Universidade do Estado do Rio de Janeiro
Centro Biomédico
Faculdade de Ciências Médicas

Leonardo Costa Farias

Modelo baseado em Lógica Fuzzy para identificação de risco, à luz da LGPD, na saúde digital

Rio de Janeiro
2024

Leonardo Costa Farias

Modelo baseado em Lógica Fuzzy para identificação de risco, à luz da LGPD, na saúde digital

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Telemedicina e Telessaúde, da Universidade do Estado do Rio de Janeiro.

Orientadora: Prof.ª Dra. Karla Tereza Figueiredo Leite

Rio de Janeiro

2024

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CB-A

F224 Farias, Leonardo Costa.
Modelo baseado em Lógica Fuzzy para identificação de risco, à luz da LGPD, na saúde digital / Leonardo Costa Farias – 2024.
141 f.

Orientadora: Prof.ª Dra. Karla Tereza Figueiredo Leite

Dissertação (Mestrado) – Universidade do Estado do Rio de Janeiro, Faculdade de Ciências Médicas. Pós-graduação em Telemedicina e Telessaúde.

1. Saúde digital – Teses. 2. Lei Geral de Proteção de Dados. 3. Lógica Fuzzy. 4. Medição de risco. I. Leite, Karla Tereza Figueiredo. II. Universidade do Estado do Rio de Janeiro. Faculdade de Ciências Médicas. III. Título.

CDU 61:004.5

Bibliotecária: Ana Rachel Fonseca de Oliveira
CRB7/6382

_____ _____

Assinatura Data

Leonardo Costa Farias

Modelo baseado em Lógica Fuzzy para identificação de risco, à luz da LGPD, na saúde digital

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Telemedicina e Telessaúde, da Universidade do Estado do Rio de Janeiro.

Aprovada em 15 de abril de 2024.

Banca Examinadora: _____

Prof.ª Dra. Karla Tereza Figueiredo Leite (Orientadora)

Faculdade de Ciências Médicas – UERJ

_____

Prof.ª Dra. Rosa Maria Esteves Moreira da Costa

Faculdade de Ciências Médicas – UERJ

_____

Dra. Raquel Elena Rinaldi Maciel

Centro Universitário Gama e Souza

Rio de Janeiro

2024

DEDICATÓRIA

Deus,

dedico esta conquista a Ti, com amor e gratidão, pois Tu és a força que me guia e me protege em todos os momentos da minha vida. Sei que nem sempre sou digno da tua graça e misericórdia, mas peço humildemente que continues a me abençoar e a iluminar o meu caminho.

Agradeço por tudo o que me tens proporcionado, pela minha família, pelos amigos, pela saúde, pelo trabalho e por todas as outras bênçãos que recebo diariamente. Sei que sem Ti nada disso seria possível, e por isso te agradeço do fundo do meu coração.

Que a tua luz continue a me guiar e que eu possa sempre estar em sintonia Contigo, seguindo os Teus mandamentos e praticando o bem. Que a Tua sabedoria e o Teu amor me acompanhem sempre, dando-me força e coragem para enfrentar os desafios da vida.

Obrigado Deus, por tudo o que tens feito por mim. Que a Tua paz esteja sempre presente em minha vida.

AGRADECIMENTOS

A Deus, obrigado por iluminar o meu caminho. A minha vida tem sido marcada por realizações diárias, que às vezes não dou o devido valor. Mas eu sei que a Sua graça se faz presente em todos os momentos da minha vida, seja diretamente ou por meio de pessoas, como instrumentos da Sua vontade. **As portas abertas pelo Senhor ninguém fecha**.

A minha amada esposa, que me acolheu com amor e carinho, e vem me fazendo ser cada vez mais forte e feliz. Dela roubei tempo precioso e mesmo assim, ela soube compreender as minhas ausências e angústias no decorrer deste Mestrado. Agradeço por sua paciência, compreensão e apoio incondicional em todos os momentos. O seu encorajamento e suporte foram fundamentais para me manter motivado e focado nos meus objetivos. **Você é o meu orgulho e a minha alegria!**

Aos meus amados pais, Carlos (*in memoriam*) e Sueli, pela minha vida, por todo o amor e apoio. Sem vocês, este caminho até aqui não seria possível.

