLIII Encontro da ANPAD - EnANPAD 2019.* ANPAD. http://arquivo.anpad.org.br/abrir_pdf.php?e=MjY2MjY=

Anderson, James C. & Gerbing, David W. (1988). Structural Equation Modeling in Practice: a review and recommended two-step approach. *Psychological Bulletin*, 103(3), 411-423. https://www3.nd.edu/~kyuan/courses/sem/readpapers/ANDERSON.pdf

Areepattamannil, Shaljan & Khine, Myint Swe. (2017). Early adolescents' use of information and communication technologies (ICTs) for social communication in 20 countries: examining the roles of ICT – related behavioral and motivacional characteristics. *Computers in Human Behavior*, 73, 263-272. https://doi.org/10.1016/j.chb.2017.03.058

Axier, Brooke & Rainie, Lee. (2019, november 15). Key takeaways on Americans' views about privacy, suveillance and data sharing. *Pew Research Center*. https://www.pewresearch.org/short-reads/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Azevedo, Marcelo Teixeira de. (2010). *Cibersegurança em sistemas de automação em plantas de tratamento de água.* [Dissertação de Mestrado, Escola Politécnica da Universidade de São Paulo]. https://www.teses.usp.br/teses/disponiveis/3/3142/tde-10012011-121525/publico/Dissertacao_Marcelo_Teixeira_de_Azevedo.pdf

Babbie, Earl. (2001). *Métodos de pesquisa survey.* UFMG.

Bagozzi, Richard P., YI, Youjae & Philips, Lynn W. (1991, setembro). Assessing Construct Validity In Organizational Research. *Administrative Science Quartely*, 36(3), 421-458. http://dx.doi.org/10.2307/2393203

Barakat, Lívia Lopes, Lara, José Edson & Gosling, Marlusa. (2011). O surgimento da escola de pensamento do marketing de relacionamento e seus fundamentos. *Pretexto*, 12(3), 29–46. https://doi.org/10.21714/pretexto.v12i3.669

Barbosa, Juliana Souza, Silva, Danihanne Borges e, Oliveira, Daniela Cabral de, Jesus, Dilça Cabral de & Miranda, Wesley Flávio de. (2021, 20 fevereiro). A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. *Research, Society and Development*, 10(2). DOI: http://dx.doi.org/10.33448/rsd-v10i2.12557

Batista, Nayara Kelly. (2018). *O uso de metáforas na análise das campanhas de marketing social sobre a prevenção de HIV/AIDS*. [Dissertação de Mestrado, Centro Universitário Unihorizontes]. https://mestrado.unihorizontes.br/wp-content/uploads/2019/03/NAYARA-KELLY-BATISTA.pdf

Brasil. (2010). *Livro verde: segurança cibernética no Brasil.* Brasília. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. http://livroaberto.ibict.br/bitstream/1/639/4/Livro%20verde%20seguran%c3%a7a%20cibern%c3%a9tica%20no%20Brasil.pdf

Brasil. (2021, 11 agosto). *Campanha alerta consumidor sobre proteção de dados.* Ministério da Justiça e Segurança Pública. https://gov.br/pt-br/noticias/justica-e-seguranca/2021/08/campanha-alerta-consumidor-sobre-protecao-de-dados

Buyucek, Nuray, Kubacki, Krzysztof, Rundle-Thiele, Sharyn & Pang, Bo. (2016). A systematic review of stakeholder involvement in social marketing interventions. *Australasian Marketing Journal* (AMJ), 24(1), 8-19. https://doi.org/10.1016/j.ausmj.2015.11.001

Camargo, Francisco. (2023, 07 agosto). Cibersegurança: VPN é coisa do passado. *Associação brasileira das empresas de software.* https://abes.com.br/cibersegurança-vpn-e-coisa-do-passado/

Canabarro, Diego Rafael. (2014). *Governança global da internet:tecnologia, poder e desenvolvimento*. [Tese de Doutorado, Universidade Federal do Rio Grande do Sul].

Cardoso, Juliana de Barros. (2020). *Letramento digital, tecnologias digitais da informação e comunicação e as perspectivas de desenvolvimento social*. [Dissertação de Mestrado, Universidade Federal de Itajubá]. https://repositorio.unifei.edu.br/jspui/handle/123456789/2189

Carretero Gomes, Stephanie, Vuorikari, R. & Punie, Y. (2017). *DigComp 2.1: The digital competence framework for citizenswith eight proficiency levels and examples of use.* EUR 28558 EN, Publications Office of the European Union, Luxemburgo. https://publications.jrc.ec.europa.eu/repository/handle/JRC106281

Carvalho, Marcelo Sávio Revoredo Menezes de. (2006). *A trajetória da internet no Brasil: do surgimento das redes de Computadores à instituição dos mecanismos de governança*. [Dissertação de Mestrado, Universidade Federal do Rio de Janeiro]

Castells, Manuel. (2003). *A Galáxia Internet: reflexões sobre a internet, negócios e a sociedade*. (Maria Luiza X. de A. Borges, Ed. & Trad.). Zahar. https://www.academia.edu/41717035/A_Galaxia_da_Internet_Manuel_Castells

Castillejos López, Berenice, Torres Gastelú, Carlos Arturo, & Lagunes Domínguez, Agustín. (2016). La seguridad en las competencias digitales de los millennials. Apertura (Guadalajara, Jal.), 8(2), 54-69. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802016000300054&lng=es&tlng=es.

Cavalcanti, José Carlos. (1997). A internet, o modelo nacional e uma proposta de enfoque para uma política de tarifas em sua operação no país. *Brazilian Journal of Political Economy*, 17(2), 299–314. https://doi.org/10.1590/0101-31571997-0941

Cavedon, Ricardo, Ferreira, Helini Silvini & Freitas, Cinthia Obladen de Almendra. (2015, janeiro/junho). O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. *Revista de Direito Ambiental e Sociedade,* 5(1), 194-223. https://www.ucs.br/etc/revistas/index.php/direitoambiental/article/viewArticle/3912

Cazelatto, Caio Eduardo Costa & Segatto, Antonio Carlos. (2014, julho/dezembro). Dos crimes informáticos sob a ótica do meio ambiente digital constitucionalizado e da segurança da informação. *Revista Jurídica Cesumar*, 14(2), 387-411. https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/3713/2469

Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil; Núcleo de Informação e Coordenação do Ponto BR, Comitê Gestor da Internet no Brasil & Autoridade Nacional de Proteção de Dados. (2021). *Cartilha de segurança para internet.* https://cert.br

Cervo, Amado Luiz. & Bervian, Pedro Alcino. (2007). *Metodologia científica.* (6ª ed.). Pearson Prentice Hall.

