

FUNDAÇÃO GETULIO VARGAS  
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

HAMILTON GOMES DE OLIVEIRA

**INFORMAÇÕES DE SAÚDE EM *CLOUD COMPUTING*: ANALISANDO AS  
PREOCUPAÇÕES COM PRIVACIDADE NO USO DE APLICATIVOS MÓVEIS**

SÃO PAULO

2021

HAMILTON GOMES DE OLIVEIRA

**INFORMAÇÕES DE SAÚDE EM *CLOUD COMPUTING*: ANALISANDO AS  
PREOCUPAÇÕES COM PRIVACIDADE NO USO DE APLICATIVOS MÓVEIS**

Trabalho Aplicado apresentado à Escola de  
Administração de Empresas de São Paulo da  
Fundação Getulio Vargas como requisito para a  
obtenção do título de Mestre em Gestão para a  
Competitividade.

Linha de Pesquisa: Tecnologia da Informação

Orientador: Prof. Dr. Claudio Luis Carvalho  
Larreira

SÃO PAULO

2021

Oliveira, Hamilton Gomes de.

Informações de saúde em *cloud computing* : analisando as preocupações com privacidade no uso de aplicativos móveis / Hamilton Gomes de Oliveira. - 2021.  
58 f.

Orientador: Cláudio Luís Carvalho Larieira.

Dissertação (mestrado profissional MPGC) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Aplicativos móveis. 2. Tecnologia medica. 3. Computação em nuvem. 4. Proteção de dados. 5. Processamento eletrônico de dados. I. Larieira, Cláudio Luís Carvalho. II. Dissertação (mestrado profissional MPGC) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 62::007

HAMILTON GOMES DE OLIVEIRA

**INFORMAÇÕES DE SAÚDE EM *CLOUD COMPUTING*: ANALISANDO AS  
PREOCUPAÇÕES COM PRIVACIDADE NO USO DE APLICATIVOS MÓVEIS**

Trabalho Aplicado apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas como requisito para a obtenção do título de Mestre em Gestão para a Competitividade.

Linha de Pesquisa: Tecnologia da Informação

Orientador: Prof. Dr. Claudio Luis Carvalho Larieira

Data da Aprovação: 23/02/2021

Banca Examinadora:

---

Prof. Dr. Claudio Luis Carvalho Larieira  
(Orientador) – FGV-EASP

---

Prof. Dr. Adilson Carlos Yoshikuni  
FGV-EASP

---

Prof. Dr. Alexandre Cappellozza  
Universidade Presbiteriana Mackenzie

## **AGRADECIMENTOS**

À minha amada esposa Erika por seu apoio incondicional nesta etapa da minha vida. A jornada foi desafiadora, quase dois anos equilibrando as muitas responsabilidades em meio à uma pandemia, mas sua paciência e carinho foram essenciais. Não posso deixar de fora nossa bebezinha, a Vicky, que tem o incrível dom de alegrar nossa casa todos os dias dando a ânimo que precisamos para lidar com quaisquer desafios.

Aos meus pais que me deram tudo que precisei em minha vida, e aos meus irmãos e primos que tornaram minha infância divertida e memorável e me guiaram até aqui.

Aos meus colegas da turma de 2019 do MPGC-TI pela parceria, amizade e troca de conhecimento e, em especial, aos meus amigos Kleber Freitas, Fabio Leandro e Carolina Mourão que além de serem pessoas incríveis, tornaram cada trabalho estressante em uma oportunidade para relaxar e dar umas risadas. Não posso deixar de lado também Murilo Catussi e Rogério Kaneko pela ajuda oportuna na fase final desta jornada.

Aos professores do MPGC-TI, com destaque ao professor Dr. Claudio Larieira pelas importantes contribuições e por todo o suporte auxiliando na organização das ideias e colocando este estudo no rumo correto. Ao professor Dr. Adilson Yoshikuni por reservar tempo para compartilhar seu conhecimento e ao professor Alexandre Cappelozza que também compôs a banca examinadora.

Por fim, agradeço a todos que mesmo indiretamente me ajudaram e espero retribuir esse generoso apoio no futuro!

*“One person can make a difference and everyone should try”.*

**John F. Kennedy**

## RESUMO

O uso de aplicativos móveis e dispositivos vestíveis, combinados com a capacidade da *cloud computing* (CC) para armazenar e processar grandes volumes de dados de saúde e bem-estar, oferecem capacidades de acesso instantâneo e o compartilhamento ágil das informações. No entanto, o volume de informações geradas e o fato delas trafegarem pela Internet pode aumentar as preocupações dos indivíduos no que tange sua privacidade e sua intenção em divulgar informações de saúde e bem-estar em aplicativos móveis que usam *cloud computing* (m-Health). Para investigar como as preocupações dos indivíduos acerca da privacidade afetam seu comportamento em compartilhar dados de saúde em plataformas m-Health foi usado o modelo *Mobile Users' Information Privacy Concerns* (MUIPC). Os resultados foram analisados por meio do método *partial least squares* (PLS-SEM) e foi demonstrado que as preocupações com privacidade da informação influenciam principalmente o comportamento dos indivíduos de meia idade e idosos na divulgação de dados no uso de m-Health. Este estudo foi baseado em uma pesquisa on-line que alcançou 300 participantes. As descobertas deste estudo fornecem uma visão abrangente que traz contribuições para a teoria, por demonstrar a aplicação do modelo MUIPC como um instrumento válido para explorar as preocupações privacidade no uso de aplicativos móveis e CC na área de saúde, mas também o papel moderador das variáveis de controle sociodemográficas como gênero, renda e idade. Para prática, as contribuições estão na apresentação das implicações do uso de m-Health aos interessados de saúde na direção de centralizar as informações de saúde do paciente e facilitar a colaboração.

**Palavras-chave:** m-Health. computação em nuvem. privacidade de dados. electronic health records. MUIPC.

## **ABSTRACT**

The use of mobile apps and wearable devices, combined with the ability of cloud computing (CC) to store and process large volumes of health and wellness data, offer instant access capabilities and agile information sharing. However, the volume of information generated and the fact that it travels over the Internet can increase individuals' concerns about privacy and their intention to disclose health and well-being information in mobile applications that use cloud computing (m-Health). To investigate how individuals' privacy concerns affect their behavior in sharing health data on m-Health platforms, it was used the Mobile Users' Information Privacy Concerns (MUIPC) model. The results were analyzed using the partial least squares method (PLS-SEM) and they demonstrated that the individuals' concerns with information privacy influence mainly the behavior of middle-aged and elderly in the disclosing of data on the use of m-Health. This study was based on an online survey that reached 300 participants. The findings of this study provide a comprehensive view that brings contributions to the theory, as it demonstrates the application of the MUIPC model as a valid instrument to explore privacy concerns in the use of mobile applications and CC in the health field, but also the moderating role of the sociodemographic variables controls such as gender, income and age. To practice, the contributions are related to the implications of using m-Health usage to health stakeholders in the direction of centralizing patient health information and facilitating the collaboration.

**Keywords:** m-Health. cloud computing. information privacy. electronic health records. MUIPC.



## LISTA DE SIGLAS

<b>AGE</b>	Idade
<b>BINT</b>	Intenção Comportamental
<b>CC</b>	<i>Cloud Computing</i>
<b>CFIP</b>	<i>Concern For Information Privacy</i>
<b>COM</b>	<i>Communication Privacy Management</i>
<b>EHR</b>	<i>Electronic Health Record</i>
<b>FIP</b>	<i>Fair Information Practices</i>
<b>GEN</b>	Gênero
<b>HTMT</b>	<i>Heterotrait-Monotrait Ratio</i>
<b>INC</b>	Renda Familiar
<b>INTR</b>	Intrusão Percebida
<b>IUIPC</b>	<i>Internet Users' Information Privacy Concerns</i>
<b>MUIPC</b>	<i>Mobile Users' Information Privacy Concerns</i>
<b>PEXP</b>	Experiência Prévia Com Violação De Privacidade
<b>PLS</b>	<i>Partial Least Squares</i>
<b>PLS-SEM</b>	<i>Partial Least Squares – Structural Equation Modeling</i>
<b>PLS-MGA</b>	<i>Partial Least Squares – Multi-Group Analysis</i>
<b>PMIS</b>	Plataforma Multilateral De Informações De Saúde
<b>SURV</b>	Vigilância Percebida
<b>SUSE</b>	Uso Secundário De Informações Pessoais

## LISTA DE FIGURAS

Figura 1 – m-Health como uma Plataforma Multilateral .....	25
Figura 2 – Modelo MUIPC.....	27
Figura 3 – Modelo MUIPC com os resultados (*p<0,05) .....	39

## LISTA DE TABELAS

Tabela 1 – Tecnologias e pesquisas relacionadas com privacidade em saúde .....	19
Tabela 2 – Evolução do Conceito de Privacidade da Informação e a Evolução da TI.....	21
Tabela 3 – Classificação demográfica da amostra.....	33
Tabela 4 – Tipo de Dispositivos Móveis .....	34
Tabela 5 – Carga Fatorial MUIPC.....	35
Tabela 6 – Resultados da Avaliação do Modelo MUIPC.....	36
Tabela 7 – Critério de Cargas Cruzadas .....	36
Tabela 8 – Heterotrait-Monotrait ratio .....	37
Tabela 9 – Intervalos de Confiança de Bootstrap para HTMT.....	37
Tabela 10 – Tamanhos do Efeito, Coeficiente de Determinação e Relevância Preditiva .....	38
Tabela 11 – Resultados do Modelo Estrutural.....	39
Tabela 12 – Segmentação em grupos da amostra.....	40
Tabela 13 – MICOM para a variável de controle AGE (AGE1 x AGE2).....	42
Tabela 14 – MICOM para a variável de controle GEN (GEN1 x GEN2).....	42
Tabela 15 – MICOM para a variável de controle INC (INC1 x INC2).....	43
Tabela 16 – Resultados da análise PLS-MGA .....	44
Tabela 17 – Resultados da análise dos resultados específicos dos grupos AGE1 e AGE2 .....	45
Tabela 18 – Escala MUIPC – Instrumento de Pesquisa .....	58

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>14</b>
1.1	QUESTÃO DE PESQUISA .....	18
1.2	OBJETIVO .....	18
1.3	JUSTIFICATIVA .....	19
1.4	ESTRUTURA DO TRABALHO .....	20
<b>2</b>	<b>BASE TEÓRICA .....</b>	<b>20</b>
2.1	PRIVACIDADE DA INFORMAÇÃO.....	20
2.2	PRIVACIDADE DA INFORMAÇÃO EM SAÚDE .....	22
<b>2.2.1</b>	<b>Privacidade da informação no uso EHR .....</b>	<b>22</b>
<b>2.2.2</b>	<b>Privacidade da informação em uma plataforma multilateral de saúde .....</b>	<b>23</b>
<b>2.2.3</b>	<b><i>Cloud computing</i> e a privacidade da informação .....</b>	<b>23</b>
2.3	M-HEALTH .....	24
<b>2.3.1</b>	<b>Privacidade de informações .....</b>	<b>24</b>
<b>3</b>	<b>MODELO DE PESQUISA.....</b>	<b>27</b>
3.1	HIPÓTESES DE PESQUISA.....	29
3.2	VARIÁVEIS DE CONTROLE .....	30
<b>4</b>	<b>METODOLOGIA .....</b>	<b>31</b>
4.1	PROCEDIMENTO PARA COLETA DE DADOS .....	31
4.2	ADEQUAÇÃO DA AMOSTRA.....	32
4.3	PERFIL DEMOGRÁFICO DA AMOSTRA .....	33
<b>5</b>	<b>RESULTADOS DA PESQUISA .....</b>	<b>35</b>
5.1	VALIDAÇÃO DA ESCALA MUIPC PARA M-HEALTH .....	35
<b>5.1.1</b>	<b>Confiabilidade interna, validade convergente e validade discriminante.....</b>	<b>35</b>
<b>5.1.2</b>	<b>Exame do modelo estrutural.....</b>	<b>38</b>
<b>5.1.3</b>	<b>Análise das variáveis de controle.....</b>	<b>40</b>
<b>5.1.4</b>	<b>Análise das variáveis individual dos grupos AGE1 e AGE2.....</b>	<b>45</b>
<b>6</b>	<b>DISCUSSÃO DOS RESULTADOS .....</b>	<b>45</b>
6.1	MODELO E HIPÓTESES DE PESQUISA .....	45
6.2	CONSIDERAÇÕES FINAIS .....	48
<b>7</b>	<b>CONCLUSÃO .....</b>	<b>49</b>
7.1	IMPLICAÇÕES PRÁTICAS .....	49

7.2	LIMITAÇÕES DA PESQUISA E SUGESTÕES PARA ESTUDOS FUTUROS .....	50
	<b>REFERÊNCIAS.....</b>	<b>52</b>
	<b>APÊNDICE A – INFORMAÇÃO DE CONTEXTO.....</b>	<b>57</b>
	<b>APÊNDICE B – INSTRUMENTO DE PESQUISA .....</b>	<b>58</b>

## 1 INTRODUÇÃO

Há mais de uma década *cloud computing* (CC) fora indicado como um modelo tecnológico impulsionador da digitalização na indústria de saúde (Agarwal, Guodong, DesRoches, e Jha, 2010). CC é a entrega de recursos de TI (servidores, rede, bancos de dados, *storage* etc.) sob demanda por meio da Internet com definição de preço e pagamento conforme o uso (Amazon Web Services, 2020; Mell e Grance, 2011; Microsoft, 2020). Conectada às iniciativas de digitalização na saúde, CC entrega benefícios relacionados a redução de custos e eficiência na gestão, a troca, processamento e armazenamento de informações de saúde (Ali, Shrestha, Soar, e Wamba, 2018).

Ao considerar como as tecnologias podem mudar a maneira de se comunicar em saúde, pesquisadores identificaram o crescente interesse em plataformas de gerenciamento de informações centradas no paciente (Agarwal et al., 2010; Yaraghi, Gopal, e Ramesh, 2019). Em 2007, a Microsoft desenvolveu e disponibilizou o *HealthVault*, uma aplicação web baseada em CC para armazenar, compartilhar e gerenciar informações pessoais de saúde, na qual os pacientes tinham controle ativo sobre suas informações (Ali et al., 2018; Ozdemir, Barron, e Bandyopadhyay, 2011). A digitalização em saúde, desde então, segue avançando em ritmo acelerado e novas opções tecnológicas são divulgadas com frequência. Por exemplo, *Mobile Health* (*m-Health*), a tecnologia que usa aplicativos em dispositivos móveis para habilitar a troca de informações de saúde, se tornou um novo canal em substituição ao tratamento de saúde presencial.

Sendo capaz de simplificar o cuidado com saúde e pesquisa médica, *m-Health* pode revolucionar a maneira com a qual indivíduos interagem com seus médicos, clínicas, laboratórios e outros provedores de saúde (Liwei, Baird, e Rai, 2019). Estimativas apontam que em 2019 cerca de 2/3 da população mundial tinham acesso a um *smartphone* (Urbaczewski e Lee, 2020). Essa adesão em massa da tecnologia móvel estimula o interesse de diversos setores, inclusive o da saúde, no desenvolvimento de aplicativos para esse canal. Muitos optam por utilizar a CC em razão de sua capacidade em acelerar o desenvolvimento de aplicações web e móveis, impelindo as empresas no lançamento de novos serviços (Battleson, West, Kim, Ramesh, e Robinson, 2016).

Se aproveitando dos recursos computacionais disponíveis com a CC e a tecnologia disponível com os *smartphones*, em 2014, a Apple lançou seu aplicativo *Health* e uma plataforma para informações de saúde chamada *Healthkit* com a capacidade de integrar dados clínicos com informações de atividade física e bem-estar (Bygstad, 2017). Google Fit e Fitbit

são outros m-Health com as capacidades de coletar, armazenar e processar informações de saúde e bem-estar com uso de CC (Benbunan-Fich, 2019; Kohli e Tan, 2016; Ozdemir et al., 2011).