A Professora Dr.ª Karla Tereza Figueiredo Leite, orientadora e amiga, que acreditou em mim, me entendeu, me defendeu, e cujos conselhos, presença e empatia viabilizaram toda a trajetória neste Mestrado. As suas orientações e sugestões foram inestimáveis para este trabalho.

Salmo 23

O Senhor é o meu pastor:
nada me faltará.

Deitar-me faz em verdes pastos,
guia-me mansamente em águas tranquilas.

Refrigera a minha alma;
guia-me pelas veredas da justiça,
por amor ao Seu nome.

Ainda que eu andasse pelo vale da sombra da morte,
não temerei mal nenhum,
porque Tu estás comigo;

a Tua vara e o Teu cajado me consolam.

Preparas uma mesa perante mim
na presença dos meus inimigos,
unges a minha cabeça com óleo,
meu cálice transborda.

Certamente que a bondade e a misericórdia
me seguirão todos os dias da minha vida:
e habitarei na casa do Senhor por longos dias.

RESUMO

FARIAS, Leonardo Costa. *Modelo baseado em Lógica Fuzzy para identificação de risco, à luz da LGPD, na saúde digital.* 2024. 141f. Dissertação (Mestrado Profissional em Telemedicina e Telessaúde) – Faculdade de Ciências Médicas, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2024.

Promulgada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), Lei Federal n.º 13.709/2018, exige que todas as empresas públicas e privadas e profissionais liberais que tratem dados pessoais e dados pessoais, inclusive os que atuam na área da Saúde Digital se adequem às suas exigências, sob pena de sanções administrativas, inclusive multa, com exceção dos órgãos públicos. As organizações que lidam com estes dados estão expostas ao risco de descumprimento desta Lei e desta forma é imprescindível que esse risco seja mensurado. Atualmente existem poucos modelos desenvolvidos para inferir o risco relativo à LGPD, mas em nenhum dos casos é utilizada uma metodologia quantitativa e/ou baseada em Lógica Fuzzy. Sendo assim, o novo modelo desenvolvido nesta dissertação visa preencher a lacuna na literatura, onde não há uma estrutura que infira riscos quantitativa e qualitativamente de empresas e profissionais liberais que atuam na Saúde Digital. O modelo para avaliação de risco para LGPD, baseado em Lógica Fuzzy, propõe uma abordagem que busca conciliar esses diferentes domínios de conhecimento. O presente estudo considera o tratamento dos referidos dados, na área da Saúde Digital, sob a perspectiva do risco ao descumprimento da LGPD, utilizando a Inteligência Artificial, através da Lógica Fuzzy e incorporando as boas práticas das normas técnicas da ABNT e da ISO. A metodologia adotada envolveu uma revisão aprofundada da literatura sobre LGPD, Lógica Fuzzy, normas técnicas, bem como trabalhos relacionados. O modelo proposto, intitulado Modelo Fuzzy-LGPD para Gestão de Riscos na Saúde Digital, foi comparado com trabalhos relacionados abordados nesta dissertação. Com base na revisão da literatura, foi possível identificar os principais desafios e oportunidades associados ao referido tratamento destes dados na Saúde Digital, especialmente no que diz respeito à conformidade legal, mitigação de riscos e garantia da privacidade dos sujeitos de cuidado, pacientes. Os resultados atenderam às expectativas, ao revelar a exposição de empresas ao risco, mostrando-se, por isso, muito promissores. Sendo assim, este estudo representa um avanço significativo no campo da proteção de dados na saúde digital, oferecendo uma estrutura abrangente que integra aspectos legais, técnicos e de Gestão de Riscos.

Palavras-chave: Lei Geral de Proteção de Dados; Identificação de riscos; lógica fuzzy.

ABSTRACT

FARIAS, Leonardo Costa. *Model based on Fuzzy Logic for risk assessment, in the light of the LGPD, in digital health*. 2024.141f. Dissertação (Mestrado Profissional em Telemedicina e Telessaúde) – Faculdade de Ciências Médicas, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2024.