Childhood. (2012). *Navegar com segurança: por uma infância conectada e livre de violência sexual*. (3ª ed.). CENPEC. WCF Brasil. https://www.childhood.org.br/app/uploads/2022/12/navegar-com-seguranca.pdf

Childhood. (2021). *Relatório de atividades 2021*. https://ch-wordpress.s3.amazonaws.com/uploads/2022/11/relatorio-de-atividades-2021-childhood-relatorio-2021-completo-v11.pdf

Clevenger, Shelly, Navarro, Jordana N., Marcum, Catherine D. & Higgins, George E. (2018). *Understanding victimology: An Active-Learning Approach.* Routledge. https://www.perlego.com/book/1506879/understanding-victimology-an-activelearning-approach-pdf

Colauto, Romualdo Douglas & Beuren, Ilse Maria. (2009). Coleta, análise e interpretação de dados. In: Beuren, Ilse Maria. *Como elaborar trabalhos monográficos em contabilidade: teoria e prática*. (3ª ed.). Atlas.

Datareportal. (2022, october 20). *DIGITAL 2022: OCTOBER GLOBAL STATSHOT REPORT.* https://datareportal.com/reports/digital-2022-october-global-statshot

Dibb, Sally. (2014, september). Up, Up and Away: Social Marketing Breaks Free. *Journal of Marketing Management*, 30(11-12), 1159-85. https://www.researchgate.net/publication/266207223_Up_up_and_away_social_marketing_breaks_free

Domegan, Christine T. (2008). Social marketing: Implications for contemporary marketing practices classification scheme. *Journal of Business and Industrial Marketing*, 23(2), 135-141. https://doi.org/10.1108/08858620810850254

Domegan, Christine T. & Layton, Roger A. (2015, april 20). Social marketing and marketing systems: Towards a coherent theory of change. *Word Social Marketing Conference*, Sydney, Australia. https://issuu.com/worldsocialmarketingconference/docs/fuse-events-australia-programme_web

Domegan, Christine T., Mchugh, Patricia, Biroscak, Brian, Bryant, Carol, Calis, Tanja. (2017). Non-linear causal modelling in social marketing for wicked problems. *Journal of Social Marketing*. 7. 305-329. DOI 10.1108/JSOCM-02-2017-0007.

Domegan, Christine T., McHugh, Patricia, Devaney, Michelle, Duane, Sinead, Hogan, Michael, Broome, Benjamin J., Layton, Roger A., Joyce, John, Mazzonetto, Marzia & Piwowarczyk, Joanna. (2016). Systems-Thinking social marketing: Conceptual extensions and empirical investigations. *Journal of Marketing Management*, 32(11-12), 1123-1144. DOI: 10.1080/0267257X.2016.1183697

Dressler-Hawker, Emma & Veer, Ekant. (2006). Making healthy eating messages more effective: combining integrated marketing communication with the behaviour ecological model. *International Journal of Consumer Studies*, 30 (4), 318-326.

Duailibi, Sérgio; Pinsky, Ilana; Laranjeira, Ronaldo. (2007). Prevalência do beber e dirigir em Diadema, estado de São Paulo. *Revista de Saúde Pública*, 41(6), 1058-1061. https://www.scielo.br/j/rsp/a/4kjVJMWddbbBWdgFypHGJqk/?format=pdf&lang=pt

Duane, Sinead, Domegan, Christine T., Mchugh, Patricia & Devaney, Michelle. (2016). From restricted to complex exchange and beyond: social marketing's change agenda. *Journal of Marketing Management*, 32(9-10), 856-876. https://doi.org/10.1080/0267257X.2016.1189449

EC-*Council*. (2021). *Network Defense Essentials*.

European Commission. (2022, may). *Final report of the Commission expert group on tackling disinformation and promoting digital literacy through education and training*. ISBN 978-92-76-55141-6

European Free Trade Association. (2022). *Safer Unternet Plus.* https://efta.int/eea/eu-programmes/safer-internet-plus

Federal Bureau of Investigation. (2022). *Internet Crime Report 2021.* Estados Unidos. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Fortinet. (2021, 24 fevereiro). *A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020.* https://fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020

Freitas, Cinthia Oladen de Almendra. (2015, 7 a 9 septiembre). A vulnerabilidade do consumidor e a exposição pública na internet. Aires José Rover, Fernando Galindo (Org.), *III Encontro de internacionalização de Conpedi* – Madrid, Facultad de Derecho de la Universidad Complutense de Madrid, Ediciones Laborum, 9. www.conpedi.org.br

Fuller, Christie M., Simmering, Marcia J., Atinc, Guclu, Atinc, Yasemin, & Babin, Barry J. (2016). Common methods variance detection in business research. *Journal of Business Research*, 69(8), 3192-3198. https://www.researchgate.net/profile/Marcia-Simmering/publication/288020168_Common_methods_variance_detection_in_business_research/links/56af6c2908ae656a38785412/Common-methods-variance-detection-in-business-research.pdf

Fýrat, A.F. & Vicdan, H. (2008, december). A New world of literacy, information technologies, and the incorporeal selves: implications for macromarketing thought. *Journal of Macromarketing*, 28(4), 381-396.

Garfinkel, Simson & Spafford, Eugene. (1997). *Web Security & Commerce: Risks, Technologies, and Strategies*. O'Reilly & Associates.

Gibson, William. (1984). *Neuromancer.* Ace Books.

Gil, Antônio Carlos. (2008). *Métodos e técnicas de pesquisa social.* (6ª ed.). Atlas. https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf

Gregson, Jennifer, Foerster, Susan B., Orr, Robin, Jones, Larry, Benedict, Jamie, Clarke, Bobbi, Hersey, James, Lewis, Jan & Zotz, Karen, (2001). System, environmental, and policy changes: using the social – ecological model as a framework for evaluating nitrition education and social marketing programs with low-income audiences. *Journal of Social Marketing,* 33, S4-S15. https://doi.org/10.1016/S1499-4046(06)60065-1

Hair, Joseph F., Babin, Barry, Money, Arthur & Samouel, Phillip. (2005). *Fundamentos de métodos de pesquisa em Administração.* Bookman.