Os aplicativos m-Health ganharam ainda mais notoriedade com a popularização dos dispositivos vestíveis. Os dispositivos vestíveis (*wearables*, em inglês) são sensores especialmente projetados no formato de um acessório usado ao corpo para coletar métricas de movimentos, descanso ou atividades físicas, com objetivo de melhorar o bem-estar físico das pessoas (Benbunan-Fich, 2019). Estimativas do setor preveem que as despesas dos usuários com dispositivos vestíveis alcance 52 bilhões de dólares em 2020 e mais da metade desta despesa será com dispositivos que permitem o monitoramento de saúde e hábitos de bem-estar (Gartner, 2019).

Quando conectados aos respectivos m-Health<sup>1</sup> e à Internet por meio de *smartphones*, os dispositivos vestíveis são capazes de monitorar a rotina e localização dos usuários. As informações coletadas geralmente são sincronizadas a partir dos *smartphones* com a CC. Na CC, os dados coletados são processados, analisados ou compartilhados com outros usuários para acompanhamento ou gamificação (James, Wallace, e Deane, 2019b), que é inserção nos aplicativos de elementos de jogos, como metas e objetivos, para atividades do dia a dia como, por exemplo, atividades bem-estar. Essa funcionalidade serve de incentivo às pessoas no uso de m-Health e as motivam a mudar seu comportamento com o objetivo de melhorar a saúde e o bem-estar, além de ser uma oportunidade de interagir com outros usuários com os mesmos interesses (James, Wallace, e Deane, 2019a).

Desta forma, m-Health emerge como uma plataforma de saúde para troca de informações. A consultoria de Jones, Hull, e Hakkennes (2019), em sua avaliação, destaca que esse tipo de plataforma é uma inovação tecnológica na indústria de saúde, pois amplia a capacidade de colaboração e interação. Esse relatório também menciona o crescente interesse relacionado com as tecnologias que habilitam a gestão remota de saúde, *e-visits* (também conhecido como telemedicina) e os benefícios resultantes no cuidado com a saúde, como redução de custos e fatores que influenciam as decisões dos pacientes a longo prazo sobre tratamentos médicos.

Os desafios apontados, por outro lado, estão relacionados à escolha da plataforma de saúde pelos indivíduos e sua integração com registros eletrônicos de saúde (EHR) (Gilbert e

---

<sup>1</sup> A partir deste ponto, utilizaremos o termo m-Health para se referir aos aplicativos em dispositivos móveis que, além de serem um canal de interação, também armazenam e processam informações de saúde em uma infraestrutura em CC.

Cribbs, 2020). EHR (*electronic health record*) é uma estrutura baseada em computador para organizar e armazenar dados de saúde e contribui para facilitar o atendimento ao paciente, a colaboração do médico, melhora a qualidade e aumenta o valor do compartilhamento de informações na área da saúde (Angst e Agarwal, 2009; Kohli e Tan, 2016; Strong et al., 2014).

Algumas formas de tratamento, como monitoramento cardíaco, exercícios e prescrições, poderiam ser regularmente monitoradas e compartilhadas com clínicas ou médicos por meio de m-Health (Liwei et al., 2019). Os m-Health podem resolver também um dos grandes dilemas do setor de saúde: a ausência de um histórico confiável de informações de saúde do indivíduo (Kohli e Tan, 2016). Assim, o uso de m-Health para receber tratamento médico e compartilhar informações pode ser uma alternativa para o setor por ser uma tecnologia que oferece benefícios para o tratamento de saúde, ao mesmo tempo que facilita a integração com outras tecnologias por utilizar padrões já em uso pelo setor mencionado.

A capacidade dos m-Health de se integrar a outros sistemas, com diversos envolvidos do setor de saúde, como médicos, clínicas, seguradoras etc., lhes permite ser enquadrados como uma plataforma multilateral (*multisided*, em inglês). Uma plataforma multilateral se refere à uma plataforma com duas ou mais comunidades participantes ativas (Sambamurthy e Zmud, 2017). Para isso, ela precisa ser atraente para as comunidades participantes, criar e maximizar efeitos de rede, isto é, as situações onde o valor ou a demanda por um bem ou serviço cresce exponencialmente em função do seu número de usuários (Sambamurthy e Zmud, 2017; Shapiro, Shapiro, e Varian, 1998).

Para entender a importância de uma plataforma de saúde multilateral, veja o exemplo relacionado à pandemia de COVID-19 em 2020. Durante a pandemia de COVID-19, a Kinsa Health, fornecedora de um termômetro inteligente conectado através de seu m-Health, foi capaz de identificar uma correlação entre o aumento de casos de febre e o surto da COVID-19 na Flórida através da coleta e análise de dados de milhares de termômetros. Essa análise detectou um aumento de enfermidade atípica quando comparado a outros dados de saúde (Klas e Conarck, 2020). Esse monitoramento e volume de informações poderia ajudar na definição de protocolos para tratamento desta enfermidade. Essa correlação só foi possível porque o termômetro inteligente tinha massa crítica, dado o número de consumidores que divulgavam seus dados capturados com o termômetro via m-Health, enviando-os para a consolidação em CC.

Outro exemplo pode ser observado em países como Coreia do Sul, Estados Unidos e Itália que, após o avanço da epidemia, também usaram aplicativos m-Health para combinar dados de contágio da COVID-19 com a localização dos indivíduos capturada através de seus



*smartphones*. O objetivo, além de monitorar e rastrear, era alertar os indivíduos sobre riscos de contágio (Urbaczewski e Lee, 2020).

Ao se estabelecer como uma plataforma multilateral, os m-Health centralizariam um grande volume de informações de saúde, e por ser em essência uma tecnologia centrada no indivíduo, as consequências negativas no caso de comprometimento das informações poderia afetar suas preocupações quanto à privacidade (Agarwal et al., 2010). Experiências negativas no passado envolvendo privacidade também podem aumentar a resistência à assimilação de determinada tecnologia e intensificar as preocupações com relação a privacidade (Smith, Milberg, e Burke, 1996).

Enquanto a digitalização no setor de saúde visa prover um melhor tratamento aos pacientes e é um tema discutido extensivamente desde a última década, ela traz consigo um tema controverso: a privacidade da informação (Agarwal et al., 2010; C. L. Anderson e Agarwal, 2011; Angst e Agarwal, 2009). Por isso, alguns países têm se esforçado em adotar padrões para o uso de dados de saúde. Nos Estados Unidos, o *Health Information Technology for Economic and Clinical Health Act* (HITECH) e o *Health Insurance Portability and Accountability Act* (HIPAA) regulam e definem padrões para o armazenamento, compartilhamento e uso de dados de saúde, sendo esse tema objeto de estudo no passado (Blumenthal, 2010). Ao implementar esses padrões, os m-Health ampliam sua capacidade de interoperar com outros sistemas de informação que também adotem os mesmos padrões.

Para reduzir as preocupações dos indivíduos quanto à privacidade, há leis específicas ao redor do mundo que protegem o dado dos cidadãos. Por exemplo, a *General Data Protection Regulation* (GDPR) (Parlamento Europeu e Conselho Da União Europeia, 27 de abril de 2016), na Europa, e a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018), no Brasil, são exemplos dos controles governamentais para processamento, compartilhamento e armazenamento de dados dos indivíduos por organizações. Essas leis colocam a privacidade do dado como um direito fundamental do indivíduo.

Outros estudos apontam que “o risco de acesso e disseminação não autorizados de informações de saúde digitalizadas e os riscos associados à privacidade do paciente tornaram-se uma das maiores preocupações associadas aos EHRs” (Kim e Kwon, 2019, p. 1185, tradução do autor). Portanto, a capacidade de fornecer mecanismos para dar transparência e controle sobre as questões de privacidade para proteger adequadamente os dados pode ser o motivador para a divulgação de dados pelos indivíduos (Adjerid, Peer, e Acquisti, 2018). Segundo C. Anderson, Baskerville, e Kaul (2017, p. 1084, tradução do autor), “um dos principais desafios para a interoperabilidade [em saúde] é manter a segurança e a privacidade das informações de

saúde protegidas que são transmitidas... [e] os controles de segurança devem ser suficientes para proteger os dados, mas não restritivos a ponto de impedir a interoperabilidade”.

Há disponível uma extensa e robusta literatura que aborda a privacidade da informação como um assunto central em estudos sobre a digitalização do setor de saúde (Agarwal et al., 2010; C. L. Anderson e Agarwal, 2011; Li e Qin, 2017). O tópico privacidade da informação e sua relação com a adoção de tecnologias como EHR, plataformas de troca de dados de saúde e CC foram abordados conforme cada tecnologia ganhava mais relevância (Ali et al., 2018; C. L. Anderson e Agarwal, 2011; Angst e Agarwal, 2009; Gao e Sunyaev, 2019; Keil, Park, e Ramesh, 2018; Li e Qin, 2017; Yaraghi et al., 2019).

Assim, os m-Health constituem um avanço tecnológico, capaz de aumentar a eficiência da prática médica, facilitar o acompanhamento médico e melhorar o cuidado com saúde e investigar as preocupações com privacidade na assimilação desta tecnologia pela divulgação de dados e uso dessa plataforma poderão trazer contribuições para a literatura e a prática. Fazendo uso do instrumento *Mobile Users' Information Privacy Concerns* (MUIPC), de Xu, Gupta, Rosson, e Carroll (2012), que foi projetado para estudo de preocupações quanto a privacidade no uso de aplicativos móveis, este estudo endereçará essa questão.

## 1.1 QUESTÃO DE PESQUISA

Baseado no contexto apresentado, nesse estudo será explorada a seguinte pergunta de pesquisa: como as preocupações com privacidade afetam a disposição dos indivíduos em divulgar informações de saúde em m-Health?

## 1.2 OBJETIVO

Esse estudo tem como objetivo investigar as preocupações dos indivíduos com relação a privacidade ao ter seus dados de saúde processados com m-Health. Os objetivos específicos são:

- estabelecer a base teórica relacionada às preocupações de privacidade no uso de informações de saúde com CC a partir de aplicativos móveis;
- validar a aplicabilidade da escala MUIPC no domínio de aplicativos móveis que usam CC para informações de saúde;
- analisar se características sociodemográficas de gênero, idade e renda moderam a relação das preocupações com privacidade com o uso de m-Health;
- discutir as implicações deste estudo focado nas preocupações com privacidade no uso de m-Health para a prática de saúde.

Este estudo de validação do modelo metodológico, que envolve também uma pesquisa confirmatória, utiliza a técnica de equações estruturais para avaliar tanto a validade do modelo de mensuração como do modelo de estrutural, e examina os relacionamentos entre os construtos e variáveis de controle.

### 1.3 JUSTIFICATIVA

O estudo de privacidade da informação na área de saúde é amplamente coberto quando se faz um levantamento da literatura sob diversas perspectivas, dada a sua relevância para o segmento de saúde e sistemas de informação (C. L. Anderson e Agarwal, 2011; Angst e Agarwal, 2009; Keil et al., 2018; Kim e Kwon, 2019; Li e Qin, 2017; Yaraghi et al., 2019). No entanto, quando se utiliza as palavras-chave “privacidade”, “saúde”, “*cloud computing*” e “aplicativos móveis” na busca de artigos nas bases de dados como o Google Scholar ou nas que compõem o *AIS Senior Scholars’ Journal Basket* (Lowry et al., 2013), percebe-se que privacidade em m-Health é um tema ainda pouco explorado.

Alguns estudos têm examinado a adoção de determinada tecnologia no setor de saúde frente os desafios relacionados com privacidade (Tabela 1). Diante da literatura disponível vê-se a oportunidade de ampliar a pesquisa no estudo das preocupações com privacidade no uso de m-Health e convém escolher uma escala adequada que consiga capturar os indicadores necessários para sua validação.

**Tabela 1** – Tecnologias e pesquisas relacionadas com privacidade em saúde

Contexto de Pesquisa	Instrumento Base	Estudos prévios
Informações Pessoais de Saúde	CPM e <i>Risk-as-feelings</i>	C. L. Anderson e Agarwal (2011)
EHR	CFIP	Angst e Agarwal (2009)
Plataforma Multilateral de saúde	CPM	Yaraghi et al. (2019)
Cloud Computing e Saúde	Análise da literatura	Gao e Sunyaev (2019)

Fonte: Elaborado pelo autor (2021).

No Brasil, o governo trabalhou com um horizonte para 2020 para promover o uso e o compartilhamento de EHR, criando um sistema de informação de saúde chamado “e-Saúde”, um sistema de informação nacional, com o objetivo de proporcionar “uma diversidade de benefícios disponibilizados aos pacientes, cidadãos, profissionais de saúde, gestores, autoridades e organizações de saúde” (Brasil, 2017). Além disso, desde 2016, o Ministério da Saúde do Brasil busca implantar o Prontuário Eletrônico do Cidadão, com o fim de integrar as informações de saúde dos cidadãos tratados no Sistema Único de Saúde (SUS) (Brasil, 2016).

Esse projeto se tornou o Rede Nacional de Dados em Saúde (RNDS), que é uma plataforma nacional de integração de dados em saúde, cujo lançamento foi impulsionado com o surgimento da pandemia de COVID-19 (Brasil, 2020). Entretanto, estudos recentes concluíram que os níveis de participação dos indivíduos em plataformas de saúde adotadas por hospitais e clínicas são baixos devido às preocupações com a privacidade (Yaraghi et al., 2019).

Portanto, ao examinar as preocupações com privacidade sob a perspectiva dos indivíduos no uso plataformas de saúde baseadas em m-Health este estudo traz contribuição para a prática e pode ajudar as organizações governamentais e privadas em sua estratégia de definir ou implementar uma plataforma multilateral na indústria de saúde.

#### 1.4 ESTRUTURA DO TRABALHO

O presente trabalho, com a Introdução, está organizado em 7 capítulos. O capítulo a seguir (2) cobre a revisão de literatura que dá o embasamento científico para ao tema e a questão de pesquisa. Segue-se então o capítulo (3), o qual oferece o modelo de pesquisa com o desenvolvimento das hipóteses, o capítulo (4), que consta a metodologia, o capítulo (5) é dedicado aos resultados da pesquisa, o capítulo (6) envolver a discussão dos resultados com as contribuições teóricas e, finalmente, o capítulo (7) oferece a conclusão do trabalho apresentando as contribuições práticas, as limitações deste estudo e sugestão para futuros estudos.

## 2 BASE TEÓRICA

Neste capítulo será apresentada a fundamentação teórica para nosso estudo relacionado às preocupações com privacidade no uso de m-Health. O primeiro passo será examinar os conceitos relacionados à privacidade da informação. Na sequência, nos aprofundaremos no tópico sobre privacidade da informação em saúde com focos no uso de registros eletrônicos de saúde, em plataforma multilateral e em CC. Por fim, analisaremos a privacidade da informação no uso de m-Health.

### 2.1 PRIVACIDADE DA INFORMAÇÃO

Privacidade da informação pode ser definida como a capacidade de dar controle ao indivíduo sobre suas informações pessoais (Smith et al., 1996) para que possam determinar quando, como e com quem elas possam ser compartilhadas (Naresh K. Malhotra, Sung, e Agarwal, 2004). Com o avanço da digitalização, as informações pessoais passaram a ser facilmente copiadas, transmitidas ou integradas, aumentando as ameaças relacionadas à privacidade (Naresh K. Malhotra et al., 2004) a ponto de, para alguns autores, a privacidade da

informação ser uma das questões éticas mais importantes da era da informação (Adjerid, Peer, et al., 2018; Smith et al., 1996; Stewart e Segars, 2002).

Em seu estudo, Smith, Dinev, e Xu (2011) discutem que o conceito de privacidade da informação está em constante evolução e que segue a evolução da tecnologia da informação, como apresentado no Tabela 2 abaixo. Como citado por Xu et al. (2012) e Smith et al. (2011), categoriza-se privacidade como um direito humano, como uma mercadoria, como um estado de acesso limitado e como a capacidade de controlar informações sobre si mesmo.