Enacted on August 14, 2018, the General Data Protection Law (LGPD), Federal Law No. 13,709/2018, mandates that all public and private companies, as well as freelance professionals who handle personal data, including those operating in the Digital Health sector, comply with its requirements, under penalty of administrative sanctions, including fines, except for public agencies. Organizations dealing with such data are exposed to the risk of non-compliance with this law, making it essential to assess and quantify this risk. Currently, there are few models developed to infer LGPD-related risks, but none of them employ a quantitative and/or fuzzy logic-based methodology. Thus, the new model developed in this dissertation aims to fill the gap in the literature, where there is no structure to infer quantitative and qualitative risks of companies and freelance professionals operating in Digital Health. The proposed risk assessment model for LGPD, based on Fuzzy Logic, offers an approach that seeks to reconcile these different knowledge domains. This study considers the treatment of such data in the Digital Health sector from the perspective of LGPD non-compliance risk, utilizing Artificial Intelligence through Fuzzy Logic and incorporating best practices from ABNT and ISO technical standards. The adopted methodology involved an in-depth literature review on LGPD, Fuzzy Logic, technical standards, as well as related works. The proposed model, titled Fuzzy-LGPD Model for Risk Management in Digital Health, was compared with related works addressed in this dissertation. Based on the literature review, it was possible to identify the main challenges and opportunities associated with the treatment of such data in Digital Health, especially regarding legal compliance, risk mitigation, and ensuring the privacy of care subjects, patients. The results met expectations by revealing companies' exposure to risk, thus proving highly promising. Therefore, this study represents a significant advancement in the field of data protection in digital health, offering a comprehensive framework that integrates legal, technical, and risk management aspects.

Keywords: General Data Protection Law; risk management; fuzzy logic.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AECI	Assessorias Especiais de Controle Interno
ANPD	Autoridade Nacional de Proteção de Dados
CCGD	Comitê Cental de Governança de Dados
CGU	Controladoria-Geral da União
CID	Confidencialidade, Integridade e Disponibilidade
CFM	Conselho Federal de Medicina
COVID-19	*Coronavirus Disease 2019*
DEM	Desvio Padrão do Erro Médio
DEMA	Desvio Padrão do Erro Médio Absoluto
DP	Dados Pessoais
DPIA	*Data Protection Impact Assessment*
EM	Erro Médio
EMA	Erro Médio Absoluto
GDPR	*General Data Protection Regulation*
GIRC	Governança, Integridade, Riscos e Controles Internos
HLPNs	*Higher Level Petri Nets*
IA	Inteligência Artificial
IDP	Inventário de Dados Pessoais
ISO	*International Organization for Standardization*
ISM	*Interpretive Structural Modeling*
IoT	*Internet of Things*
LGPD	Lei Geral de Proteção de Dados
MCTI	Ministério da Ciência, Tecnologia e Inovação
MJ	Ministério da Justiça
MJSP	Ministério da Justiça e Segurança Pública
MP	Ministério Público
MS	Ministério da Saúde
MSAs	*Multiple Sensitive Attributes*
OMS	Organização Mundial da Saúde
PL	Projeto de Lei

PoC	*Proof-of-Concept*
RE	Risco Esperado
RO	Risco Obtido
RNP	Rede Nacional de Ensino e Pesquisa
RUTE	Rede Universitária de Telemedicina
SGD	Secretaria de Governo Digital
SQL	*Structured Query Language*
TCI	Termo de Consentimento Informado
TCLE	Termo de Consentimento Livre e Esclarecido
TCU	Tribunal de Contas da União
TDIC	Tecnologia Digital de Informação e de Comunicação
TFISM	*Textual Fuzzy Interpretive Structural Modeling*
TIC	Tecnologia da Informação e Comunicação
UE	União Europeia
UERJ	Universidade do Estado do Rio de Janeiro
UNASUS	Universidade Aberta do SUS

SUMÁRIO

INTRODUÇÃO

Descrição do tema

A pandemia desencadeada pelo novo coronavírus (SARS-CoV-2), que se espalhou rapidamente pelo mundo a partir do final de 2019, afetando milhões de pessoas, e levando a uma crise de saúde global sem precedentes na história recente, ficou conhecida no mundo como *Coronavirus Disease 2019* (COVID-19), e reconhecida no Brasil sob o mesmo nome (Secretaria de Estado da Saúde de São Paulo, 2019). Esta pandemia impulsionou significativamente a digitalização dos negócios relacionados à área da Saúde. Este avanço foi notadamente perceptível no crescimento da Telemedicina e da Telessaúde, cujas definições serão exploradas posteriormente. Como consequência imediata dessa transformação, observou-se um aumento exponencial no tratamento[1] de dados pessoais[2], e principalmente, dados pessoais sensíveis[3], por meio de sistemas de Tecnologia da Informação e Comunicação (TIC). Atualmente, uma questão premente em escala global envolve a proteção da privacidade dos dados, especialmente aqueles relacionados à saúde, os quais pertencem intrinsecamente aos indivíduos aos quais estão associados. Esta preocupação torna-se ainda mais significativa quando consideramos o tratamento desses dados pessoais por parte das organizações de saúde e outras entidades responsáveis para a guarda destes dados pessoais sensíveis.