Hair, Joseph F., Hult, Tomas M. G, Ringle, Christian M., & Sarstedt, Marko. (2014). *A primer on Partial Least Squares Structural Equations Modeling (PLS-SEM)*. SAGE. https://www.researchgate.net/publication/354331182_A_Primer_on_Partial_Least_Squares_Structural_Equation_Modeling_PLS-SEM

Hair, Joseph F., Black, William C., Babin, Barry J., Anderson, Rolph E., & Tatham, Ronald L. (2009). *Análise multivariada de dados*. Bookman. https://pt.slideshare.net/ngsouza/livro-analise-multivariada-de-dados-hair-et-al

Halder, Debarati. (2022). *Cyber Vivtimology. Decoding Cyber-crime Victimisation.* Routledge https://www.routledge.com/Cyber-Victimology-Decoding-Cyber-Crime-Victimisation/Halder/p/book/9781032107523

Hastings, Matthew B. (2007, august). An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*. DOI:10.1088/1742-5468/2007/08/P08024

Ikanos.eus. (2022). *Digital Skills Self-assessment*. https://test.ikanos.eus/en/ikanos-model/audit/ikanos-test

Ilomäki, Liisa & Rantanen, Pirkko. (2007). Intensive use of ICT in school: Developing differences in studentes' ICT expertise. *Computers & Education*, 48(2007), 119-136. https://doi.org/10.1016/j.compedu.2005.01.003

Instituto Brasileiro de Geografia e Estatística. (2018). *Pesquisa Nacional por Amostra de Domicílios Contínua – Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2017*. https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf

Instituto Brasileiro de Geografia e Estatística. (2020). *Pesquisa Nacional por Amostra de Domicílios Contínua – Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2018.* https://biblioteca.ibge.gov.br/visualizacao/livros/liv101705_informativo.pdf

Instituto Brasileiro de Geografia e Estatística. (2022). *Pesquisa Nacional por Amostra de Domicílios Contínua – Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2021*. https://biblioteca.ibge.gov.br/visualizacao/livros/liv101963_informativo.pdf

International World Stats. *Estatísticas de crescimento da internet.* https:// www.internetworldstats.com/emarketing.html

Jagadale, Sujit Raghunathrao, & Kemper, Joya. (2022). 'Give It Up!': A Macro-Social Marketing Approach to India's Clean Cooking Fuel Access. *Journal of Macromarketing*, 42(3), 433–453. https://doi.org/10.1177/02761467221107556.

Jenkins, Henry. (2008). *Convergence culture: la cultura de la convergencia de los medios de comunicación.* Paidós Ibérica S.A. https://stbngtrrz.files.wordpress.com/2012/10/jenkins-henry-convergence-culture.pdf

Kalmus, Veronika, Opermann, Signe & Tikerperi, Mari-Liis. (2022). *Eesti õpilaste digipädevus: ülevaade ySKILLS'i küsitlusuuringu 1. laine tulemustest*. https://www.researchgate.net/publication/359311528_Eesti_opilaste_digipadevus_ulevaade_ySKILLS'i_kusitlusuuringu_1_laine_tulemustest

Kaspersky. (2023a). *Ransomare: definição, prevenção e remoção*. https://www.kaspersky.com.br/resource-center/threats/ransomware

Kaspersky. (2023b). *Aprenda sobre malware e como proteger todos os seus dispositivos contra eles*. https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Kaspersky. (2023c). *O que é scareware? Definição e explicação*. https://www.kaspersky.com.br/resource-center/definitions/scareware

Kennedy, Ann-Marie. (2016). Macro-social Marketing. *Journal of Macromarketing*. 36(3), 354-365. https://doi.org/10.1177/0276146715617509

Kennedy, Ann-Marie. (2017). Macro-Social Marketing Research: Philosophy, Methodology and Methods. *Journal of Macromarketing*. 37(4), 347-355. https://doi.org/10.1177/0276146717735467

Kennedy, Ann-Marie. (2020). *Macro-Social Marketing Insights: Systems thinking for wicked problems.* New York and London: Routledge.

Kennedy, Ann-Marie & Parsons, Andrew. (2012). Macro-social marketing and social engineering: a systems approach. *Journal of Social Marketing*, 2(1), 37 – 51. https://doi.org/10.1108/20426761211203247

Kennedy, Ann-Marie & Parsons, Andrew. (2014). Social engineering and social marketing: why is one "good" and the other "bad"? *Journal of Social Marketing*, 4(3), 198-209. DOI:10.1108/JSOCM-01-2014-0006

Kennedy, Ann-Marie, Kapitan, Sommer, Bajaj, Neha, Bakonyi, Angelina & Sands, Sean. (2017). Uncovering wicked problem's system structure: seeing the forest for the trees. *Journal of Social Marketing*, 7(1), 51-73. https://doi.org/10.1108/JSOCM-05-2016-0029

Kennedy, Ann-Marie & Smith, Johnpaul. (2022). Socially Responsible (Macro-Social) Marketing. *Journal of Macromarketing*, 1-11. https://doi.org/10.1177/02761467221087356

Kline, Rex B. (2005). *Principals and Practice of The Structural Equation Modeling*. (2ª ed.). The Guilford Press. https://www.researchgate.net/profile/Cahyono-St/publication/361910413_Principles_and_Practice_of_Structural_Equation_Modeling/links/62cc4f0ed7bd92231faa4db1/Principles-and-Practice-of-Structural-Equation-Modeling.pdf

Kotler, Philip & Lee, Nancy. (2011). *Social marketing: influencing behaviors for good.* (4ª ed.). SAGE Publications.

Kotler, Philip & Zaltman, Gerald. (1971). Social Marketing: An Approach to Planned Social Change. *Journal of Marketing*, 35(july), 3-12. https://doi.org/10.2307/1249783

Levy, Michael Robert. (1978). *Methodology for improving marketing productivity through efficient utilization of customer services resources.* [Doctoral dissertation, Ohio State University]. https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=osu1487083152951477&disposition=inline

Lima, Alessandro Barbosa, Fiorentini, Bruno, Costa, Caio Túlio, Yamamuro, Herberto, Schiavoni, José Luiz, Fernandes, Manoel, Coutinho, Marcelo, Barcellos, Marco, Aranha, Marcos de Souza, Busarello, Romeo, Lindenberg, Ruy, Cavalcanti, Sérgio, Meira, Silvio & Fontoura, Wagner. (2009). *Do broadcast ao socialcast: perspectivas, tendências e reflexões.* W3 Geoinformação Editora. https://issuu.com/bites/docs/do_broadcast_ao_socialcast

Malhotra, Naresh K. (2012). *Pesquisa de marketing: uma orientação aplicada.* Bookman.