**Tabela 2** – Evolução do Conceito de Privacidade da Informação e a Evolução da TI

Período	Características
Cenário base privacidade 1945-1960	Desenvolvimentos limitados de tecnologia da informação, alta confiança do público no setor governamental e empresarial e conforto geral com a coleta de informações.
1ª era do desenvolvimento contemporâneo da privacidade 1961-1979	Aumento da privacidade das informações como uma questão explícita social, política e legal. Formulação da Estrutura de <i>Fair Information Practices</i> (FIP) e estabelecimento de mecanismos regulatórios governamentais estabelecidos como a Lei de Privacidade de 1974.
2ª era de desenvolvimento de privacidade 1980-1989	Aumento dos sistemas de computador e rede, recursos de banco de dados, legislação federal projetada para canalizar as novas tecnologias para o FIP, incluindo a Lei de Proteção à Privacidade de 1984. Os países europeus adotam leis nacionais de proteção de dados para os setores público e privado
3ª Era do Desenvolvimento da Privacidade 1990 – data atual	A ascensão da Internet, da Web 2.0 e do ataque terrorista de 11 de setembro de 2001 mudou dramaticamente o cenário da troca de informações. As preocupações relacionadas sobre privacidade atingiram novos níveis.

Nota: Smith et al. (2011, p. 991, tradução do autor)

Como não há possibilidade de mensurar privacidade, dada as características mencionadas, muitos estudos passaram a medir preocupações com privacidade como principal construto (Smith et al., 2011) e, para isso, alguns modelos foram desenvolvidos. Por exemplo, Smith et al. (1996) elaboraram a escala *Concern for Information Privacy* (CFIP) que se aplica principalmente no estudo das preocupações dos indivíduos com privacidade na prática organizacional. Angst e Agarwal (2009) integraram ao CFIP o *Elaboration Likelihood model* para examinar a adoção de sistemas baseados em EHR. Naresh K. Malhotra et al. (2004) criaram a escala *Internet Users' Information Privacy Concerns* (IUIPC) que auxilia no estudo das preocupações com privacidade dos indivíduos que são usuários da Internet. Essa escala foi referenciada por alguns autores no estudo de privacidade na área de saúde (Agarwal et al., 2010; C. L. Anderson e Agarwal, 2011). A teoria proposta por Petronio (2002), denominada *Communication Privacy Management*, explica como os indivíduos gerenciam a divulgação ou encobrem suas informações privadas em diversos contextos, inclusive saúde. C. L. Anderson e

Agarwal (2011) incorporaram esta teoria ao modelo *risk-as-feelings* para examinar os motivadores na divulgação de informações pessoais de saúde.

Como diferentes tipos de informação pessoal, mecanismos de proteção, captura e finalidade de uso podem ter diferentes influências no comportamento do indivíduo na divulgação de suas informações e, embora o setor de saúde possua características únicas, a principal dessas características são as preocupações com privacidade (Lin, Chen, Brown, Li, e Yang, 2017). Sendo assim, o modelo elegido para este estudo foi o MUIPC, concebido por Xu et al. (2012) especialmente para examinar as preocupações com privacidade dos indivíduos no uso de dispositivos móveis. O modelo MUIPC será analisado com mais detalhes a partir do capítulo 3.

## 2.2 PRIVACIDADE DA INFORMAÇÃO EM SAÚDE

### 2.2.1 Privacidade da informação no uso EHR

EHR flexibiliza a integração dos dados de pacientes por estabelecer um padrão para a troca de informações entre diferentes sistemas computacionais de saúde, inclusive através da Internet (Kohli e Tan, 2016). Essa capacidade “facilita muito a disponibilidade de informações completas sobre a saúde do paciente” (Ozdemir et al., 2011, p. 491, tradução do autor). O uso de EHR elimina erros de grafia e erros com diagnósticos resultantes de documentos ilegíveis escritos à mão (James Bender e Mecklenburg, 2017). Atualmente, o EHR é o principal padrão adotado por sistemas computacionais na área da saúde (Yaraghi et al., 2019).

A ampla adoção de EHR viabilizou a troca de informações de saúde entre os diversos envolvidos no setor e essa possibilidade é hoje mais importante do que nunca (Yaraghi et al., 2019). No entanto, a interoperabilidade impulsionada pelo uso de EHR agrava as preocupações com privacidade. Pesquisa anterior já discutiu a relevância do tema “privacidade de informações de saúde” e as questões que surgiam estavam relacionadas à quanta informação precisa ser disponibilizada, como e para quem (Angst e Agarwal, 2009). Por facilitar a troca e distribuição das informações entre os diferentes interessados, EHR apresenta dificuldades em capturar e controlar o consentimento do paciente na divulgação e compartilhamento de suas informações (Angst e Agarwal, 2009; Kim e Kwon, 2019; Yaraghi et al., 2019; Yaraghi, Ye Du, Sharman, Gopal, e Ramesh, 2015).

Fatores adicionais que implicam as preocupações com privacidade estão relacionados com a governança sobre os dados, propriedade, apropriação da informação e também envolvem os dispositivos que controlam a guarda, compartilhamento e manutenção da informação (Kohli

e Tan, 2016). Outro componente agravante para as preocupações com a privacidade da informação com o uso de EHR é a facilidade para transmitir informações de saúde através da Internet (Angst e Agarwal, 2009).

### **2.2.2 Privacidade da informação em uma plataforma multilateral de saúde**

A disponibilização de uma base estruturada e padronizada de informações de saúde possibilita a melhoria dos serviços e redução de custos em saúde (Adjerid, Adler-Milstein, e Angst, 2018; Yaraghi et al., 2015), além de facilitar o compartilhamento e a organização de um histórico completo de saúde dos pacientes (Ozdemir et al., 2011). Essas competências ajudam a identificar fatores que descrevem o estado de saúde de um indivíduo (Kohli e Tan, 2016).

Estudos estimam que a unificação das informações de saúde em uma plataforma multilateral de informações de saúde (PMIS) pode reduzir em centenas de bilhões de dólares por ano as despesas com saúde (Adjerid, Adler-Milstein, et al., 2018; Ozdemir et al., 2011; Yaraghi et al., 2019; Yaraghi et al., 2015). Os benefícios relacionados à integração de dados, planejamento, investigação clínica e gestão de saúde pressionam governos, como por exemplo o governo brasileiro, na implementação de uma plataforma única de saúde (Brasil, 2016).

No entanto, os desafios para gerenciar e proteger a privacidade das informações dos pacientes são barreiras na expansão de uma PMIS (Yaraghi et al., 2019). Para o uso e operacionalização de uma PMIS é necessário capturar o consentimento dos pacientes quanto ao uso de suas informações pessoais e de saúde (Yaraghi et al., 2019; Yaraghi et al., 2015). A capacidade de controlar o consentimento é resultado do desejo dos indivíduos por maior controle sobre suas informações, acentuado pelo aumento da preocupação com privacidade em razão do volume e natureza das informações envolvidas (Kohli e Tan, 2016).

Uma PMIS permite o acesso completo ao registro histórico do paciente para prover um tratamento de saúde mais apropriado, suporta as decisões médicas e direciona questões de saúde pública, minimizando tratamentos redundantes (Adjerid, Adler-Milstein, et al., 2018; Kohli e Tan, 2016). Entretanto, restringir o acesso e controlar a privacidade das informações do paciente diante dos múltiplos envolvidos com distintos interesses são tópicos importantes e, por isso, desconsiderar esse tema comprometeria o sucesso e os potenciais benefícios trazidos por esta plataforma (Yaraghi et al., 2019).

### **2.2.3 *Cloud computing* e a privacidade da informação**

A crescente adesão de CC na saúde pode, em princípio, reduzir custos com infraestrutura e operação de tecnologia computacional pela economia de escala (Agarwal et al., 2010; Gao e Sunyaev, 2019). A combinação do uso de CC e EHR é um estímulo à integração e interoperabilidade de informações de saúde (Ozdemir et al., 2011), pois CC é uma tecnologia adequada para o compartilhamento de dados entre diferentes sistemas através da Internet, trazendo agilidade e flexibilidade, enquanto EHR é um modelo padrão definido para este tipo de dado (Ali et al., 2018).

Por reduzir a sobrecarga operacional e obsolescência de uma arquitetura “*on-premises*”, onde as instituições de saúde são responsáveis por manter a infraestrutura de hardware e software local (Gao e Sunyaev, 2019), CC é uma opção viável para o setor de saúde (Ali et al., 2018). Nos últimos 15 anos, vários fornecedores de tecnologia – como, IBM, Microsoft, Dell e GE – aproveitando esta oportunidade, lançaram soluções para o armazenamento e processamento de informações de saúde destinado às empresas de cuidados de saúde (Ali et al., 2018; Sultan, 2014).

Várias ameaças, porém, são capazes de restringir a aceitação de CC em saúde. Algumas dessas ameaças são criptografia fraca, acesso público ao dado, vírus, *malwares*, além de questões relacionadas ao uso do dado (Ali et al., 2018). Essas ameaças se relacionam com o fator determinante na adoção de CC em saúde: a preocupação com privacidade no tratamento de informações sensíveis (Battleson et al., 2016). Se os indivíduos não confiarem que suas informações pessoais de saúde serão tratadas adequadamente, eles podem relutar em divulgar informações confidenciais ou sensíveis (Keil et al., 2018).

Algumas pesquisas indicam que as preocupações com privacidade das informações de saúde para uso com CC são um dos principais obstáculos a serem superados (Gao e Sunyaev, 2019; Sultan, 2014). Em seu estudo Kim e Kwon (2019) recomendam a implementação de certificados e diretivas na implementação de controles de privacidade no uso de EHR, o que desafia os prestadores e provedores de serviços em saúde a atender certos padrões relacionados a privacidade e segurança de dados.

## 2.3 M-HEALTH

### 2.3.1 Privacidade de informações

A transação primária em uma plataforma m-Health é a informação de saúde do indivíduo que pode ser estruturado seguindo padrões EHR para facilitar o acesso e a interoperabilidade (Ozdemir et al., 2011). Já o uso de CC flexibiliza a integração dos dados

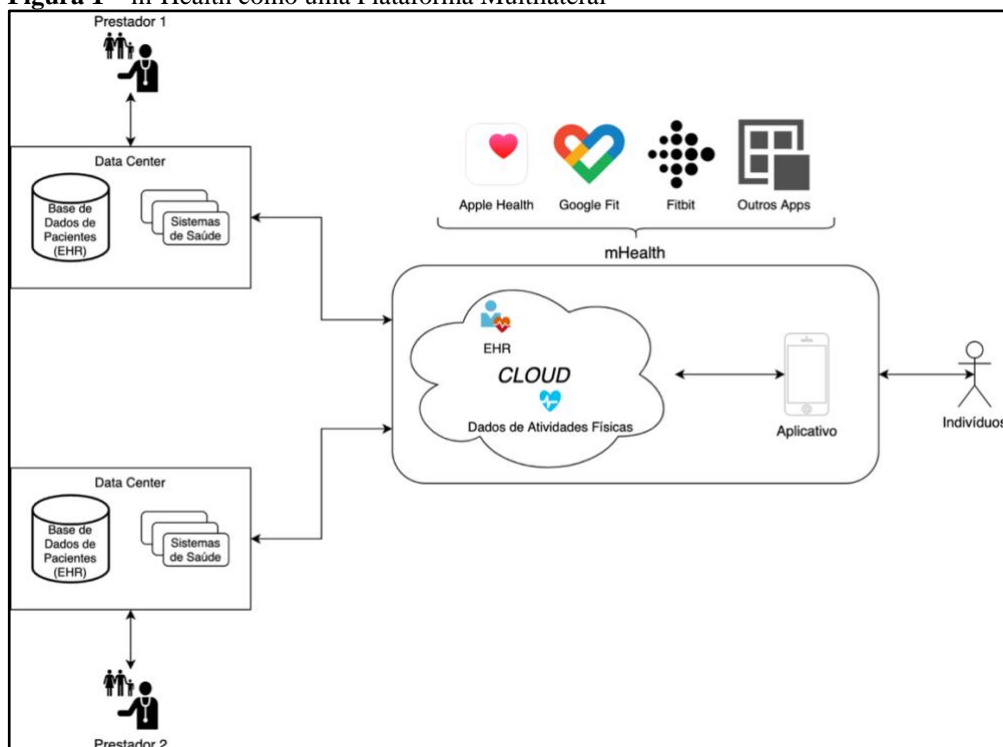


entre diferentes sistemas e partes interessadas, além de estimular a colaboração (Gao e Sunyaev, 2019). Essas características possibilitam que os m-Health atuem como um canal intermediário conectando indivíduos, prestadores, provedores e outros interessados na área de saúde. Como apresentado na Figura 1, os m-Health funcionam como uma plataforma multilateral, patrocinadora da rede, com os indivíduos e demais interessados como elementos pertencentes à rede (Shapiro et al., 1998) . Aplicativos populares de saúde que possuem as características que definem os m-Health são Apple Health, Google Fit ou Fitbit.

A centralização de grandes volumes de informações de saúde com m-Health, onde a informação de saúde dos indivíduos da rede possa ser ativamente analisada, faz com que seja possível verificar, por exemplo, tendências de contágio, avanço de doenças e disparo de alertas para partes interessadas (Sultan, 2014). No entanto, o volume de informações trafegada amplia os desafios relacionados com a privacidade de dados (Yaraghi et al., 2019).

Juhee e Eric Johnson (2018) destacam os desafios relacionados à integração para compartilhamento de informações de saúde, as medidas de segurança de dados necessárias para isso e enfatizam o alto número de pacientes comprometidos com vazamento de dados. Uma plataforma que implemente o uso de EHR tem como consequência o armazenamento de uma grande quantidade de dados clínicos digitalizados transitando pela Internet e, na eventualidade de um comprometimento da plataforma, uma das principais consequências seria o prejuízo com a confidencialidade dos dados do paciente (Agarwal et al., 2010).

**Figura 1** – m-Health como uma Plataforma Multilateral



Fonte: Elaborado pelo autor (2021).

De acordo com o HIPAA, do ponto de vista legal, o uso de padrões dá aos pacientes mais controle sobre suas informações de saúde, estabelece limites para o uso e liberação de registros de saúde e define procedimentos apropriados que os prestadores de cuidados de saúde e outros devem seguir para proteger a privacidade das informações de saúde (Estados Unidos da América, 21 de agosto de 1996). Por oferecer os controles para obter o consentimento com o objetivo de armazenar e processar as informações de saúde, aplicativos transferem o controle e autonomia dos dados para os pacientes. Yaraghi et al. (2015) observaram que capturar o consentimento do paciente antes de que qualquer interessado possa acessar seus registros médicos pode reduzir as preocupações dos indivíduos quanto à privacidade das suas informações, pois estes passariam a ser informados de antemão sobre como seus dados serão tratados.

Os dados de saúde pertencem aos pacientes e estes deveriam ter o poder de decidir como usar, com quem compartilhar e ter controle sobre seu dado (Sultan, 2014). Dar aos indivíduos controle sobre suas informações de saúde pode estimular positivamente a intenção de divulgação de dados entre interessados do setor e a adoção de determinada tecnologia (Kim e Kwon, 2019; Li e Qin, 2017; Yaraghi et al., 2019).

A percepção de maior controle e proteção dos dados também pode resultar em uma maior disposição dos indivíduos de revelar informações de saúde nessas plataformas e uma menor preocupação com sua privacidade ao usá-las (Adjerid, Peer, et al., 2018). “O mero aumento no controle percebido sobre quem pode acessar e usar informações pessoais on-line pode resultar em uma maior probabilidade de fazer divulgações sensíveis e arriscadas” (Adjerid, Peer, et al., 2018, p. 468, tradução nossa).

Contudo, em uma plataforma composta por diversos interessados, pode ser difícil conseguir o acordo com todas as partes, consentindo com os termos que endereçam as preocupações dos indivíduos com privacidade e sejam aderentes às regulamentações focadas na proteção dos dados de saúde e outros dados sensíveis (Adjerid, Adler-Milstein, et al., 2018). Essa combinação de fatores, contribuem para ampliar a importância do estudo sobre privacidade para uso de m-Health.