Esta dissertação intersecciona múltiplas áreas do saber, englobando a Medicina, com enfoque especial na Saúde Digital, além de tópicos fundamentais como Privacidade e Segurança da Informação, a análise e identificação de Riscos, e a Inteligência Artificial (IA), com ênfase na Lógica Fuzzy. A pesquisa também aborda aspectos jurídicos e regulatórios, incluindo

1 Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2 Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

3 Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

compliance[4] e a aderência às normas técnicas estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT) e pela *International Organization for Standardization* (ISO), entre outras. Importante ressaltar que, embora o presente estudo não vise a uma análise exaustiva de cada disciplina mencionada, ele busca estabelecer um entendimento equilibrado de sua relevância individual, assegurando assim uma compreensão integrada do conteúdo aqui discutido.

A Saúde Digital representa a integração das tecnologias da informação e comunicação ao âmbito da saúde, visando o aprimoramento contínuo da qualidade assistencial, o incremento da eficiência operacional e a segurança dos pacientes, além de promover a saúde e o bem-estar geral. Este campo abarca um espectro amplo de inovações tecnológicas, que vão desde os sistemas eletrônicos de registros em saúde e as plataformas de telemedicina e telessaúde, até os aplicativos de monitoramento de saúde em dispositivos móveis e os dispositivos vestíveis, ou *wearables*[5], para acompanhamento da atividade física. Tais inovações têm aplicabilidade extensiva na saúde, abrangendo diagnóstico, manejo clínico, prevenção e fomento ao bem-estar. A Saúde Digital é reconhecida como uma via promissora para transpor obstáculos geográficos e econômicos, democratizando o acesso aos serviços de saúde em regiões isoladas ou carentes de recursos. Contudo, a implementação dessa vertente digital enfrenta desafios significativos, que incluem a proteção da privacidade e a segurança dos dados dos usuários, assim como a garantia de acessibilidade e a adequação ao uso por diferentes populações (Organização Pan-Americana da Saúde, 2015).

A Privacidade vem sendo debatida no mundo, desde o século XIX, com conceitos que foram evoluindo ao longo das décadas. As regras que protegem a privacidade dão aos cidadãos ao redor do mundo, a capacidade de fazerem valer seus direitos em face de desequilíbrios de poderes significativos, como os que são detidos por grandes empresas, com destaque para as

---

[4] *Compliance*: requisitos que uma organização ou pessoa natural, mandatoriamente ou voluntariamente, têm que cumprir, a fim de atender a determinadas obrigações resultantes de suas atividades, produtos e serviços, e avaliações de impactos em suas operações.

5 Dispositivo vestível ou *werable*: é um tipo de tecnologia eletrônica que pode ser vestida no corpo, como parte de um acessório ou até mesmo integrada nas roupas. Esses dispositivos geralmente têm capacidades inteligentes, como conexão à internet, sensores para monitorar diversos aspectos da saúde e do bem-estar, e a habilidade de interagir com outros dispositivos inteligentes, como smartphones e computadores. Alguns exemplos comuns de dispositivos *wearables* incluem: ***Smartwatches***: Relógios que fazem muito mais do que apenas mostrar as horas. Eles podem rastrear atividades físicas, monitorar a saúde, receber notificações de mensagens e e-mails, e até mesmo fazer chamadas; ***Fitness Trackers***: Dispositivos focados em monitorar atividades físicas e saúde, como a contagem de passos, monitoramento do sono, frequência cardíaca e outras métricas de exercício; **Óculos Inteligentes**: Óculos equipados com tecnologia que pode oferecer realidade aumentada, mostrar notificações ou até mesmo tirar fotos; **Roupas Inteligentes**: Roupas que têm sensores integrados para coletar dados sobre o corpo do usuário, como a postura, a respiração e o movimento; e **Dispositivos Médicos *Wearables***: Dispositivos projetados para monitorar condições médicas específicas, como monitores de glicose para diabéticos.