Malhotra, Naresh; Nunan, Daniel & Birks, David F. (2017). *Marketing Research: an applied approach*. (5th Ed.). Pearson. http://www.pmm.edu.my/zxc/2022/lib/ebok/Marketing%20Research%20An%20Applied%20Approach%20(1).pdf

Martins, Lucimara. (2021). *Modelo de referência para o desenvolvimento de competências digitais pertinentes a letramento digital e estilos de aprendizagem no ensino superior*.[Dissertação de Mestrado, Universidade Federal de Santa Catarina]. https://repositorio.ufsc.br/handle/123456789/229185

Mascheroni, Giovanna & Cino, Davide. (2022). *Risultati della prima somministrazione della survey ySKILLs Italia (2021)*. Zenodo. https://doi.org/10.5281/zenodo.6376258

May, Cybele & Previte, Josephine. (2016). Understanding the midstream environment within a social change systems continuum. *Journal of Social Marketing*, 6(3), 258-276. https://doi.org/10.1108/JSOCM-04-2015-0023.

McHugh, Patricia, Domegan, Christine & Duane, Sinead. (2018). Protocols for stakeholder participation in social marketing systems. *Social Marketing Quartely*, 24 (3), 164-193. https://doi.org/10.1177/152450041876162

Melnyk, Vladimir, Carrillat, François A., & Melnyk, Valentyna. (2022). The influence of social norms on consumer behavior: a meta-analysis. *Journal of Marketing*, 86(3), 98-120. http://hdl.handle.net/10453/164195

Morgan, George A. & Griego, Orlando V. (1998). *Easy Use and Interpretation of SPSS for Windows: answering research questions with statistics*. Lawrence Erlbaum Associates.

National Center for Education Statistics. (2021). *Programme for the Internacional Assessement of Adult Competencies*. http://nces.ed.gov/surveys/piaac

Nguyen, Dang, Brennan, Linda & Parker, Lukas. (2014). The taboo question: condom retailing in Vietnam and social marketing implications**.** *Journal of Social Marketing*, 4(2), 133-154. https://doi.org/10.1108/JSOCM-08-2013-0053

Núcleo de Informação e Coordenação do Ponto BR. (2014, 3 setembro). CGI.br: *Governança multissetorial e pluriparticipativa da internet do Brasil* [Vídeo]. YouTube. https://www.youtube.com/watch?v=5CD6TPfIIYs

Núcleo de Informação e Coordenação do Ponto BR. (2022, 3 junho). *Homenagem do CGI.br e do NIC.br a Tadao Takahashi* [Vídeo]. YouTube. https://www.youtube.com/watch?v=k2GGXhyhk-I

Oliveira Júnior, Gildásio Antonio de. (2016). *HoneySELK: Um Ambiente para Pesquisa e Visualização de Ataques Cibernéticos em Tempo Real*. [Dissertação de Mestrado, Faculdade de Tecnologia. Universidade de Brasília]. https://repositorio.unb.br/handle/10482/22886

Olmstead, Kenneth & Smith, Aaron. (2017, january 26). Americans and Cybersecurity: Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives. *Pew Research Center*. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Pagliano, Adriana Grelle Antunes, Faria, Ana Claudia Loureiro, Lago, Lisleine Uchôa do, Cruz, Lúcia Maria Santa & Silva, Maurício Paiva da. (1999). *Marketing Social: o novo mandamento para as organizações*. IBMEC. https://www.academia.edu/1270997/Marketing_Social_O_novo_mandamento_para_as_empresas

Parchen, Charles Emmanuel, Freitas, Cinthia Obladen Amendra & Meireles, Jussara Maria Leal de. (2018, janeiro/fevereiro). Vício do consentimento através do neuromarketing nos contratos na era digital. *Revista de Direito do Consumidor*, 115(27), 331-356.

Pereira, Matias José. (2016). *Manual de metodologia da pesquisa científica.* (4ª ed.). São Paulo: Atlas. ISBN 9788522469758.

Pereira, Jefferson Rodrigues, Sousa, Caissa Veloso e, Matos, Eliane Bragança de, Rezende, Leonardo Benedito Oliveira, Bueno, Natália Xavier, & Dias, Álvaro Machado. (2016). Doar ou não doar, eis a questão: uma análise dos fatores críticos da doação de sangue. *Ciência & Saúde Coletiva,* 21(8), 2475-2484. https://doi.org/10.1590/1413-81232015218.24062015

Pereira, Jefferson Rodrigues, Sousa, Caissa Veloso e, Shigaki, Helena Belintani & Lara, José Edson. (2018). Cannabis Sativa: Aspectos Relacionados ao Consumo de Maconha no Contexto Brasileiro. *Revista de Administração Hospitalar e Inovação em Saúde,* 15(1), 1-16. https://doi.org/10.21450/rahis.v15i1.4573

Pereira, Sara Margarida Teófilo. (2022). *Cibersegurança: o papel de polícia de segurança pública na prevenção do cibercrime*. [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna. Lisboa]. http://hdl.handle.net/10400.26/41482

Perovano, Dalton Gean. (2016). *Manual de metodologia de pesquisa científica.* Intersaberes.

Perroti, P. (2020). *Qual o impacto prático da Lei Geral de Proteção de Dados (LGPD) nas corporações?* [video]. http://youtu.be/hUEHPb28o

Pezzella, Maria Cristina Cereser & Wenczenovicz, Thaís Janaina. (2015, 7 a 9 septiembre). Banco de dados, conhecimento e redes científicas: a visibilidade na sociedade da informação. Aires José Rover, Fernando Galindo (Org.), *III Encontro de internacionalização de Conpedi* – Madrid, Facultad de Derecho de la Universidad Complutense de Madrid, Ediciones Laborum, 9. www.conpedi.org.br

Pestana, Maria Helena & Gageiro, João Nunes. (2000). *Análise de dados para ciências sociais: a complementaridade do SPSS*. (6ª ed.). Sílabo. DOI:10.13140/2.1.2491.7284

Pijls-Hoekstra, Ruth, Groen, Brenda H., Galetzka, Mirjam & Pruyn, Adriaan T.H. (2017). Measuring the experience of hospitality: Scale development and validation. *International Journal of Hospitality Management,* Vol. 67, 125-133. https://doi.org/10.1016/j.ijhm.2017.07.008

Ponte, Cristina, Batista, Susana & Baptista, Rita. (2022). *Resultados da 1ª série do questionário ySKILLS (2021) – Portugal.* ySKILLS. https://www.fcsh.unl.pt/static/documentos/informacao/ySkills_Relato%CC%81rio_Portugal.pdf

Rainie, Lee, Kiesler, Sara, Kang, Ruogu & Madden, Mary. (2013, september 05). Anonymity, Privacy, and Security Online. *Pew Research Center.* https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/