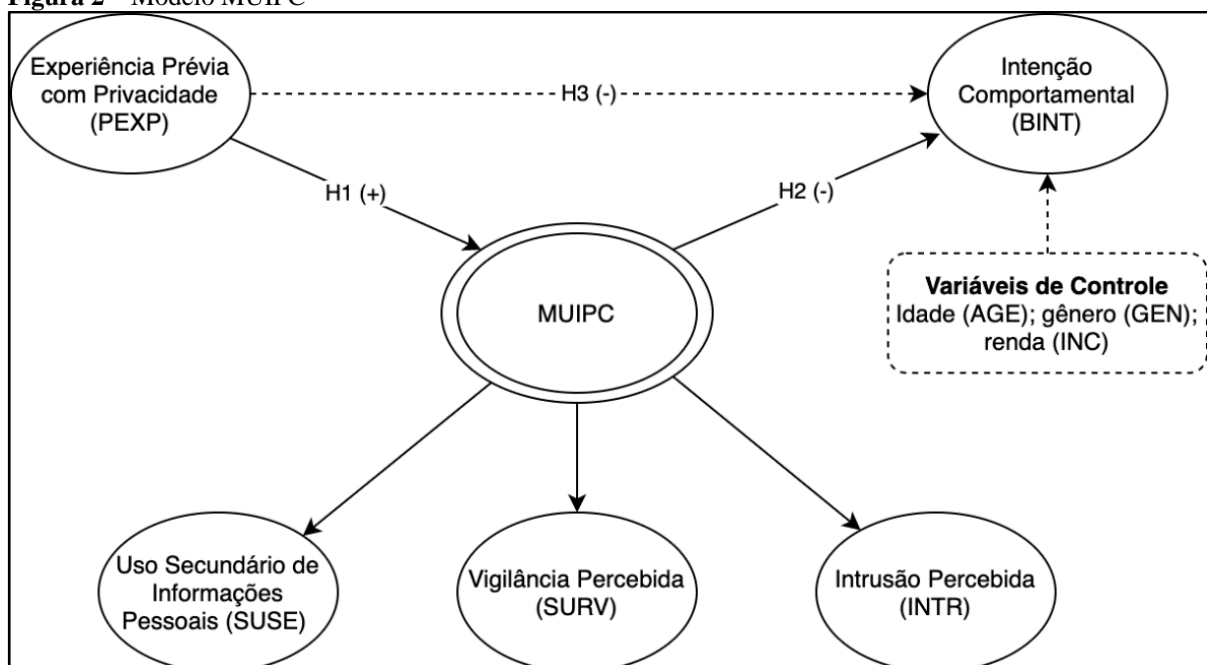
Em 2010, Agarwal et al. (2010) ao examinar temas de interesse para os anos seguintes, destacaram a importância de ferramentas que transferem aos pacientes o controle sobre suas informações de saúde e bem-estar e discutiram a relevância de pesquisar a perspectiva dos indivíduos quanto as preocupações com a privacidade de suas informações de saúde em um modelo centrado no paciente (*patient-centric*).

Por meio da análise desses estudos foi possível observar que a preocupação com privacidade é capaz de influenciar negativamente a intenção do indivíduo na divulgação de informações em tecnologias na indústria de saúde, seja no uso de EHR (Angst e Agarwal, 2009; Kim e Kwon, 2019; Yaraghi et al., 2019; Yaraghi et al., 2015), em uma plataforma multilateral de saúde (Yaraghi et al., 2019; Yaraghi et al., 2015) ou no uso de CC (Gao e Sunyaev, 2019; Sultan, 2014), o que permite supor que o mesmo comportamento poderá se apresentar no uso de m-Health.

### 3 MODELO DE PESQUISA

MUIPC, *mobile users' information privacy concerns*, é o modelo proposto por Xu et al. (2012) construído sobre os modelos CFIP (Smith et al., 1996), IUIPC (Naresh K. Malhotra et al., 2004) e, principalmente, CPM (Petronio, 2002). Foi desenhada exclusivamente para o estudo das preocupações com perda da privacidade no contexto do uso de dispositivos móveis, mas também foi utilizada em estudos relacionados ao uso de dispositivos vestíveis (Wiegard, Guhr, Krylow, e Breitner, 2019). Esta escala, apresentada na Figura 2, está dividida em três dimensões de primeira ordem: vigilância percebida, intrusão percebida e uso secundário de informações pessoais.

**Figura 2** – Modelo MUIPC



Nota: Adaptado de Xu et al. (2012, tradução do autor).

Apesar do termo CC estar relacionado ao uso de recursos computacionais através da Internet (Mell e Grance, 2011) e a escala IUIPC ser desenhada especificamente para estudos concernentes às preocupações com privacidade através da Internet (Naresh K. Malhotra et al.,

2004), a inclusão do contexto de aplicativos móveis faz com que a escala MUIPC seja a mais adequada para este estudo. Além disso, estudos recentes se basearam nessa escala para examinar o efeito das preocupações com privacidade no uso de informações de bem-estar por dispositivos móveis (Vitak, Liao, Kumar, Zimmer, e Kritikos, 2018), bem como do consentimento de permissões por aplicativos móveis (K. Degirmenci, 2020).

Na escala proposta por Xu et al. (2012), MUIPC é o construto de maior ordem mensurado em um relacionamento reflexivo com os de menor ordem – vigilância percebida (SURV), intrusão percebida (INTR) e uso secundário de informações pessoais (SUSE) – que, por sua vez, são mensurados por indicadores reflexivos.

Vigilância percebida é descrita como o monitoramento e análise de perfil dos usuários de dispositivos móveis através do uso dos recursos tecnológicos embutidos e disponíveis (Xu et al., 2012). A coleta de dados pelos dispositivos é o ponto de partida para as preocupações com privacidade (Naresh K. Malhotra et al., 2004) e essa pode ser feita pelos sensores, câmeras, e os aplicativos presentes no dispositivo ou conectados a ele (Xu et al., 2012). “Usuários de dispositivos móveis resistem aos aplicativos móveis por temer que suas atividades possam ser assistidas, gravadas e transmitidas a várias entidades” (Xu et al., 2012, p. 4, tradução do autor). Isso aconteceria se as informações integradas ao m-Health para visão única do estado de saúde dos indivíduos fossem divulgadas através da CC para uso impróprio.

Intrusão é a invasão do espaço pessoal do indivíduo que pode perturbar sua rotina ou solidão causando-lhe desconforto (Solove, 2006). Ela está relacionada ao uso não autorizado ou malicioso da informação pelo destinatário, que pode tirar proveito desse acesso para uso indevido das informações (Xu et al., 2012). Pelo fato de os m-Health armazenarem e processarem informações sensíveis e, em alguns casos, confidenciais, se estas informações forem acessadas por outros aplicativos indevidamente, os usuários podem criar resistência para novos compartilhamentos em função deste acesso indesejado.

O uso secundário de informações pessoais é a coleta das informações dos indivíduos para uma finalidade diferente da inicialmente autorizada (Smith et al., 1996). No caso de m-Health, o uso secundário de informações pessoais está ligado, por exemplo, ao uso promocional das informações de saúde dos indivíduos ou para fins de análise de perfil de saúde, sem seu consentimento. Essa situação pode ser considerada vazamento de informações, criando uma sensação de vulnerabilidade e falta de controle (Xu et al., 2012).

Xu et al. (2012) validaram o construto MUIPC ao posicioná-lo mediando dois outros construtos: experiência prévia com violação de privacidade e intenção comportamental. Experiência prévia com violação de privacidade (PEXP) é descrita como a exposição ou

invasão da privacidade que resultaria em mal uso dos dados do indivíduo que, como consequência, teria fortes preocupações com a privacidade de seus dados (Smith et al., 1996).

Naresh K. Malhotra et al. (2004) definem intenção comportamental (BINT) como a disposição do indivíduo em fornecer informações pessoais em determinado meio. Se refere a probabilidade de uma pessoa se comportar de uma forma específica ao utilizar determinada tecnologia. Na área de saúde foi um construto usado para medir aspectos do comportamento que relacionam a adoção e uso de determinada tecnologia que envolvem divulgação de dados pessoais (Angst e Agarwal, 2009) e, no contexto dessa pesquisa, a mesma definição se aplica, pois esta se refere a disposição do indivíduo em adotar ou usar m-Health e divulgar suas informações pessoais de saúde.

Ainda que Xu et al. (2012) tenham testado o modelo MUIPC para entender as preocupações com privacidade de usuários de aplicativos móveis e Silva Junior (2015) e Silva Junior, Luciano, e Lübeck (2020) tenham testado essa escala no contexto brasileiro, esse estudo se propõe também a averiguar a aderência da escala para o uso de aplicativos móveis que utilizem CC como uma segunda camada tecnológica e também examinar a influência das variáveis de controle gênero, idade e renda.

### 3.1 HIPÓTESES DE PESQUISA

Através da escala MUIPC, esse estudo pretende endereçar a pergunta de pesquisa que tem como propósito investigar as preocupações com privacidade no uso de m-Health, analisando os construtos de primeira ordem da escala MUIPC – vigilância percebida, intrusão percebida e uso secundário de informações pessoais (Xu et al., 2012). Xu et al. (2012) também propõem MUIPC como mediador dos construtos entre segunda ordem experiência prévia com privacidade (Smith et al., 1996) e intenção comportamental, ou intenção de divulgação de informações pessoais (Naresh K. Malhotra et al., 2004).

Como fundamentado na análise teórica, o grande número de dados trafegando pela Internet incrementa o risco de exposição das informações dos indivíduos e, se por uma experiência negativa com privacidade no passado, esses não confiarem que suas informações pessoais de saúde serão tratadas adequadamente, eles podem relutar em divulgar informações confidenciais ou sensíveis (Keil et al., 2018) e indivíduos expostos a violação de privacidade no passado apresentam maiores preocupações com privacidade por temerem o mal uso de suas informações pessoais (Smith et al., 1996). Assim, foi proposta a seguinte hipótese:

**H1:** Experiência anterior com violação de privacidade influencia positivamente as preocupações com privacidade da informação no uso de m-Health.

Estudos anteriores na área de sistemas de informação já explicaram o efeito negativo das preocupações com privacidade na intenção comportamental para divulgação de informações pessoais dos indivíduos (Adjerid, Peer, et al., 2018; Smith et al., 1996; Xu et al., 2012), inclusive relacionados com saúde (C. L. Anderson e Agarwal, 2011). Com base nessas evidências, pode-se presumir que as preocupações com privacidade também influenciam negativamente o uso de m-Health pelos indivíduos. O risco de acesso e disseminação não autorizados de informações de saúde e os riscos associados à privacidade do paciente são fatores preponderantes para tomada de decisão e para a adoção de uma plataforma de troca de dados de saúde (C. L. Anderson e Agarwal, 2011; Angst e Agarwal, 2009; Yaraghi et al., 2019). Estima-se então que o aumento das preocupações de privacidade, eventualmente, pode levar a uma redução na disposição dos indivíduos em adotarem m-Health para divulgarem informações de saúde. A partir desse argumento, é proposta a seguinte hipótese:

**H2:** Preocupações com privacidade da informação no uso de m-Health influenciam negativamente a intenção comportamental.

Xu et al. (2012) posicionaram MUIPC como mediador entre experiência prévia com violação de privacidade com intenção comportamental. Indivíduos que foram vítimas de violação de suas informações pessoais tem fortes preocupações com privacidade e, por sua vez, maiores preocupações com privacidade aumentam a probabilidade de recusa da divulgação de suas informações pessoais ou uso de soluções que as solicitam (Smith et al., 1996; Stewart e Segars, 2002). Com o objetivo de examinar este argumento, propõe-se a seguinte hipótese:

**H3:** Preocupações com privacidade da informação no uso de m-Health mediam a relação entre experiência anterior com perda de privacidade e a intenção comportamental.

### 3.2 VARIÁVEIS DE CONTROLE

Com o objetivo de avaliar o efeito moderador das características sociodemográficas na Intenção Comportamental e ampliar a pesquisa anterior publicada por Xu et al. (2012), variáveis de controle foram incluídas no modelo. Variáveis de controle podem afetar ou influenciar as variáveis dependentes e, por isso, “desempenham um papel ativo em estudos quantitativos” (Creswell, 2012, p. 107). Estudo anterior que examinou as preocupações com privacidade no uso de EHR (C. L. Anderson e Agarwal, 2011) identificou diferenças entre diversas variáveis de controle sociodemográficas. Além disso Yaraghi et al. (2019) destacam o papel da variável de controle “gênero” em influenciar os indivíduos ao formar opiniões quanto à privacidade de suas informações. Sendo assim, decidiu-se analisar no modelo o efeito moderador das variáveis gênero (GEN), renda (INC) e idade (AGE).

## 4 METODOLOGIA

Esta é uma pesquisa que usa uma abordagem quantitativa com uma estratégia de investigação de levantamento de seção cruzada, onde os dados foram coletados em um único intervalo de tempo que permite extrair uma descrição quantitativa ao estudar uma amostra de uma população (Creswell, 2012).

O aplicativo SmartPLS versão 3.3.2 foi usado neste estudo como ferramenta para analisar os resultados, validar empiricamente as hipóteses levantadas e a escala escolhida (MUIPC). PLS é usada no desenvolvimento e extensão de teorias em pesquisas confirmatórias. PLS-SEM é uma técnica analítica de variância com modelagem por equações estruturais que permite simultaneamente explorar as relações entre as variáveis latentes (construtos) e os indicadores, visando maximizar a variância em uma modelagem conceitual causal (Chin, 1998; Fornell e Bookstein, 1982). Usando as capacidades da ferramenta, primeiro foi avaliada a confiabilidade e validade do modelo, antes de se testar o modelo estrutural.

A escolha do algoritmo PLS-SEM se deve ao fato dessa técnica permitir simultaneamente testar a escala e estimar o modelo estrutural, além de ser adequada para modelos com uma amostra reduzida (Chin, Marcolin, e Newsted, 2003). Os construtos estão alinhados com a escala definida por Xu et al. (2012), usando indicadores reflexivos, em uma escala reflexiva-reflexiva.

### 4.1 PROCEDIMENTO PARA COLETA DE DADOS

Devido à estratégia de investigação, optou-se pela coleta de dados através de uma *survey*. Esta técnica de coleta consegue explicar as razões e fontes de eventos, características e correlações observadas e facilita a aplicação cuidadosa do pensamento lógico, além de ser empiricamente verificável (Babbie, 1999). O *survey* enviado incluiu questões sociais e demográficas, como renda, gênero e idade, que auxiliaram na análise estrutural do modelo.

Como o objetivo principal desse estudo é examinar a preocupação dos indivíduos com privacidade no uso de m-Health, o questionário apresentado forneceu informação contextual sobre a função dos aplicativos de saúde, seu armazenamento na nuvem e as principais questões envolvidas com o intuito de compartilhar um entendimento comum sobre a questão principal.

Os respondentes, não necessariamente já deveriam ser usuários ativos de m-Health, pois a intenção comportamental faz parte do escopo da pesquisa. Antes da fase de coleta de dados foi necessária a tradução da escala desenvolvida por Xu et al. (2012) e, para tal, utilizou-se como referência a tradução realizada por Silva Junior (2015) e Silva Junior et al. (2020), que já

havam traduzido a escala MUIPC usando retrotradução, técnica usada para identificar erros de tradução (N.K. Malhotra, 2006).

O estudo procurou obter com clareza o consentimento dos respondentes, uma vez que a intenção era capturar informações pessoais e sensíveis com o fim de cumprir com questões éticas (Creswell, 2012). Além disso, assegurou-se que as informações compartilhadas seriam anônimas e confidenciais. Para evitar ambiguidade, a pesquisa apresentou definições claras dos conceitos envolvidos e seus objetivos (APÊNDICE A), baseados na definição da literatura disponível (Ali et al., 2018; Mell e Grance, 2011; Ozdemir et al., 2011; Yaraghi et al., 2015) e a escala usada incluiu dimensões e itens bem estabelecidos.

O questionário construído usando a plataforma *Google Forms* e sua validade foram verificados com a submissão a um pré-teste para 20 estudantes de pós-graduação *strictu sensu*, entre os dias 13 a 15 de setembro de 2020, escolhidos por conveniência. Ao final do pré-teste, apenas um ajuste em uma questão demográfica (Renda Familiar) foi recomendada alteração pois faltava um intervalo entre os valores e foi aceita.

Entre 24 de setembro e 20 de outubro de 2020, o questionário foi distribuído através de posts e artigos nas redes sociais WhatsApp e LinkedIn, resultando em uma amostra por conveniência, uma vez que os participantes voluntariamente decidiram participar da pesquisa (Creswell, 2012). Para coleta de dados foi utilizada também uma técnica amostragem não probabilística, resultado do uso da técnica amostragem bola de neve.

Os respondentes deveriam responder todas as perguntas, mas nenhuma informação que prejudicasse o seu anonimato foi requisitada. Como já mencionado, a pesquisa enviada tentou capturar informações demográficas apropriadas, além dos indicadores necessários. Com o objetivo de incentivar a participação, o autor decidiu doar com R\$ 1,00 para cada resposta, limitado a R\$ 1.000,00, para a Associação de Pais e Amigos dos Excepcionais (APAE) de Campo Limpo Paulista – SP.

Para responder cada um dos itens da escala MUIPC discutidos a seguir, usou-se a escala Likert com intervalo de 7 pontos, entre 1 (discordo totalmente) e 7 (concordo totalmente). Esses itens são apresentados no Apêndice B desse trabalho. Esse intervalo foi escolhido para alcançar maior precisão quanto a percepção do respondente para cada item avaliado, limitando a ocorrência de variações significativamente altas ou baixas nos dados.

## 4.2 ADEQUAÇÃO DA AMOSTRA

Antes de discutir a caracterização da amostra e a análise dos resultados da pesquisa, foram realizadas algumas verificações de controle de qualidade e adequação da amostra para



que pudessem ser identificadas respostas inválidas, ausentes, padrões de respostas suspeitas e valores discrepantes (*outliers*). Um total de 310 respostas foram capturadas pela pesquisa, mas após a execução dos procedimentos mencionados a seguir obteve-se 262 válidas.

Devido a uma limitação da ferramenta de coleta, algumas respostas do mesmo indivíduo foram enviadas em duplicidade. Através da ferramenta IBM SPSS foi possível fazer comparação entre todos os atributos, detectar 37 duplicidades e eliminá-las da amostra.

O questionário não permitia ausência de resposta para quaisquer dos itens analisados por usar mecanismos no formulário que impediam os respondentes de seguir em frente ou enviar as informações sem o preenchimento de todos os dados solicitados e, para identificar respostas suspeitas (*straightlining*) foi usado método de análise do desvio padrão onde 1 resposta suspeita foi detectada.

No que tange aos valores discrepantes, por meio da ferramenta IBM SPSS foi aplicada uma avaliação pelo cálculo da distância quadrada de Mahalanobis (Hair, Hult, Ringle, e Sarstedt, 2017) e, como resultado, foram encontrados e removidos 10 *outliers* multivariados.

#### 4.3 PERFIL DEMOGRÁFICO DA AMOSTRA

Da amostra válida de 262 respondentes, a maioria dos indivíduos são do sexo masculino, cerca de 62,60%, valor próximo da distribuição demográfica da principal rede usada, o LinkedIn que, de acordo com fontes externas, possui 57% de usuários do sexo masculino (Aslam, 2020). Do total dos respondentes 71,76% têm entre 26-44 anos. Outros dados interessantes de serem evidenciados é a renda média familiar de 61,83% dos respondentes, que ganham acima de R\$ 10.000,00, e o nível de escolaridade, onde 61,07% afirmaram possuir curso superior e já terem feito alguma pós-graduação, seja *stricto sensu* ou *lato sensu*.

Apesar da tentativa de se alcançar várias regiões através da rede social, os respondentes são em sua maioria residentes no estado de São Paulo, correspondendo a 91,60% da amostra. O número de respondentes que mora fora do Brasil – 2,67% – foi maior que qualquer outro estado. Estas são importantes variáveis usadas em grande parte das pesquisas citadas neste estudo e foi possível usá-las como referência para medir as preocupações com privacidade dos indivíduos segundo sua classificação demográfica.

A Tabela 3 a seguir apresenta o perfil sociodemográfico completo dos respondentes.

**Tabela 3** – Classificação demográfica da amostra

Característica Demográfica	Categoria/Sigla	Frequência	Percentual
Gênero	Feminino	96	36,64%
	Masculino	164	62,60%
	Prefiro não dizer	2	0,76%

Idade	< 25	20	7,63%
	26 – 35	86	32,82%
	36 – 44	102	38,93%
	45 – 55	39	14,89%
	> 55	15	5,73%
Renda mensal	R\$ 0 - R\$ 1.000,00	3	1,15%
	R\$ 1.000,01 - R\$ 5.000,00	17	6,49%
	R\$ 5.000,01 - R\$ 10.000,00	44	16,79%
	R\$ 10.000,01 - R\$ 20.000,00	60	22,90%
	Mais que R\$ 20.000,00	102	38,93%
Escolaridade	Prefiro não informar	36	13,74%
	Pós-graduação ( <i>lato sensu</i> ou <i>stricto sensu</i> )	160	61,07%
	Superior Completo	82	31,30%
	Ensino Médio Completo	16	6,11%
	Ensino Fundamental Completo	4	1,53%
Estado civil	Solteiro(a)	55	20,99%
	Casado(a) ou em união estável	187	71,37%
	Separado(a) / Divorciado (a)	19	7,25%
	Viúvo(a)	1	0,38%
Estado	ES	1	0,38%
	MG	3	1,15%
	MS	1	0,38%
	PB	2	0,76%
	PR	3	1,15%
	RJ	2	0,76%
	RS	1	0,38%
	SC	2	0,76%
	SP	240	91,60%
	Moro fora do Brasil	7	2,67%

Fonte: Elaborado pelo autor (2021).

A Tabela 4 abaixo apresenta que 65,65% dos respondentes possuem um dispositivo iOS, contra 33,97% que possuem dispositivos que usam plataforma Android, e apenas 0,38% que usam ambas as plataformas. Como o estudo visa analisar as preocupações com privacidade com m-Health, o objetivo de se coletar esta informação é garantir que a pesquisa não fique restrita a determinada plataforma móvel.

**Tabela 4 – Tipo de Dispositivos Móveis**

Dispositivos usados	Frequência	Percentual
iOS	172	65,65%
Android	89	33,97%
Ambos	1	0,38%

Fonte: Elaborado pelo autor (2021).

Por fim, as variáveis pesquisadas permitiram examinar eventuais diferenças socioeconômicas nos construtos e indicadores da escala MUIPC, bem como as relativas

preocupações com privacidade. Com isso, pôde-se determinar se o modelo seria replicável em diferentes contextos.

## 5 RESULTADOS DA PESQUISA

### 5.1 VALIDAÇÃO DA ESCALA MUIPC PARA M-HEALTH

#### 5.1.1 Confiabilidade interna, validade convergente e validade discriminante

Para responder uma hipótese de pesquisa deve-se utilizar uma escala válida. Portanto, como objetivo específico desse trabalho está a validação do MUIPC para m-Health. O primeiro passo usado para validar o modelo foi analisar as cargas fatoriais (*outer loadings*) dos indicadores MUIPC pesquisados. A execução do algoritmo PLS-SEM convergiu após 7 interações, atingindo assim uma solução estável com poucas interações. Uma definição amplamente aceita é a de que baixas cargas fatoriais, isto é, abaixo de 0,70 são consideradas fracas (Hulland, 1999) e, portanto, deve-se examinar a possibilidade de eliminá-la do modelo. Com base nesta regra, a Tabela 5 apresenta que o indicador SURV1 é candidato a eliminação, já que apresenta um desajuste em relação à escala, similarmente ao que ocorreu em outros estudos (Kenan Degirmenci, Guhr, e Breitner, 2013; Silva Junior, 2015; Silva Junior et al., 2020) não estabelecendo assim validade convergente para este indicador. Já o indicador PEXP2 foi mantido, pois ele está no limite tolerável de 0,40 – 0,70.

**Tabela 5** – Carga Fatorial MUIPC

Construtos	Indicadores	Carga Fatorial
Intenção Comportamental	BINT1	0,886
	BINT2	0,965
	BINT3	0,964
Intrusão Percebida	INTR1	0,916
	INTR2	0,938
	INTR3	0,904
Experiência Prévia	PEXP1	0,840
	PEXP2	0,636
	PEXP3	0,860
Vigilância Percebida	SURV1	0,157
	SURV2	0,963
	SURV3	0,959
Uso Secundário	SUSE1	0,947
	SUSE2	0,956
	SUSE3	0,941

Fonte: Elaborado pelo autor (2021).

Sem o indicador SURV1, o algoritmo PLS-SEM novamente convergiu após 7 interações. Utilizando o critério de Fornell-Larcker, apresentado na Tabela 6, no qual a raiz quadrada de AVE – valores na diagonal, em negrito – deve ser maior que as correlações com os demais construtos, observou-se que há validade discriminante.

A seguir, optou-se por analisar a confiabilidade composta para demonstrar a consistência interna do modelo. Todos os construtos apresentaram valores acima do limite recomendado de 0,70 (Hair, Hult, et al., 2017), confirmando a confiabilidade do modelo. Foi analisada também a Variância Média Extraída (AVE), cujo valor mínimo exigido é de 0,50 (Fornell e Larcker, 1981). Todos os construtos apresentaram valores acima do limite estabelecido, o que demonstra alto nível de validade convergente.

**Tabela 6** – Resultados da Avaliação do Modelo MUIPC

Construto	1	2	3	4	5
1 - Intenção Comportamental (BINT)	<b>0,939</b>				
2 - Intrusão Percebida (INTR)	-0,294	<b>0,919</b>			
3 - Vigilância Percebida (SURV)	-0,279	0,790	<b>0,963</b>		
4 - Experiência Prévia (PEXP)	-0,033	0,245	0,169	<b>0,786</b>	
5 - Uso Secundário (SUSE)	-0,145	0,727	0,687	0,248	<b>0,948</b>
Confiabilidade Composta	0,957	0,943	0,963	0,826	0,964
Variância Média Extraída (AVE)	0,882	0,845	0,928	0,617	0,899

Fonte: Elaborado pelo autor (2021).

Também foram avaliados os critérios de cargas cruzadas (Tabela 7) como técnica adicional para determinar a validade discriminante. Nesse caso, a validade discriminante é estabelecida quando a carga dos indicadores atribuídas a um construto é maior que as cargas cruzadas dos indicadores atribuídos aos demais construtos (Hair, Hult, et al., 2017). Novamente, há evidências de validade discriminante para os indicadores reflexivos.

**Tabela 7** – Critério de Cargas Cruzadas

Indicadores	Intenção Comportamental	Intrusão Percebida	Vigilância Percebida	Experiência Prévia	Uso Secundário
BINT1	<b>0,887</b>	-0,238	-0,209	-0,032	-0,091
BINT2	<b>0,965</b>	-0,272	-0,257	-0,015	-0,132
BINT3	<b>0,964</b>	-0,309	-0,305	-0,044	-0,172
INTR1	-0,233	<b>0,916</b>	0,749	0,259	0,621
INTR2	-0,260	<b>0,938</b>	0,746	0,230	0,717
INTR3	-0,320	<b>0,904</b>	0,682	0,187	0,665
SURV2	-0,263	0,769	<b>0,964</b>	0,152	0,662
SURV3	-0,275	0,753	<b>0,963</b>	0,174	0,662

PEXP1	0,006	0,171	0,134	<b>0,842</b>	0,176
PEXP2	-0,019	0,150	0,131	<b>0,633</b>	0,205
PEXP3	-0,057	0,245	0,134	<b>0,861</b>	0,202
SUSE1	-0,104	0,692	0,654	0,223	<b>0,947</b>
SUSE2	-0,160	0,691	0,673	0,280	<b>0,956</b>
SUSE3	-0,148	0,685	0,626	0,202	<b>0,941</b>

Fonte: Elaborado pelo autor (2021).

Há situações, porém, nas quais essas técnicas são ineficazes em medir a validade discriminante (Henseler, Ringle, e Sarstedt, 2015) e, por isso, como medida de contorno, optou-se também por avaliar a técnica HTMT (*Heterotrait-Monotrait ratio*). Hair *et al.* (2018) recomendam considerar valores inferiores ao limite de 0,85 para HTMT para confirmar a validade discriminante entre dois construtos reflexivos. Embora a Tabela 8 a seguir apresente apenas um valor nesta relação acima do limite proposto, o valor está abaixo de 0,90, limite estabelecido por Henseler et al. (2015) para HTMT, confirmando então a validade discriminante do modelo.

**Tabela 8** – Heterotrait-Monotrait ratio

Construtos	BINT	INTR	SURV	PEXP	SUSE
BINT					
INTR	0,316				
SURV	0,295	0,862			
PEXP	0,05	0,308	0,216		
SUSE	0,149	0,785	0,736	0,311	

Fonte: Elaborado pelo autor (2021).

Finalmente, como recomendado por Hair, Hult, et al. (2017), é importante testar se os valores HTMT são significativamente diferentes de 1. Os resultados apresentados na Tabela 9 demonstram que estes suportam validade discriminante uma vez que o cálculo de intervalos de confiança de *bootstrap* demonstra que a relação entre os construtos nos intervalos de confiança (entre 2,5% e 97,5%) não passam pelo valor 1.

**Tabela 9** – Intervalos de Confiança de Bootstrap para HTMT

Relação	Coefficiente	2,50%	97,50%
INTR → BINT	0,316	0,186	0,438
SURV → BINT	0,295	0,162	0,419

SURV → INTR	0,862	0,808	0,911
PEXP → BINT	0,050	0,040	0,189
PEXP → INTR	0,308	0,156	0,465
PEXP → SURV	0,216	0,080	0,368
SUSE → BINT	0,149	0,051	0,272
SUSE → INTR	0,785	0,706	0,854
SUSE → SURV	0,736	0,650	0,811
SUSE → PEXP	0,311	0,160	0,459

Fonte: Elaborado pelo autor (2021).

Os construtos INTR, SURV e SUSE apresentaram índices satisfatórios para que houvesse consistência interna com o modelo e conseguiram explicar a relação que está se mensurando. Em resumo, o modelo proposto, conforme análises acima apresentadas, possui confiabilidade interna, validade convergente e validade discriminante.

### 5.1.2 Exame do modelo estrutural

Um exame do modelo estrutural também deve ser avaliado antes de qualquer afirmação. O coeficiente de determinação, também chamado de  $R^2$ , é uma medida de ajuste de um modelo estatístico linear generalizado e é a maneira mais comum de avaliar o modelo estrutural, onde valores entre 0 e 1 indicam maior exatidão preditiva. Hair, Hult, et al. (2017, p. 199, tradução nossa) destaca que “é difícil prover uma regra para valores de coeficientes de determinação aceitáveis e esse depende da complexidade do modelo e da disciplina de pesquisa”. Para este estudo, usaremos como referência (Cohen, 1988), que considera valores de  $R^2$  em 2%, 13% e 26% indicando respectivamente uma variância explicada pequena, média e grande. Sendo assim, o valor dos  $R^2$  nos relacionamentos entre os construtos examinados é pequeno.