Rezende, Leonardo Benedito Oliveira, Sousa, Caissa Veloso e, Pereira, Jefferson Rodrigues, Rezende, Liliane de Oliveira. (2015, julho/setembro). Doação de órgãos no Brasil: uma análise das campanhas governamentais sob a perspectiva do marketing social. *Revista Brasileira de Marketing,* 14(3), 362-376. https://doi.org/10.5585/remark.v14i3.2902

Sales, Patrícia da Silva Almêda & Bonat, Debora. (2022). A era da IA e o 5G: qual a velocidade da (des)informação? Danielle Jacon Ayres Pinto, Maiquel Ângelo Dezordi Wermuth (Org.), XXIX *Congresso Nacional do Conpedi* Balneário Camboriu – SC, Internet: Dinâmicas da segurança pública e internacional, pp. 175 a 191. www.conpedi.org.br

Safernet Brasil. ([n.d.]). *Apresentação do Dia Internet Segura – Brasil - 2009.* https://safernet.org.br/site/sid/o-que-e

Safernet Brasil. (2021). *Safernet participa no TSE de seminário internacional sobre desinformação e eleições.* https://new.safernet.org.br/

Safernet Brasil. (2022a). *Uso excessivo.* https://new.safernet.org.br/content/uso-excessivo#mobile

Safernet Brasil. (2022b). *Dia da Internet Segura.* https://www.safernet.org.br/ste/sid2022/outras-edicoes

Safernet Brasil. (2023a). *Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos.* https://indicadores.safernet.org

Safernet Brasil. (2023b). *Observatório do legislativo.* https://www.safernet.org.br/ste/institucional/projetos/obsleg#:~text=O%20Observat%C3%B3rio%20do%Legislativo%20foi,civil%20nas%20discuss%20C3%B5es%20sobre%20crimes

Safernet Brasil. (2023c). *Parceria com a Google Brasil.* https://www.safernet.org.br/ste/institucional/parcerias/petrobas

Safernet Brasil. (2023d). *Parceria com Petrobas.* https://www.safernet.org.br/ste/institucional/parcerias/google

Safernet Brasil. (2023e). *Dia da Internet Segura.* https://safernet.org.br/site/sid2023/programacao

Santana, Luciano Rocha & Oliveira, Thiago Pires. (2006). Guarda responsável e dignidade dos animais. *Revista Brasileira de Direito Animal*, Salvador, 1(1), 67-104. https://doi.org/10.9771/rbda.v1i1.32362

Santos, Susana Isabel da Silva. (2018). *Estudo das Percepções de Cibersegurança e Cibercrime e das Implicações na Formulação de Políticas Públicas: Estudo Exploratório do Caso Português*. [Dissertação de Mestrado, Instituto Superior de Ciências Sociais e Políticas. Lisboa]. https://catalogo-iscsp.biblioteca.ulisboa.pt/cgi-bin/koha/opac-detail.pl?biblionumber=624375

Senac. (2021). *Segurança e auditoria de sistema de informação.* Editora Senac.

Shaw, Eric H., & Tamilia, Robert D. (2001). Robert Bartels and the History of Marketing Thought. *Journal of Macromarketing*, 21(2), 156–163. https://doi.org/10.1177/0276146701212006

Silva, Vergilio Ricardo Britto da. (2015). *Preocupação da privacidade na internet:uma pesquisa exploratória no cenário brasileiro.* [Dissertação de Mestrado, Faculdade de Administração, Contabilidade e Economia. PUCRS], Porto Alegre. https://tede2.pucrs.br/tede2/bitstream/tede/6018/2/468737%20-%20Texto%20Completo.pdf

Silva, Washington Rodrigues da. (2018). *Análise econômica dos impactos de ataques cibernéticos.* [Dissertação de Mestrado em Economia. Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas. Universidade de Brasília]. https://repositorio.unb.br/handle/10482/34838

Smahel, David, Machackova, Hana, Mascheroni, Giovanna, Dedkova, Lenka, Staksrud, Elisabeth, Ólafsson, Kjartan, Livingstone, Sonia & Hasebrink, Uwe (2020). *EU Kids Online 2020: Survey results from 19 countries.* EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Soares, Hebert Junior, Araújo, Nelcileno V. de S. & Souza. Patricia de. (2020). Privacidade e segurança digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade. *Anais do workshop sobre as implicações da computação na sociedade (WICS). XL Congresso da Sociedade Brasileira de Computação (CSBC 2020)*. Doi 10.5753/wics.2020

Solagna, Fabricio. (2020). *30 anos de governança da Internet no Brasil: coalizões e ideias em disputa pela rede*. [Tese de Doutorado, Universidade Federal do Rio Grande do Sul]

Sousa, Caissa Veloso e, Pereira, Jefferson Rodrigues, Resende, Lousanne Cavalcanti Barros & Rezende, Leonardo Benedito Oliveira. (2017). Donate to save: an analysis of the intention to donate organs under the perspective of social marketing. *Revista Gestão & Tecnologia*, 17(1), 10-35. https://doi.org/10.20397/2177-6652/2017.v17i1.1113.

Spiri, Raquel Torrecilha. (2020). *Cibersegurança no Brasil: Uma análise de seus desdobramentos à luz da Securitização*. [Dissertação de Mestrado, Universidade Estadual Paulista]. Marília. http://www.inscricoes.fmb.unesp.br/upload/trabalhos/20191219164236.pdf

Steinberg, Joseph. (2021). *Cibersegurança para leigos.* Alta Books.

Tambara, Isabelle, Batista, Osvaldo Henrique dos Santos & Freitas, Cinthia Obladen de Almendra. (2014, setembro/dezembro). A proteção do consumidor e as técnicas de neuromarketing no comércio eletrônico que potencializam sua vulnerabilidade. *Revista de Direito Empresarial - RDEmp,* 11(3), 89-107. https://bdjur.stj.jus.br/dspace/handle/2011/91536

Terence, Ana Claudia Fernandes & Escrivão Filho, Edmundo. (2006, 9 a 11 outubro). Abordagem quantitativa, qualitativa e a utilização da pesquisa-ação nos estudos organizacionais. *Anais do XXVI Encontro Nacional de Engenharia de Produção – ENEGEP*. ABEPRO. https://www.abepro.org.br/publicacoes/index.asp?ano=2006

TecMundo. (2018, 1 maio). *A história da internet no Brasil - TecMundo* [Vídeo]. YouTube. https://www.youtube.com/watch?v=k_inQhpKprg

Unicef. (2013). *O uso da internet por adolescentes. https://crianca.mppr.mp.br/arquivos/File/publi/unicef/br_uso_internet_adolescentes.pdf*

Unisys. (2021). *2021 Unisys Security Index: Global Report. Reputation Leaders Ltd*. https://www.unisys.com/siteassets/microsites/unisys-security-index-2021/report-usi-2021.pdf

Velho, Jesus Antonio. (2016). *Tratado de computação forense.* Milenium.