Usando as regras que definem os critérios para análise do tamanho do efeito ( $f^2$ ), onde 0,02, 0,15 e 0,35 indicam respectivamente um fraco, médio e forte efeito do construto exógeno no endógeno (Hair, Hult, et al., 2017), é possível afirmar o tamanho do efeito para todos os relacionamentos do modelo também ser pequeno. Após uma avaliação da relevância preditiva de Stone-Geisser ( $Q^2$ ) observou-se valores acima de 0, indicando relevância preditiva em relação aos construtos endógenos (Hair, Hult, et al., 2017). Todos estes resultados estão apresentados na Tabela 10 a seguir:

**Tabela 10** – Tamanhos do Efeito, Coeficiente de Determinação e Relevância Preditiva

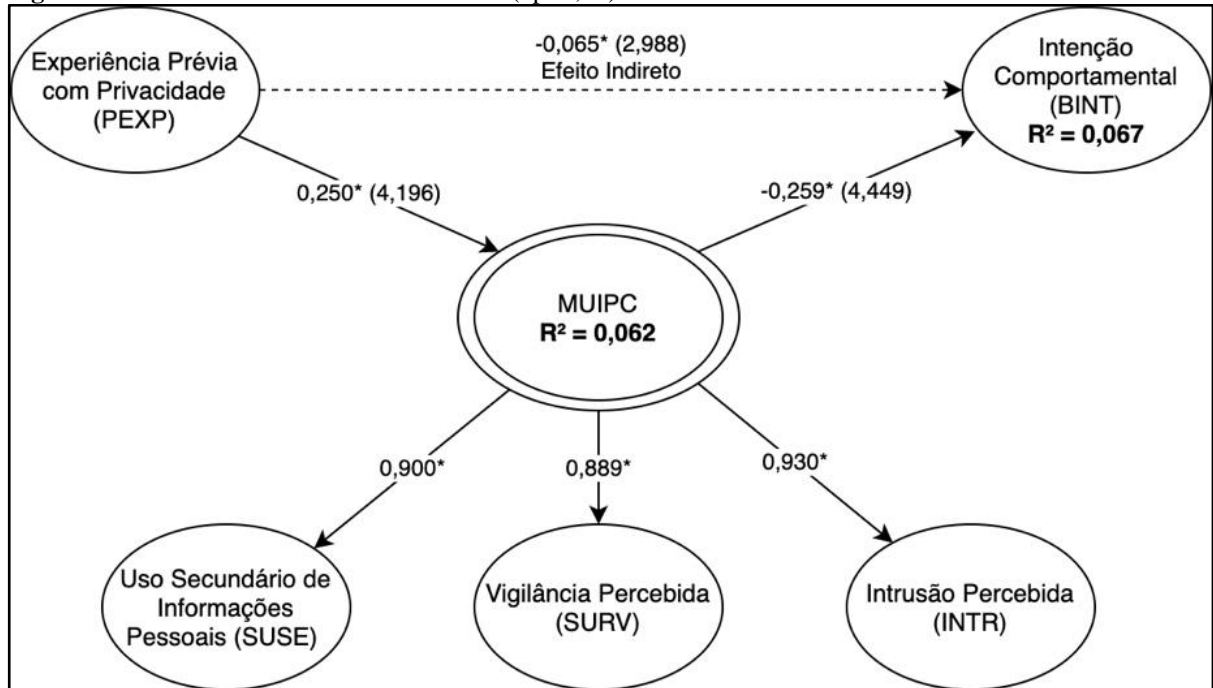
Relação estrutural	$f^2$	$R^2$	$Q^2$
PEXP → MUIPC	0,066	0,062	0,045

MUIPC → BINT	0,072	0,067	0,056
PEXP → MUIPC → BINT			

Fonte: Elaborado pelo autor (2021).

Para simplificar a visualização, a Figura 3 apresenta um resumo da análise dos coeficientes estruturais padronizados, valor-t e coeficientes de determinação.

**Figura 3** – Modelo MUIPC com os resultados (\* $p < 0,05$ )



Nota: Adaptado de Xu *et al.* (2012). Tradução do autor (2021).

A Tabela 11 abaixo detalha os coeficientes estruturais, valor-t, desvio padrão e valor-p e pode-se observar a relevância dos efeitos diretos da experiência prévia em MUIPC e de MUIPC com relação à intenção comportamental e, assumindo um nível de significância de 5% ( $p < 0,05$ ), é possível avaliar que todos os relacionamentos do modelo estrutural suportam todas as hipóteses propostas. Embora o efeito indireto de PEXP em BINT tenha apresentado significância estatística, o relacionamento foi fraco. Adicionalmente, o efeito direto da relação entre PEXP e BINT não atingiu o nível de significância assumido ( $p < 0,05$ ), o que indica uma mediação total.

**Tabela 11** – Resultados do Modelo Estrutural

Efeitos	Relação estrutural	Hipóteses e Avaliação	Coefficiente Estrutural	Desvio Padrão	Valor-t	Valor-p
Direto	PEXP → MUIPC	H1 - OK	0,250	0,059	4,196	0,000
Direto	MUIPC → BINT	H2 - OK	-0,259	0,058	4,449	0,000
Indireto	PEXP → MUIPC → BINT	H3 - OK	-0,065	0,022	2,988	0,003

Nota: Elaborado pelo autor (2021). Valores-p estimados por *bootstrapping* com 5000 repetições.

### 5.1.3 Análise das variáveis de controle

Para analisar o efeito moderador das variáveis de controle optou-se por segmentar a amostra, para adequação, em dois grupos por variável de controle. A variável de controle GEN foi segmentada segundo o gênero. A variável INC foi dividida usando como linha delimitadora a classificação da Associação Brasileira de Empresas de Pesquisa (2019) e, assim, INC1 inclui da classe extremamente pobre (DE) até a classe média (B1) e INC2 a classe alta (B1 e A). Para variável de controle AGE, por sua vez, seguiu-se critérios de divisão de classes proposto pela Organização Mundial da Saúde (Ahmad, Boschi Pinto, e Lopez, 2001) segmentando os grupos AGE2 (meia idade e grupos acima) e AGE1 (demais grupos).

A distribuição deste agrupamento está descrita na Tabela 12 abaixo:

**Tabela 12** – Segmentação em grupos da amostra

Variável de controle	Grupos unificados	Grupos iniciais	Frequência após unificação
AGE	AGE1	< 25	208
		26 – 35	
		35 – 44	
	AGE2	45 – 55 > 55	54
GEN	GEN1	Feminino Prefiro não dizer	98
	GEN2	Masculino	164
INC	INC1	Prefiro não informar R\$ 0 - R\$ 10.000,00	100
	INC2	Mais que R\$ 10.000,01	162

Fonte: Elaborado pelo autor (2021).

Para então investigar o efeito da variável de controle contínua AGE e das variáveis categóricas GEN e INC e evitar conclusões incorretas, procurou-se examinar a heterogeneidade dos dados através da técnica de análise multigrupos. Análises multigrupo são uma abordagem eficiente para avaliar a moderação entre os relacionamentos de um modelo, mas antes de prosseguir com essa técnica, é necessário avaliar a medida de invariância para confirmar que o mesmo atributo é medido corretamente em diferentes condições (Hair, Ringle, Sarstedt, e Gudergan, 2017; Henseler, Ringle, e Sarstedt, 2016). Para isso foi escolhida a técnica de



mensuração de invariância de modelos compostos (MICOM), que avalia a invariância da medição por permutação em três etapas: invariância de configuração, invariância composicional e igualdade de valores médios e variância de composição (Hair, Hult, et al., 2017). Para aplicação da técnica MICOM, recomenda-se por rigor que cada grupo seja composto por pelo menos 54 observações (Hair, Ringle, et al., 2017).

A invariância de configuração avalia a igualdade dos indicadores, do tratamento dos dados e algoritmos de análise dos grupos para testar se o modelo de mensuração é o mesmo para os diferentes grupos (Hair, Hult, et al., 2017; Hair, Ringle, et al., 2017). A invariância composicional é estabelecida pela análise estatística dos pesos, ou *scores*, entre os construtos são os mesmos (Hair, Hult, et al., 2017). Se a invariância composicional não for alcançada, cada grupo deve ser analisado separadamente. Por outro lado, se for estabelecida, têm-se a medida de invariância parcial confirmada e a análise multigrupo para medir os coeficientes de caminho é possível. Também, com a confirmação da medida de invariância parcial pode-se analisar a igualdade de valores médios e variância de composição e, se esta for obtida a amostra pode ser analisada no nível de dados agrupados (Hair, Hult, et al., 2017).

Com bases nessas definições foi executado o procedimento MICOM para cada uma das variáveis de controle propostas, especificando 1.000 permutações e assumido nível de significância em 0,05. A Etapa 1 do procedimento MICOM já foi estabelecida pela opção de usar um modelo onde, para todos os grupos examinados, foram usados os mesmos indicadores por construto, idêntico tratamento de dados e critérios de otimização e configuração.

Na Etapa 2 do procedimento MICOM foi avaliada a invariância composicional através de testes não paramétricos de permutação (Hair, Ringle, et al., 2017). Comparando a correlação entre escores compostos entre grupos de cada variável de controle procura-se observar se os valores estão acima do limite de 5% da distribuição empírica das correlações para todas as variáveis de controle analisadas. Este resultado é suportado também pelo valor-p que é maior do que 0,05.

Se confirmada a invariância parcial, a Etapa 3 do procedimento MICOM é também analisada. Nesta etapa busca-se checar se a média e a variância dos modelos de composição estão no intervalo de confiança de 95% e o valor-p da permutação acima de 0,05.

Examinando a variável de controle AGE, representada pela Tabela 13, é possível concluir que o valor-p da igualdade dos valores médios é não significativo em todas as relações na Etapa 2 e Etapa 3 confirmando uma medida de invariância total. Segundo Hair, Ringle, et al. (2017) neste caso tanto a análise agrupada da amostra como multigrupo são técnicas viáveis.

**Tabela 13** – MICOM para a variável de controle AGE (AGE1 x AGE2)

<b>MICOM - Etapa 1</b>				
Variância configuracional estabelecida pelo modelo agrupado				
<b>MICOM - Etapa 2</b>				
<b>Construto</b>	<b>Correlação original</b>	<b>5.0%</b>	<b>Valores-P da permutação</b>	<b>Invariância composicional</b>
BINT	0,999	0,945	0,633	OK
MUIPC	1,000	1,000	0,112	OK
INTR	1,000	1,000	0,443	OK
SURV	1,000	1,000	0,102	OK
PEXP	0,898	0,569	0,232	OK
SUSE	1,000	1,000	0,072	OK
<b>MICOM - Etapa 3</b>				
<b>Construto</b>	<b>Média - diferença Original</b>	<b>Intervalo de confiança em 95%</b>	<b>Valor-p da permutação</b>	<b>Igualdade de valores médios</b>
BINT	-0,034	[-0,307; 0,302]	0,824	OK
MUIPC	-0,227	[-0,295; 0,316]	0,149	OK
INTR	-0,252	[-0,301; 0,296]	0,108	OK
SURV	-0,291	[-0,297; 0,300]	0,057	OK
PEXP	-0,188	[-0,320; 0,303]	0,249	OK
SUSE	-0,101	[-0,286; 0,302]	0,532	OK
<b>Construto</b>	<b>Variância - Diferença Original</b>	<b>Intervalo de confiança em 95%</b>	<b>Valor-p da permutação</b>	<b>Igualdade de variância composicional</b>
BINT	0,204	[-0,342; 0,451]	0,300	OK
MUIPC	0,205	[-0,368; 0,490]	0,374	OK
INTR	0,141	[-0,322; 0,404]	0,456	OK
SURV	0,229	[-0,303; 0,392]	0,216	OK
PEXP	-0,107	[-0,330; 0,409]	0,554	OK
SUSE	0,255	[-0,404; 0,587]	0,325	OK

Fonte: Elaborado pelo autor (2021). Adaptado de (Hair, Ringle, et al., 2017)

O mesmo comportamento foi observado com a variável de controle GEN (Tabela 14), portanto, tanto a análise agrupada da amostra como multigrupo são técnicas viáveis.

**Tabela 14** – MICOM para a variável de controle GEN (GEN1 x GEN2)

<b>MICOM - Etapa 1</b>				
Variância configuracional estabelecida pelo modelo agrupado				
<b>MICOM - Etapa 2</b>				
<b>Construto</b>	<b>Correlação original</b>	<b>5.0%</b>	<b>Valores-P da permutação</b>	<b>Invariância composicional</b>
BINT	0,999	0,988	0,531	OK
MUIPC	1,000	1,000	0,339	OK
INTR	1,000	1,000	0,291	OK
SURV	1,000	1,000	0,937	OK
PEXP	0,952	0,834	0,284	OK
SUSE	1,000	1,000	0,869	OK

MICOM - Etapa 3				
Construto	Média - diferença Original	Intervalo de confiança em 95%	Valor-p da permutação	Igualdade de valores médios
BINT	0,048	[-0,257; 0,236]	0,717	OK
MUIPC	0,003	[-0,252; 0,252]	0,977	OK
INTR	0,013	[-0,240; 0,246]	0,911	OK
SURV	-0,077	[-0,244; 0,266]	0,564	OK
PEXP	0,233	[-0,236; 0,249]	0,059	OK
SUSE	0,051	[-0,247; 0,244]	0,690	OK

Construto	Variância - Diferença Original	Intervalo de confiança em 95%	Valor-p da permutação	Igualdade de variância composicional
BINT	0,015	[-0,312; 0,346]	0,421	OK
MUIPC	0,007	[-0,317; 0,338]	0,773	OK
INTR	0,006	[-0,275; 0,281]	0,761	OK
SURV	0,008	[-0,279; 0,284]	0,863	OK
PEXP	0,004	[-0,295; 0,293]	0,072	OK
SUSE	0,006	[-0,377; 0,418]	0,633	OK

Fonte: Elaborado pelo autor (2021). Adaptado de (Hair, Ringle, et al., 2017)

Para a variável de controle INC (Tabela 15) a igualdade dos valores médios do construto BINT apresentou valor-p não significativo, o que implica medida de invariância parcial, mas ainda assim a análise multigrupo é uma técnica viável (Hair, Ringle, et al., 2017).

**Tabela 15** – MICOM para a variável de controle INC (INC1 x INC2)

MICOM - Etapa 1				
Variância configuracional estabelecida pelo modelo agrupado				
MICOM - Etapa 2				
Construto	Correlação original	5.0%	Valores-P da permutação	Invariância composicional
BINT	0,994	0,987	0,135	OK
MUIPC	1,000	1,000	0,899	OK
INTR	1,000	1,000	0,398	OK
SURV	1,000	1,000	0,178	OK
PEXP	0,941	0,836	0,220	OK
SUSE	1,000	1,000	0,256	OK

MICOM - Etapa 3				
Construto	Média - diferença Original	Intervalo de confiança em 95%	Valor-p da permutação	Igualdade de valores médios
BINT	-0,359	[-0,258; 0,235]	0,005	NOK
MUIPC	0,100	[-0,235; 0,241]	0,415	OK
INTR	0,090	[-0,239; 0,249]	0,481	OK
SURV	0,092	[-0,252; 0,258]	0,466	OK
PEXP	-0,073	[-0,270; 0,241]	0,572	OK
SUSE	0,090	[-0,244; 0,237]	0,464	OK

Construto	Variância - Diferença Original	Intervalo de confiança em 95%	Valor-p da permutação	Igualdade de variância composicional
BINT	-0,076	[-0,332; 0,308]	0,644	OK
MUIPC	0,004	[-0,377; 0,331]	0,980	OK
INTR	0,051	[-0,307; 0,291]	0,752	OK
SURV	-0,078	[-0,329; 0,285]	0,585	OK
PEXP	0,043	[-0,291; 0,292]	0,763	OK
SUSE	-0,084	[-0,437; 0,375]	0,705	OK

Fonte: Elaborado pelo autor (2021). Adaptado de (Hair, Ringle, et al., 2017)

Para ampliar a análise dos efeitos específicos das variáveis de controle e seus respectivos grupos, aplicou-se então a técnica de *Multi-Group Analysis* (MGA) PLS-MGA. Este teste tem como objetivo indicar se há uma diferença significativa entre o coeficiente estrutural dos grupos de cada variável de controle por comparar a estimativa de *bootstrap* de um grupo com todas as outras estimativas de *bootstrap* do mesmo parâmetro no outro (Hair, Hult, et al., 2017; Hair, Ringle, et al., 2017).

Os resultados apresentados na Tabela 16 apontam que há diferença significativa entre os coeficientes estruturais ( $p < 0,1$ ) apenas entre os grupos AGE1 e AGE2 em uma das relações. Entre os grupos GEN1 e GEN2 não houve diferenças significativas entre os coeficientes estruturais de quaisquer das relações e o mesmo comportamento foi observado para INC1 e INC2.

**Tabela 16** – Resultados da análise PLS-MGA

Variável de Controle: AGE (AGE1 x AGE2)			
Relação Estrutural	Diferença entre os coeficientes estruturais	valor p original unilateral	valor-p
MUIPC → BINT	0,200	0,047	0,093
PEXP → MUIPC	-0,091	0,793	0,414
Variável de Controle: GEN (GEN1 x GEN2)			
Relação Estrutural	Diferença entre os coeficientes estruturais	valor p original unilateral	valor-p
MUIPC → BINT	0,032	0,383	0,766
PEXP → MUIPC	0,037	0,379	0,758
Variável de Controle: INC (INC1 x INC2)			
Relação Estrutural	Diferença entre os coeficientes estruturais	valor p original unilateral	valor-p
MUIPC → BINT	-0,140	0,905	0,190

PEXP → MUIPC	-0,099	0,770	0,460
--------------	--------	-------	-------

Fonte: Elaborado pelo autor (2021)

#### 5.1.4 Análise das variáveis individual dos grupos AGE1 e AGE2

Como técnica adicional foi conduzida uma análise dos resultados dos grupos AGE1 e AGE2 com o objetivo de verificar os resultados específicos para cada grupo e comparar com a amostra agrupada com relação à variância explicada, tamanho do efeito e coeficientes de determinação. Os resultados estão apresentados na Tabela 17.

**Tabela 17** – Resultados da análise dos resultados específicos dos grupos AGE1 e AGE2

	<b>Amostra Original</b>	<b>AGE1 (Até 44 anos)</b>	<b>AGE2 (+44 anos)</b>
<b>Total de Indivíduos</b>	262	208	54
<b>Tamanho Relativo dos Grupos</b>	100%	79,4%	20,6%
<b>Coefficientes Estruturais (*p&lt;0,05)</b>			
PEXP → MUIPC	0,250*	0,248*	0,339*
MUIPC → BINT	-0,259*	-0,228*	-0,428*
<b>Análise Fatorial Confirmatória</b>			
Validade Convergente (AVE)	OK	OK	OK
Confiabilidade Composta	OK	OK	OK
Validade Discriminante (HTMT)	OK	OK	OK
<b>Análise do modelo estrutural</b>			
<b>Valores R<sup>2</sup></b>			
PEXP → MUIPC	6,2%	6,2%	11,5%
MUIPC → BINT	6,7%	5,2%	18,3%
<b>Tamanho do Efeito f<sup>2</sup></b>			
PEXP → MUIPC	0,066	0,066	0,130
MUIPC → BINT	0,072	0,055	0,224

Fonte: Elaborado pelo autor (2021). Adaptado de (Hair, Ringle, et al., 2017)

## 6 DISCUSSÃO DOS RESULTADOS

### 6.1 MODELO E HIPÓTESES DE PESQUISA

As preocupações com privacidade têm papel importante na decisão de se adotar determinadas tecnologias na área da saúde, seja do ponto de vista dos indivíduos ou de outros interessados do setor (Ali et al., 2018; C. L. Anderson e Agarwal, 2011; Angst e Agarwal, 2009; Keil et al., 2018; Kim e Kwon, 2019; Li e Qin, 2017; Yaraghi et al., 2019). Em linha com a literatura levantada, o objetivo geral desse estudo foi esclarecer o papel das preocupações com a privacidade na divulgação de informações de saúde e no uso de aplicativos móveis que as armazenam e processam na CC para buscar um melhor entendimento da relação entre os

construtos preocupações com privacidade no uso de aplicativos móveis e intenção comportamental.

Para atingir o objetivo principal, os objetivos específicos foram propostos e adotou-se o modelo *Mobile Users' Information Privacy Concerns*. Os resultados analisados através do instrumento PLS-SEM apontam que o modelo se mostrou capaz de confirmar as hipóteses propostas, porém, com valores de  $R^2$  baixos, sendo 6,2% de PEXP para MUIPC e de 6,7% de MUIPC para BINT. Devido aos  $R^2$  serem relativamente baixos para a amostra agrupada, as contribuições deste estudo estão na inclusão das variáveis de controle gênero, idade e renda.

Ao incluir variáveis moderadoras, este estudo pôde, além de validar o modelo para um cenário específico relacionado à análise das preocupações de privacidade na divulgação ou uso m-Health, ampliar a pesquisa original de Xu et al. (2012). Assim como observado por Angst e Agarwal (2009) em seu estudo sobre privacidade da informação na divulgação de EHR, as variáveis socioeconômicas usadas nesta pesquisa também apresentaram influência na relação entre construtos no exame das preocupações com privacidade da informação em saúde.

As variáveis GEN e INC não confirmaram diferenças significativas nos resultados na comparação entre os grupos definidos para cada variável, diferente dos resultados da variável AGE. Como mencionado anteriormente, Hair, Hult, et al. (2017, p. 199, tradução do autor) destacam que “é difícil prover uma regra para valores de coeficientes de determinação ( $R^2$ ) aceitáveis e esse depende da complexidade do modelo e da disciplina de pesquisa”, portanto, uma abordagem baseada unicamente no coeficiente de determinação não é recomendada. Por isso, para análise da influência da variável de controle AGE examinamos os resultados específicos entre os grupos AGE1, AGE2 e a amostra agrupada, e notou-se diferenças significativas (valor- $p < 0,1$ ) nos coeficientes estruturais, valores de  $R^2$  e  $f^2$ . Como referência para interpretação da variância explicada foi usada como referência Cohen (1988), que considera valores de  $R^2$  em 2%, 13% e 26% indicando respectivamente uma variância explicada pequena, média e grande e os critérios para análise do tamanho do efeito ( $f^2$ ), são 0,02 (fraco), 0,15 (médio) e 0,35 (forte) (Hair, Hult, et al., 2017).

A hipótese H1 foi confirmada para a amostra agrupada que apresentou influência positiva direta ( $\beta=0,250$ ) com nível de significância  $p < 0,001$  e um efeito pequeno ( $f^2 = 0,066$ ) com  $R^2$  em 6,2% na relação  $PEXP \rightarrow MUIPC$  e resultados similares aos encontrados em estudo anterior que mensura relação similar (C. L. Anderson e Agarwal, 2011), sendo que a relação se altera sensivelmente quando o segmento analisado é AGE2. Os valores ampliam para  $\beta=0,336$ ,  $f^2 = 0,13$  e  $R^2 = 11,5\%$  e esses resultados confirmam a reflexão apresentada na literatura disponível que menciona que indivíduos de meia idade e idosos que experimentaram violação

de privacidade no passado tendem a ter maiores preocupações com privacidade (Gupta e Chennamaneni, 2018). Os coeficientes estruturais também apresentaram uma variação acima de 0,140 para o grupo INC2 (alta renda).

Assim, esse estudo contribui ao expandir o estudo destes construtos para m-Health e medir o efeito das variáveis moderadoras e por mostrar que esse é um construto confiável para medir esta relação em estudos futuros no modelo utilizado.

Similar comportamento foi observado na confirmação da hipótese H2. Para a amostra agrupada MUIPC mostrou ter influência negativa direta ( $\beta = -0,259$ ) com nível de significância  $p < 0,001$  e um efeito pequeno ( $f^2 = 0,072$ ) em BINT. A literatura corrente havia explicado o efeito negativo das preocupações com privacidade na intenção comportamental para divulgação de informações pessoais e de saúde dos indivíduos (Adjerid, Peer, et al., 2018; Agarwal et al., 2010; Angst e Agarwal, 2009; Yaraghi et al., 2019) e este estudo veio confirmar que a mesma relação foi observada referente às preocupações com privacidade em m-Health. No entanto, ao examinar as variáveis de controle para o segmento AGE2 observou-se significativa alteração. Os valores saltam para  $\beta = -0,428$ ,  $f^2 = 0,224$  e  $R^2 = 18,3\%$ , isto é, com tamanho do efeito entre médio e forte e coeficiente de determinação médio.

Novamente, as contribuições estão no exame do papel das variáveis de controle nas relações entre os construtos relacionados às preocupações com privacidade e intenção comportamental e ao apresentar a variação dessa relação para indivíduos de meia idade e idosos.

Já com relação a H3, constatou-se que não há relação significativa direta entre PEXP e BINT e, embora, a relação indireta entre PEXP e BINT com MUIPC como construto mediador tenha sido comprovada, o coeficiente estrutural indicou uma relação fraca ( $\beta = -0,065$ ) com nível de significância  $p < 0,01$ . Estudos anteriores corroboram este resultado ao explicar que experiência prévia com violação de privacidade afetam as crenças relacionadas aos riscos e confiança na adoção de determinada tecnologia (Naresh K. Malhotra et al., 2004) e poder servir como um antecedente na relação entre as preocupações com privacidade e a intenção comportamental (Smith et al., 1996).

Como a intensidade dessa mediação é baixa, a descoberta contribui com a literatura ao abrir oportunidade para estudos futuros avaliarem a inserção de outros antecedentes no modelo, como o construto “Controle Percebido” (Heng, Hock-Hai, Tan, e Agarwal, 2012) já que estudos anteriores mencionam que maior controle e proteção dos dados podem resultar em uma maior disposição dos indivíduos de revelar informações de saúde (Adjerid, Peer, et al., 2018).

## 6.2 CONSIDERAÇÕES FINAIS

Como abordado no decorrer deste estudo, m-Health, aplicativos móveis que armazenam e processam informações de saúde em *cloud computing*, tem se apresentado como uma tecnologia de interesse no segmento de saúde e examinar as preocupações com privacidade na ótica do indivíduo amplia a literatura disponível que foram em EHR e plataformas únicas de saúde.

Por examinar o papel moderador das variáveis de controle gênero, renda e idade este estudo, além de validar o modelo elaborado por Xu et al. (2012), o estende. Adicionalmente, este estudo mostrou que há indícios que as preocupações com privacidade têm uma influência negativa na intenção comportamental mais significativa para pessoas de meia idade e idosos. Baseado no resultado da pesquisa elaborada com base na escala MUIPC, nota-se que a experiência com violação privacidade no passado influencia a preocupação dos indivíduos quanto a privacidade e preocupações com privacidade no uso de m-Health, interferindo na divulgação de informações de saúde nesse canal.

Esse estudo também traz contribuições no campo de pesquisas relacionadas à privacidade de dados pois traz uma escala adicional – MUIPC – em estudos na área de sistemas de informação para exame das preocupações com privacidade na área de saúde que, anteriormente, usavam principalmente escalas como CFIP ou CPM. Essa pesquisa reflete também o papel dos construtos vigilância e intrusão percebidas e uso secundário das informações no uso de m-Health pelos indivíduos. Assim, contribuições que emergem com este estudo mostram a relevância destas variáveis latentes e a preocupação com privacidade, fortalecendo a validade da escala MUIPC.

Uma terceira contribuição se relaciona com a aplicabilidade da escala MUIPC em pesquisas no Brasil. Este estudo confirmou as descobertas de Silva Junior et al. (2020) relacionadas a um dos indicadores da escala, o SURV1, apresentado na Tabela 18 no Apêndice, que, em função de sua validade estatística, foi eliminado do modelo. Há um consenso que sugere certa dificuldade na interpretação deste indicador pelos respondentes abrindo oportunidade para um ajuste deste ao construto principal.

Devido às limitações desse estudo, há oportunidades para um aprofundamento no tema por agregar outros antecedentes à experiência prévia com privacidade utilizando a escala MUIPC.



## 7 CONCLUSÃO

Como uma opção à EHR e prontuários únicos do paciente, os m-Health oferecem controle de acesso, consentimento na mão dos indivíduos e poder de processamento escalável enquanto implementam funcionalidades necessárias para prontuários únicos, seguindo padrões de mercado. Adicionalmente, como opção às funcionalidades de bem-estar, essas plataformas oferecem funcionalidades para troca de dados e acessibilidade. Dadas essas características, foi crítico entender as preocupações dos indivíduos quanto à privacidade na divulgação de dados nessas plataformas e antecedentes que afetam suas escolhas e observar o efeito nas pessoas de meia-idade e idosos foi a principal contribuição. Esse estudo cumpriu, assim, seu objetivo e deu o primeiro passo em avaliar m-Health como plataforma única de saúde e as implicações relacionadas com respeito às preocupações com privacidade, servindo como referência na avaliação das opções para mitigá-las.

### 7.1 IMPLICAÇÕES PRÁTICAS

Esse estudo focou no tópico crucial envolvido na adoção de uma plataforma de saúde: as preocupações relacionadas à privacidade. Ele aponta um caminho em direção ao uso de m-Health para unificação dos dados de saúde do indivíduo e sua digitalização, apresentando essa plataforma como uma opção às iniciativas em torno da criação de um prontuário único do paciente baseadas principalmente em EHR e o equilíbrio que estas plataformas oferecem em termos de segurança, privacidade e controle. Foi possível entender, dentro de um escopo definido, as preocupações com privacidade na ótica do indivíduo no uso de m-Health e foi possível avaliar a influência na disposição de se adotar essa tecnologia pelos indivíduos.

As descobertas principalmente em relação à privacidade no ponto de vista de pessoas de meia idade e idosas apresentam informações que permitem às organizações avaliarem mecanismos que proporcionem a conscientização e informação sobre as práticas de segurança implementadas pelas soluções de m-Health e os benefícios de seu uso para mitigar esse risco à adoção tecnológica.

Este estudo pôde apresentar as implicações e opções potenciais para o uso de m-Health e o atalho que a adoção desta plataforma apresenta aos interessados de saúde na direção de centralizar as informações de saúde do paciente, enquanto minimizam o *overhead* de gestão de infraestrutura e sua obsolescência, controle de consentimento e acesso ao dado, uma vez transferem a responsabilidade de escolha da plataforma, e o controle sobre os dados aos indivíduos.

Também na perspectiva prática, provedores de plataformas m-Health podem utilizar os resultados desse estudo para buscarem opções para reduzir as preocupações quanto a privacidade no uso de m-Health. Opções de pesquisa para isso seriam a avaliação do papel das iniciativas regulatórias, como LGPD e HIPAA, na redução das preocupações com privacidade entre os usuários de m-Health e sua intenção comportamental.

Embora não fosse o objetivo deste estudo, ele contribuiu também ao discutir a capacidade de aplicações de m-Health como uma plataforma única de informações de saúde e, com isso, abriu portas para se estudar os benefícios e oportunidades em futuros estudos.

## 7.2 LIMITAÇÕES DA PESQUISA E SUGESTÕES PARA ESTUDOS FUTUROS

Esse estudo se propôs a examinar a influência das preocupações no uso de m-Health na intenção comportamental dos indivíduos, já que havia certa escassez de estudos que examinassem o uso dessas plataformas. Futuros estudos deveriam investigar como provedores, fornecedores e seguradoras de saúde percebem as plataformas de m-Health em termos de funcionalidade, competitividade e controle de privacidade. Uma pesquisa mais aprofundada também pode esclarecer se o indivíduo é o principal influenciador em alavancar o uso destas plataformas ou se o papel em as disseminar está entre os outros envolvidos no segmento de saúde, como médicos, hospitais, clínicas, seguradoras ou outros prestadores.

Há oportunidades para inclusão de construtos adicionais no exame das preocupações quanto à privacidade no uso de m-Health para correlacionar com a divulgação dos dados de saúde. Além disso, há espaço para estudar os benefícios percebidos no uso dessas plataformas, em adição às preocupações com privacidade.

Explorar o compartilhamento de dados com outros envolvidos com m-Health é também uma opção, principalmente quando os dados dos indivíduos devem ser acessados por um número significativo de interessados para, por exemplo, tratamento de uma doença crônica ou pesquisa médica. Além disso, observar o papel do consentimento no acesso ao dado em m-Health e a intenção do indivíduo em conceder o consentimento é um campo no qual esse estudo não aprofundou.

Apesar de permitir generalizar os resultados considerando plataformas populares de m-Health, esse estudo não se limitou a uma plataforma específica e, dadas sutis diferenças entre aplicativos atualmente disponíveis, há campo para estudar e comparar os mesmos resultados em diferentes plataformas e segmentos demográficos.