Vidigal, Armando Amorim Ferreira. (2004). O Basil diante dos desafios internacionais em segurança e defesa. In J.R. de Almeida Pinto, A.J. Ramalho da Rocha, R. Doring Pinho da Silva (Orgs), *O Brasil no cenário internacional de defesa e segurança*. (2, pp. 13-35). Ministério da Defesa, Secretaria de Estudos e de Cooperação. https://livroaberto.ibict.br/bitstream/1/658/4/O%20Brasil%20no%20cen%C3%A1rio%20internacional%20de%20defesa%20e%20seguran%C3%A7a.pdf

Virgillito, Salvatore Benito. (2010). *Pesquisa de marketing: uma abordagem quantitativa e qualitativa*. Saraiva.

Vos, Martijn Christiaan, Galetzka, Mirjam; Mobach, Mark, van Hagen, Mark & Pruyn, Adriaan T.H. (2019). Measuring perceived cleanliness in service environments: Scale development and validation. *International journal of hospitality management*, 83, 11-18. https://doi.org/10.1016/j.ijhm.2019.04.005

Waechter, Natalia, Stuhlpfarrer, Elena, Böttcher, Christin, Bernhardt, Marius, & Kadera, Stepanka. (2022). 1. Welle ySKILLS Survey (2021) Deutschland. Zenodo. https://doi.org/10.5281/zenodo.6921738

Wandarti, M. (2019, 04 abril). Como viver em sociedade influencia nossos comportamentos individuais? *ArchDaily Brasil*. https://www.archdaily.com.br/br/914293/como-viver-em-sociedade-influencia-nossos-comportamentos-individuais

Warfield, John N. (1974). *Structuring complex systems.* Battelle Memorial Institute.

Wei, Chongyi, Herrick, Amy, Raymond, H. Fisher, Anglemyer, Andrew, Gerbase, Antonio & Noar, Seth M. (2011). Social marketing interventions to increase HIV/STI testing uptake among men who have sex with men and male-to-female transgender women. *Cochrane Database Syst. Reviews*, 9. https://doi.org/10.1002/14651858.CD009337

Wicht, Alexandra, Reder, Stephen & Lechner, Clemens M. (2021). Sources of individual differences in adults' ICT skills: a large-scale empirical test of a new guiding framework. *PLoS One*. Doi 10.1371/journal.pone.0249574. https://ncbi.nlm.nih.gov/pmc/articles/PMC8054998/pdf/pone.0249574.pdf

Xavier, Maria Joserlane Lima Borges, Figueiredo, Iolanda Gonçalves de Alencar, Xavier, Aldo Luis Borges, Neres, Emanuella Alburquerque de França & Lavôr, Antônia Laryssa de Moura. (2018, janeiro/abril). Influência das tecnologias na adolescência: uma revisão integrativa. *Revista Educação, Psicologia e Interfaces*, 2(1), 135-151. https://doi.org/10.37444/issn-2594-5343.v2il.109.

Zuboff, Shoshana. (2021). *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder* (George Schlesinger Trad.). Intrínseca.

APÊNDICE A – QUESTIONÁRIO

Termo de Consentimento Livre e Esclarecido (TCLE)

Prezado(a) Senhor(a),

Você está sendo convidado(a) a participar da pesquisa **O PAPEL DA TRÍADE SOCIEDADE, GOVERNO E INDIVÍDUO NA PREVENÇÃO DE CIBERCRIMES: um estudo no âmbito do marketing macrossocial** desenvolvida no Curso de Mestrado em Administração do Centro Universitário Unihorizontes.

A pesquisa é de autoria da mestranda Marciana Carvalho Pereira de Souza que está sendo orientada pela Professora Caíssa Veloso e Sousa.

Sua participação é voluntária e são garantidos o seu anonimato e o sigilo das informações.

Você não deve escrever seu nome em nenhum lugar no questionário.

Unihorizontes
Secretaria da Pós-Graduação
(31)3349-2925

1. **Você concorda em participar desta pesquisa?**

☐ Sim ☐ Não (Obrigada)

Para as perguntas a seguir marque **apenas uma alternativa**.

2. **Qual sua faixa etária?**

☐ 18 - 25 anos
☐ 26 - 40 anos
☐ 41 - 60 anos
☐ Acima de 60 anos

3. **Você tem internet em casa?**

☐ sim ☐ não

4. **Com qual frequência usa os dispositivos com internet?**

☐	Nunca
☐	Pelo menos uma vez por semana
☐	Duas a quatro vezes por semana
☐	A maior parte dos dias
☐	Todos os dias

Para a pergunta a seguir você **poderá marcar mais de uma alternativa**.

5. **Como você adquiriu seus atuais conhecimentos sobre Tecnologias de Informação e Comunicação (TIC)?**

(Marque todas as opções que se aplicam)

☐	Tenho habilidades de TI muito básicas
☐	Sou autodidata (recursos disponíveis na *web*, experiência prática…)
☐	Em serviços públicos abertos de formação (telecentros)
☐	Nos centros públicos de formação profissional não regulamentados
☐	Em centros de treinamento privados

Sobre as informações que encontra na internet, marque a opção que mais adapta ao seu comportamento.

6. Eu sei quando suspeitar das informações que encontro.

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

7. Consigo identificar se uma fonte de informação é confiável

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

8. Eu descarto informações indesejadas adequadamente

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

9. Sou capaz de comparar informações de diferentes *sites*, de acordo com sua utilidade

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

10. Participo de *sites q*ue publicam informações que me interessam para meu trabalho ou hobbies

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

11. Participo de sites que publicam informações que me interessam para meu trabalho ou *hobbies*

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

12. Ensino outras pessoas a avaliar criticamente as informações que elas acessam

☐	Sempre
☐	Quase sempre
☐	Às vezes
☐	Nunca

Para a pergunta a seguir é possível marcar **apenas uma alternativa em cada linha**.
Marque **Sim** ou **Não** em cada linha.

Como você compartilha informações e conteúdo digital com outras pessoas?

		Sim	**Não**
13.	Uso *e-mail* para compartilhar conteúdo digital: documentos, fotos, vídeos, etc.		
14.	Uso ferramentas online para compartilhar esses conteúdos: *Google Drive, Scribd, Slide share, Instagram…*		
15.	Participo de redes sociais e fóruns online para compartilhar conhecimento		
16.	Tenho um canal no qual publico meus conteúdos e recebo comentários dos leitores		
17.	Através da internet, colaboro com outras pessoas na minha área educacional ou profissional (minha rede pessoal de aprendizagem ou PLN)		
18.	Encorajo e ensino outras pessoas a usar ferramentas digitais para trocar informações e conteúdo		

Para a pergunta a seguir é possível marcar **apenas uma alternativa em cada linha**.
Marque **Sim** ou **Não** em cada linha.

Sobre o uso dos dispositivos digitais:

		Sim	**Não**
19.	Uso antivírus e faço atualizações		
20.	Sou cauteloso ao receber mensagens cujo remetente ou anexo não conheço (SPAM)		
21.	Uso senhas diferentes para meus dispositivos e serviços digitais e as modifico periodicamente		
22.	Troco periodicamente a chave da rede Wi-Fi da minha casa		
23.	Ajudo pessoas próximas a mim a evitar riscos de segurança com os dispositivos		

Para a pergunta a seguir é possível marcar **apenas uma alternativa em cada linha**.
Marque **Sim** ou **Não** em cada linha.

Sobre os dados na internet:

		Sim	**Não**
24.	Sei que meus dados podem ser usados por outras pessoas		
25.	Conheço o perigo de ser substituído na internet (roubo de identidade, chantagem, ...)		
26.	Tomo extremas precauções antes de fornecer informações pessoais pela internet (DN, endereço, idade, telefone, dados bancários / cartões de crédito, fotos pessoais, ...)		
27.	Sei que o Regulamento Geral de Proteção de Dados (GDPR) existe para proteger dados pessoais na internet		
28.	Sei quando uma página usada tem um certificado de segurança		
29.	Saberia identificar páginas da web ou mensagens de *e-mail* com as quais posso ser enganado		
30.	Participo de atividades para promover hábitos de proteção e privacidade		

Para as perguntas a seguir é possível marcar **apenas uma alternativa em cada linha**.
Marque uma opção nas perguntas a seguir conforme a legenda abaixo:

1 – Discordo totalmente
2 – Discordo parcialmente
3 – Neutro – se não concorda e nem discorda
4 – Discordo parcialmente
5 – Concordo totalmente

31. Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

32. Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

33. Utilizo palavras-passes diferentes para fazer login em dispositivos da escola ou do trabalho ou de *lanhouse*

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

34. Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

35. Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

36. Desconfio de mensagens recebidas de desconhecidos

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

37. Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

38. Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

39. Antes de abrir mensagem ou documentos que recebo pelo *WhatsApp* ou *e-mail*, verifico a confiabilidade da informação

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

40. A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

41. Tomo precauções para que meus dados não sejam roubados digitalmente

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

42. Os pais acompanham seus filhos enquanto esses utilizam a internet

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

43. As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus *sites*

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

44. A escola é responsável pela educação digital de seus alunos

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

45. As empresas monitoram os comportamentos suspeitos em seus *sites*

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

46. As pessoas sabem denunciar crimes cibernéticos

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

47. As empresas são as principais responsáveis por um ambiente digital seguro

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

48. As pessoas, em geral, deixam suas senhas salvas nos sites de compras, para facilitar acessos futuros

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

49. As empresas usam os dados pessoais de seus clientes com transparência

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

50. A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

51. O governo brasileiro promove leis para um ambiente seguro da internet

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

52. Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

53. É fácil denunciar um crime cibernético

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

54. O governo é o principal responsável por um ambiente digital seguro

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

55. O governo promove campanhas sobre segurança na internet

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

56. O governo oferece recursos educativos digitais para a segurança na internet

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

57. Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

58. Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

59. As pessoas tomam precauções quando utilizam um Wi-Fi público

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

60. Em geral, as pessoas utilizam palavras-passes diferentes para fazer login em dispositivos diferentes do seu pessoal

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

61. As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

62. As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

63. As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

64. Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

65. As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

66. As pessoas antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável

	1	2	3	4	5	
Discordo totalmente	☐	☐	☐	☐	☐	Concordo totalmente

67. Em geral, as pessoas tomam precauções para que seus dados não sejam roubados digitalmente

	1	2	3	4	5	
Discordo totalmente	☐	☐	☐	☐	☐	Concordo totalmente

68. Com qual gênero você se identifica?

- ☐ mulher
- ☐ homem
- ☐ prefiro não responder
- ☐ Outro: _____

69. Qual sua escolaridade?

- ☐ Ensino fundamental completo/incompleto
- ☐ Ensino médio completo/incompleto
- ☐ Ensino superior completo/incompleto
- ☐ Pós-graduação latu sensu/MBA
- ☐ Mestrado/doutorado

70. Em qual estado você reside?

☐ Minas Gerais	☐ Goiás	☐ Rio de Janeiro
☐ Acre	☐ Maranhão	☐ Rio Grande do Norte
☐ Alagoas	☐ Mato Grosso	☐ Rio Grande do Sul
☐ Amapá	☐ Mato Grosso do Sul	☐ Rondônia
☐ Amazonas	☐ Pará	☐ Roraima
☐ Bahia	☐ Paraíba	☐ Santa Carina
☐ Ceará	☐ Paraná	☐ São Paulo
☐ Distrito Federal	☐ Pernambuco	☐ Sergipe
☐ Espírito Santo	☐ Piauí	☐ Tocantins

71. Qual sua renda?

- [ ] Não estou trabalhando e não tenho renda
- [ ] Não estou trabalhando e sou estudante
- [ ] Até R$1.400,00
- [ ] De R$1.401,00 até R$4.200,00
- [ ] De R$4.201,00 até R$8.400,00
- [ ] De R$8.401,00 até R$14.000,00
- [ ] De R$14.001,00 até R$28.000,00
- [ ] Acima de R$28.000,00

72. Qual o maior nível de escolaridade das pessoas com quem você mora? (Considere a pessoa de maior escolaridade)

- [ ] Moro sozinho
- [ ] Ensino fundamental completo / incompleto
- [ ] Ensino médio completo / incompleto
- [ ] Ensino superior completo / incompleto
- [ ] Pós-graduação *latu sensu* / MBA
- [ ] Mestrado / Doutorado