Finalmente, apesar de ter participação de pessoas fora do Brasil, a pesquisa foi distribuída exclusivamente em português e, por sua vez, restrita aos indivíduos que entendem esse idioma. Assim, diferenças culturais podem ser percebidas se uma investigação similar, relacionada ao tema deste estudo for conduzida em outra cultura ou país.

## REFERÊNCIAS

- Adjerid, I., Adler-Milstein, J., e Angst, C. (2018). Reducing medicare spending through electronic health information exchange: The role of incentives and exchange maturity. *Information Systems Research*, 29(2), 341-361.
- Adjerid, I., Peer, E., e Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, 42(2), 465-A465.
- Agarwal, R., Guodong, G., DesRoches, C., e Jha, A. K. (2010). The digital transformation of healthcare: Current status and the road ahead. *Information Systems Research*, 21(4), 796-809.
- Ahmad, O. B., Boschi Pinto, C., e Lopez, A. D. (2001). Age standardization of rates: A new who standard. *GPE Discussion Paper Series: No 31*, 10-12.
- Ali, O., Shrestha, A., Soar, J., e Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158.
- Amazon Web Services. (2020). O que é a computação em nuvem? Retrieved from <https://aws.amazon.com/pt/what-is-cloud-computing/>
- Anderson, C., Baskerville, R. L., e Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, 34(4), 1082-1112.
- Anderson, C. L., e Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490.
- Angst, C. M., e Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339-370.
- Aslam, S. (2020, 29-jul-2020). LinkedIn by the numbers: Stats, demographics & fun facts. Retrieved from <https://www.omnicoreagency.com/linkedin-statistics/>
- Associação Brasileira de Empresas de Pesquisa. (2019). Critério de classificação econômica brasil. Retrieved from [http://www.abep.org/criterioBr/01\\_cceb\\_2019.pdf](http://www.abep.org/criterioBr/01_cceb_2019.pdf)
- Babbie, E. R. (1999). *Metodos de pesquisas de survey*: Editora UFMG.
- Battleson, D. A., West, B. C., Kim, J., Ramesh, B., e Robinson, P. S. (2016). Achieving dynamic capabilities with cloud computing: An empirical investigation. *European Journal of Information Systems*, 25(3), 209-230.
- Benbunan-Fich, R. (2019). An affordance lens for wearable information systems. *European Journal of Information Systems*, 28(3), 256-271.
- Blumenthal, D. a. T. M. (2010). The meaningful use regulation for electronic health records. *The New England journal of medicine*, 363, 501-504.

- Brasil. (2016). *Comissão intergestores tripartite. Resolução nº 7 de 24 de novembro de 2016*. Conselho Nacional de Secretários de Saúde. [http://www.conass.org.br/wp-content/uploads/2016/12/RESOLUCAO-N\\_7\\_16.pdf](http://www.conass.org.br/wp-content/uploads/2016/12/RESOLUCAO-N_7_16.pdf)
- Brasil. (2017). *Estratégia e-saúde para o brasil*. Ministério da Saúde. [https://saudedigital.saude.gov.br/wp-content/uploads/2020/02/Estrategia-e-saude-para-o-Brasil\\_CIT\\_20170604.pdf](https://saudedigital.saude.gov.br/wp-content/uploads/2020/02/Estrategia-e-saude-para-o-Brasil_CIT_20170604.pdf)
- Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018*. [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm)
- Brasil. (2020). *Portaria gm/ms nº 1.434, de 28 de maio de 2020*. Ministério da Saúde. <https://rnds.saude.gov.br/>
- Bygstad, B. (2017). Generative innovation: A comparison of lightweight and heavyweight it. *Journal of Information Technology (Palgrave Macmillan)*, 32(2), 180-193.
- Chin, W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly*, 22.
- Chin, W., Marcolin, B., e Newsted, P. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14, 189-217.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*: Lawrence Erlbaum Associates.
- Creswell, J. W. (2012). Projeto de pesquisa: Métodos qualitativo, quantitativo e misto; tradução magda lopes. – 3 ed. – porto alegre: Artmed, 296 páginas, 2010. *Cadernos de Linguagem e Sociedade*, 13(1), 205-208.
- Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, 50, 261-272.
- Degirmenci, K., Guhr, N., e Breitner, M. (2013). Mobile applications and access to personal information: A discussion of users' privacy concerns. *Editor (Ed.), Proceedings of the International Conference on Information Systems (ICIS)*, 3, 2570-2590.
- Estados Unidos da América. (21 de agosto de 1996). *Health insurance portability and accountability act*. <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
- Fornell, C., e Bookstein, F. L. (1982). Two structural equation models: Lisrel and pls applied to consumer exit-voice theory. *Journal of Marketing Research*, 19(4), 440-452.
- Fornell, C., e Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.
- Gao, F., e Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. *International Journal of Information Management*, 48, 120-138.

- Gartner. (2019). Gartner says global end-user spending on wearable devices to total \$52 billion in 2020. In L. Goasduff (Ed.): Gartner.
- Gilbert, M., e Cribbs, J. (2020). Hype cycle for consumer engagement with healthcare and wellness. In: Gartner.
- Gupta, B., e Chennamaneni, A. (2018). Understanding online privacy protection behavior of the older adults: An empirical investigation. *Journal of Information Technology Management*, 29(3), 1-13.
- Hair, J., Hult, G. T. M., Ringle, C., e Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling*, 2nd edition: Sage.
- Hair, J., Ringle, C., Sarstedt, M., e Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*: Sage Publications, Inc.
- Heng, X., Hock-Hai, T., Tan, B. C. Y., e Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23(4), 1342-1363.
- Henseler, J., Ringle, C., e Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115-135.
- Henseler, J., Ringle, C. M., e Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review*, 33(3), 405-431.
- Hulland, J. (1999). Use of partial least squares (pls) in strategic management research: A review of four recent studies. *Strategic Management Journal*, 20(2), 195-204.
- James Bender, A., e Mecklenburg, R. S. (2017). How the emr is increasing innovation and creativity in health care. *Harvard Business Review Digital Articles*, 1-5.
- James, T. L., Wallace, L., e Deane, J. K. (2019a). An application of goal content theory to examine how desired exercise outcomes impact fitness technology feature set selection. *Information Systems Journal*, 29(5), 1010-1039.
- James, T. L., Wallace, L., e Deane, J. K. (2019b). Using organismic integration theory to explore the associations between users' exercise motivations and fitness technology feature set use. *MIS Quarterly*, 43(1), 287-312.
- Jones, M., Hull, S., e Hakkennes, S. (2019). Healthcare innovation trends: Transforming care delivery. In: Gartner.
- Juhee, K., e Eric Johnson, M. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly*, 42(4), 1043-1067.
- Keil, M., Park, E. H., e Ramesh, B. (2018). Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle-blowing intentions. *Information Systems Journal*, 28(5), 818-848.

- Kim, S. H., e Kwon, J. (2019). How do ehRs and a meaningful use initiative affect breaches of patient information? *Information Systems Research*, 30(4), 1184-1202.
- Klas, M. E., e Conarck, B. (2020, MARCH 20, 2020). Thermometer company: Florida compares only to nyc in spike in fever data. *Miami Herald*.
- Kohli, R., e Tan, S. S.-L. (2016). Electronic health records: How can is researchers contribute to transforming healthcare? *MIS Quarterly*, 40(3), 553-574.
- Li, X.-B., e Qin, J. (2017). Anonymizing and sharing medical text records. *Information Systems Research*, 28(2), 332-352.
- Lin, Y.-K., Chen, H., Brown, R. A., Li, S.-H., e Yang, H.-J. (2017). Healthcare predictive analytics for risk profiling in chronic care: A bayesian multitask learning approach. *MIS Quarterly*, 41(2), 473-A473.
- Liwei, C., Baird, A., e Rai, A. (2019). Mobile health (mhealth) channel preference: An integrated perspective of approach-avoidance beliefs and regulatory focus. *Journal of the Association for Information Systems*, 20(12), 1743-1773.
- Lowry, P. B., Gaskin, J., Humpherys, S. L., Moody, G. D., Galletta, D. F., Barlow, J. B., e Wilson, D. W. (2013). Evaluating journal quality and the association for information systems senior scholars' journal basket via bibliometric measures: Do expert journal assessments add value? *MIS Quarterly*, 37(4), 993-1012.
- Malhotra, N. K. (2006). *Pesquisa de marketing: Uma orientação*: Bookman.
- Malhotra, N. K., Sung, S. K., e Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
- Mell, P. M., e Grance, T. (2011). *Sp 800-145. The nist definition of cloud computing*. Retrieved from
- Microsoft. (2020). O que é computação em nuvem? Retrieved from <https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/>
- Ozdemir, Z., Barron, J., e Bandyopadhyay, S. (2011). An analysis of the adoption of digital health records under switching costs. *Information Systems Research*, 22(3), 491-503.
- Parlamento Europeu, e Conselho Da União Europeia. (27 de abril de 2016). *Regulamento (ue) 2016/679 do parlamento europeu e do conselho*. <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY, US: State University of New York Press.
- Sambamurthy, V., e Zmud, R. W. (2017). *Guiding the digital transformation of organizations* (Second Edition ed.): Legerity Digital Press, LLC.
- Shapiro, C., Shapiro, C., e Varian, H. R. (1998). *Information rules: A strategic guide to the network economy*: Harvard Business School Press; Edição: 1.

- Silva Junior, S. D. d. (2015). *O efeito enquadramento nas decisões sobre a divulgação de informações pessoais: Um estudo experimental no âmbito dos aplicativos móveis*.
- Silva Junior, S. D. d., Luciano, E. M., e Lübeck, R. M. (2020). Revalidação da escala mobile users' information privacy concerns para o contexto brasileiro. 2020, 19(2), 19.
- Smith, H. J., Dinev, T., e Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 980-A927.
- Smith, H. J., Milberg, S. J., e Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-564.
- Stewart, K. A., e Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.
- Strong, D. M., Johnson, S. A., Tulu, B., Trudel, J., Volkoff, O., Pelletier, L. R., . . . Garber, L. (2014). A theory of organization-e-hr affordance actualization. *Journal of the Association for Information Systems*, 15(2), 53-85.
- Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, 34(2), 177-184.
- Urbaczewski, A., e Lee, Y. J. (2020). Information technology and the pandemic: A preliminary multinational analysis of the impact of mobile tracking technology on the covid-19 contagion control. *European Journal of Information Systems*.
- Vitak, J., Liao, Y., Kumar, P., Zimmer, M., e Kritikos, K. (2018) Privacy attitudes and data valuation among fitness tracker users. In: *Vol. 10766 LNCS. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 229-239).
- Wiegard, R., Guhr, N., Krylow, S., e Breitner, M. H. (2019). Analysis of wearable technologies' usage for pay-as-you-live tariffs: Recommendations for insurance companies. *Zeitschrift für die gesamte Versicherungswissenschaft*, 108(1), 63-88.
- Xu, H., Gupta, S., Rosson, M. B., e Carroll, J. M. (2012). *Measuring mobile users' concerns for information privacy*. Paper presented at the International Conference on Information Systems, ICIS 2012.
- Yaraghi, N., Gopal, R. D., e Ramesh, R. (2019). Doctors' orders or patients' preferences? Examining the role of physicians in patients' privacy decisions on health information exchange platforms. *Journal of the Association for Information Systems*, 20(7), 928-952.
- Yaraghi, N., Ye Du, A., Sharman, R., Gopal, R. D., e Ramesh, R. (2015). Health information exchange as a multisided platform: Adoption, usage, and practice involvement in service co-production. *Information Systems Research*, 26(1), 1-18.



## **APÊNDICE A – Informação de Contexto**

### **O que são os aplicativos de saúde que usam computação em nuvem e por que considerar privacidade nesse contexto é importante?**

São aplicativos capazes de usar computação em nuvem, ou seja, usar recursos compartilhados de tecnologia da informação através da internet para armazenar e processar informações de saúde. Apple Health, Google Fit e Fitbit são exemplos aplicativos que sincronizam suas informações de rotina, saúde e bem-estar com a nuvem. Muitos desses podem ser conectados a dispositivos vestíveis como relógios e pulseiras inteligentes ou outros dispositivos inteligentes de monitoramento, como termômetros ou balanças.

Aplicativos de saúde como estes podem se integrar com informações do prontuário de saúde do paciente e, com isso, poderiam resolver um dos grandes dilemas do setor de saúde: a ausência de um histórico confiável de informações de saúde do indivíduo.

Por exemplo, usando recursos de computação em nuvem, durante a pandemia de Covid-19, a Kinsa Health, fornecedora de um termômetro inteligente conectado através da internet, foi capaz de identificar pela coleta e análise de dados de milhares de termômetros, uma correlação entre o aumento de casos de febre e o surto da Covid-19 na Flórida.

Por outro lado, informações de saúde são informações consideradas sensíveis e o vazamento de informações como essas podem comprometer a privacidade do indivíduo.

## APÊNDICE B – Instrumento de pesquisa

**Tabela 18** – Escala MUIPC – Instrumento de Pesquisa

Construtos	Indicadores
Vigilância percebida	<p>Ao instalar um aplicativo no meu dispositivo móvel que colete e monitore minhas informações de saúde e bem-estar usando computação em nuvem...</p> <p>SURV1. Eu acredito que a localização do meu dispositivo móvel será monitorada por pelo menos parte do tempo.</p> <p>SURV2. Fico preocupado que estes aplicativos colem muitas informações sobre mim.</p> <p>SURV3. Fico preocupado que estes aplicativos monitorem minhas atividades através de meu dispositivo móvel.</p>
Intrusão percebida	<p>Ao usar um aplicativo no meu dispositivo móvel que colete e monitore minhas informações de saúde e bem-estar usando computação em nuvem...</p> <p>INTR1. Sinto que, como resultado do uso destes aplicativos, outras pessoas saberiam mais sobre mim do que estou confortável.</p> <p>INTR2. Acredito que, como resultado do uso destes aplicativos, as informações sobre mim que considero privadas estariam agora mais disponíveis para outras pessoas do que eu gostaria.</p> <p>INTR3. Eu sinto que, como resultado do uso destes aplicativos, informações sobre mim estariam acessíveis e, se usadas, invadirão minha privacidade.</p>
Uso secundário de informações pessoais	<p>Ao usar um aplicativo no meu dispositivo móvel que colete e monitore minhas informações de saúde e bem-estar usando computação em nuvem...</p> <p>SUSE1. Eu fico preocupado que estes aplicativos possam usar minhas informações pessoais para outros fins sem me notificar ou obter minha autorização.</p> <p>SUSE2. Quando forneço informações pessoais para estes aplicativos, fico preocupado que os aplicativos possam usar minhas informações para outros fins.</p> <p>SUSE3. Fico preocupado que estes aplicativos possam compartilhar minhas informações pessoais com outras entidades sem pedir minha autorização.</p>
Experiência prévia com privacidade	<p>PEXP1. Com que frequência você já passou por incidentes pessoais nos quais suas informações pessoais foram usadas por alguma empresa ou site de comércio eletrônico sem sua autorização?</p> <p>PEXP2. Quanto você ouviu ou leu durante o ano passado sobre o uso e o potencial uso indevido das informações coletadas na Internet?</p> <p>PEXP3. Com que frequência você foi pessoalmente vítima de algo que sentiu ser uma invasão indevida de privacidade?</p>
Intenção comportamental	<p>Considerando um aplicativo no meu dispositivo móvel que colete e monitore minhas informações de saúde e bem-estar usando computação em nuvem...</p> <p>BINT1. É provável que eu divulgue minhas informações pessoais para usar estes aplicativos nos próximos 12 meses.</p> <p>BINT2. Prevejo que usarei estes aplicativos nos próximos 12 meses.</p> <p>BINT3. Pretendo usar estes aplicativos nos próximos 12 meses.</p>

*Nota:* Adaptado de Xu et al. (2012). Likert com intervalo de 7 pontos, entre 1 (discordo totalmente) e 7 (concordo totalmente) como na escala original de Xu et al. (2012).