APÊNDICE B - VARIÁVEIS DA PESQUISA

CÓDIGO	VARIÁVEIS
Dow1	Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital
Dow2	Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger
Dow3	Utilizo palavras-passes diferentes para fazer *login* em dispositivos da escola ou do trabalho ou de *lanhouse*
Dow4	Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais
Dow5	Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais
Dow6	Desconfio de mensagens recebidas de desconhecidos
Dow7	Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas
Dow8	Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos
Dow9	Antes de abrir mensagem ou documentos que recebo pelo *WhatsApp* ou *e-mail* verifico a confiabilidade da informação
Dow10	A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital
Dow11	Tomo precauções para que meus dados não sejam roubados digitalmente
Mid1	Os pais acompanham seus filhos enquanto esses utilizam a internet.
Mid2	As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus sites.
Mid3	A escola é responsável pela educação digital de seus alunos.
Mid4	As empresas monitoram os comportamentos suspeitos em seus sites.
Mid5	As pessoas sabem denunciar crimes cibernéticos
Mid6	As empresas são as principais responsáveis por um ambiente digital seguro
Mid7	As pessoas, em geral, deixam suas senhas salvas nos *sites* de compras, para facilitar acessos futuros
Mid8	As empresas usam os dados pessoais de seus clientes com transparência

(continua)

CÓDIGO	VARIÁVEIS
Ups1	A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet
Ups2	O governo brasileiro promove leis para um ambiente seguro da internet.
Ups3	Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.
Ups4	É fácil denunciar um crime cibernético.
Ups5	O governo é o principal responsável por um ambiente digital seguro
Ups6	O governo promove campanhas sobre segurança na internet.
Ups7	O governo oferece recursos educativos digitais para a segurança na internet.
Ups8	Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.
Seg1	Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital
Seg2	As pessoas tomam precauções quando utilizam um Wi-Fi público.
Seg3	Em geral, as pessoas utilizam palavras-passes diferentes para fazer l*ogin* em dispositivos diferentes do seu pessoal.
Seg4	As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.
Seg5	As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.
Seg6	As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.
Seg7	Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.
Seg8	As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.
Seg9	As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.
Seg10	Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente

Fonte: European Commission (2022) e *site* da Ikanos.eus (2022). Elaborado pela autora (2023).

APÊNDICE C – CONSTRUTOS DA PEQUISA

CONSTRUTO	DEFINIÇÃO CONCEITUAL	REFERÊNCIAS	VARIÁVEIS
DOWNSTREAM	Está relacionado às influências sobre o comportamento ao nível individual de personalidade, sofrendo influências dos níveis *midstream* e *upstream*	DOMEGAN, 2008 GORDON, 2012 KENNEDY; PARSONS, 2012 NGUYEN *et. al*, 2014 HUFF et al., 2017	Sempre utilizo antivírus para verificar se há alguma ameaça em meu dispositivo digital
			Quando utilizo Wi-Fi de locais públicos utilizo uma rede virtual pessoal (VPN) para me proteger
			Utilizo palavras-passes diferentes para fazer login em dispositivos da escola ou do trabalho ou de *lanhouse*
			Sei propor novas ideias e processos para garantir a proteção de tecnologias digitais
			Sei onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais
			Desconfio de mensagens recebidas de desconhecidos
			Sei proteger meus dispositivos móveis do ataque de pessoas maliciosas
			Minhas senhas na internet são senhas fortes, ou seja, são complexas para prevenir ataques maliciosos
			Antes de abrir mensagem ou documentos que recebo pelo WhatsApp vou email verifico a confiabilidade da informação
			A pessoa que usa o dispositivo móvel é a principal responsável pela sua segurança digital
			Tomo precauções para que meus dados não sejam roubados digitalmente
MIDSTREAM	Está relacionado ao ambiente social mais imediato, ou seja, nível comunitário, escolas, familiares, instituições e ambientes estruturais impactados por políticas públicas maiores. Assim, o seu poder de influência em relação ao nível *upstream* é menor.	DOMEGAN, 2008 GORDON, 2012 KENNEDY; PARSONS, 2012 NGUYEN *et. al*, 2014 HUFF et al., 2017	Os pais acompanham seus filhos enquanto esses utilizam a internet.
			As empresas são responsáveis pela segurança da informação das pessoas que utilizam seus *sites*.
			A escola é responsável pela educação digital de seus alunos.
			As empresas monitoram os comportamentos suspeitos em seus sites.
			As pessoas sabem denunciar crimes cibernéticos
			As empresas são as principais responsáveis por um ambiente digital seguro
			As pessoas, em geral, deixam suas senhas salvas nos *sites* de compras, para facilitar acessos futuros
			As empresas usam os dados pessoais de seus clientes com transparência

(continua)

CONSTRUTO	DEFINIÇÃO CONCEITUAL	REFERÊNCIAS	VARIÁVEIS
UPSTREAM	Está relacionado ao ambiente estrutural, isto é, as condições econômicas, as legislações, as políticas, etc. que podem impactar o comportamento dos indivíduos.	DOMEGAN, 2008 KENNEDY; PARSONS, 2012 NGUYEN *et. al*, 2014 HUFF et al., 2017	A Lei Geral de Proteção dos Dados (LGPD) consegue inibir os crimes da internet
			O governo brasileiro promove leis para um ambiente seguro da internet.
			Se uma pessoa cometer um crime cibernético poderá ser punida a partir de leis regulamentadas no país.
			É fácil denunciar um crime cibernético.
			O governo é o principal responsável por um ambiente digital seguro
			O governo promove campanhas sobre segurança na internet.
			O governo oferece recursos educativos digitais para a segurança na internet.
			Acredito que as legislações de segurança na internet podem contribuir positivamente com o avanço tecnológico no país.
SEGURANÇA	É a adoção de medidas de modo abrangente da rede capaz de prever, proteger, monitorar, analisar, detectar e responder diante da identificação de intrusos	GARFINKEL, 1997 EC-*Council*, p.5-8, 2021 ISO/IEC 27.001 ISO/IEC 27.002 NBR ISO 27001:2006 NBR ISO 27002:2007	Em geral, as pessoas utilizam antivírus para verificar se há alguma ameaça em seu dispositivo digital
			As pessoas tomam precauções quando utilizam um Wi-Fi público.
			Em geral, as pessoas utilizam palavras-passes diferentes para fazer login em dispositivos diferentes do seu pessoal.
			As pessoas sabem onde fazer a denúncia no caso de identificar algum crime relacionado ao uso de dispositivos digitais.
			As pessoas podem denunciar no caso de terem seus dispositivos tecnológicos invadidos.
			As pessoas sabem dos riscos ao abrir mensagens recebidas de desconhecidas.
			Em geral as pessoas sabem proteger seus dispositivos móveis do ataque de pessoas maliciosas.
			As pessoas geralmente usam senhas fortes na internet, ou seja, são complexas para prevenir ataques maliciosos.
			As pessoas, antes de abrirem mensagens ou documentos recebidos pelo *WhatsApp* verificam se foram enviadas por alguém confiável.
			Em geral as pessoas tomam precauções para que seus dados não sejam roubados digitalmente

Fonte: European Commission (2022) e *site* da Ikanos.eus (2022). Elaborado pela autora (2023).