Big Techs[6], como, por exemplo, Apple, Amazon, Facebook, Google e Microsoft. Essas organizações têm um enorme impacto na economia global e na vida cotidiana das pessoas, e são conhecidas por coletar e armazenar grandes quantidades de dados pessoais de usuários de seus produtos, o que levanta questões sobre privacidade e segurança de dados. Devido ao seu tamanho e influência, essas empresas têm sido alvo de escrutínio regulatório em muitos países, com debates em andamento sobre como lidar com suas práticas de negócios e impacto na sociedade em geral (Privacy International, 2017).

A Gestão de Riscos de Privacidade configura-se como uma metodologia estratégica essencial para a administração dos riscos atrelados à privacidade dos indivíduos e à salvaguarda dos seus dados pessoais, especialmente aqueles de natureza sensível, como os dados de saúde. Esta gestão envolve a identificação criteriosa dos dados que requerem proteção elevada e a implementação de controles robustos para atenuar potenciais riscos. Portanto, é imperativo que organizações e profissionais que tratem dados pessoais e dados pessoais sensíveis de pacientes, parceiros ou colaboradores, conforme o caso, adotem práticas rigorosas de privacidade e segurança da informação. A Gestão de Riscos de Privacidade é fundamental para avaliar a magnitude do risco de violações de privacidade e para a instauração de estratégias preventivas e de redução de riscos. Ademais, esta abordagem é vital para que as empresas consolidem a confiança de seus clientes e atendam às exigências legais e éticas concernentes à proteção de dados pessoais (Roberto *et al*., 2020).

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709, datada de 14 de agosto de 2018, impôs a todas as entidades públicas e privadas, assim como a pessoas físicas que tratam dados pessoais e/ou sensíveis para fins comerciais, uma nova onda de desafios e incertezas. O perigo de tratar tais dados sem fundamentação legal adequada para o seu tratamento, sem um ciclo de vida definido e sem aderência às melhores práticas – isto é, em desacordo com as exigências da LGPD – é substancialmente alto, especialmente pela falta de conformidade regulatória, conhecida como *compliance*.

A LGPD, nos artigos 7º e 11, delineia um conjunto abrangente de diretrizes para a gestão de dados pessoais e sensíveis. Estes artigos estipulam as hipóteses legais para tratamento de dados pessoais e dados pessoais sensíveis, respectivamente. O principal objetivo dessa norma-

[6] *Big Techs*: é o termo utilizado para se referir às grandes empresas de tecnologia, predominantemente baseadas no Vale do Silício, nos Estados Unidos, que têm um impacto significativo na economia global, na sociedade e na cultura devido à sua escala, alcance e poder de mercado. Estas empresas são líderes em inovação, desenvolvendo produtos e serviços que são amplamente utilizados em todo o mundo e influenciando significativamente o modo como vivemos e trabalhamos.

tiva é assegurar a privacidade e garantir a segurança dos dados pessoais e dados pessoais sensíveis dos indivíduos, estabelecendo um conjunto de fundamentos, princípios e obrigações que devem ser seguidos por todas as partes envolvidas no tratamento desses dados. (Brasil, 2018).

Além das disposições da LGPD, é importante salientar a existência de um arcabouço jurídico que contempla a privacidade em diversas outras normas constitucionais, codificadas, esparsas ou consolidadas. Contudo, a Constituição Federal do Brasil, de 1988, é um marco que eleva a privacidade ao patamar de direito fundamental. O artigo 5º, inciso X, da Carta Magna, assevera a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo o direito à reparação de prejuízos materiais ou morais resultantes de sua transgressão. Este enunciado constitucional é um pilar para a proteção da privacidade no ordenamento jurídico brasileiro, e serve de fundamento para a legislação infraconstitucional, incluindo a própria LGPD (Brasil, 1988).

Dessa forma, a Constituição brasileira reconhece a importância da privacidade e estabelece a proteção do direito à intimidade, vida privada, honra e imagem das pessoas, bem como a proteção do sigilo das comunicações e dos dados pessoais. Esses direitos fundamentais têm sido ampliados e regulamentados por leis específicas, como a LGPD, que tem como objetivo garantir a privacidade e a proteção de dados pessoais dos cidadãos brasileiros.

Motivação

O problema que motivou o desenvolvimento deste projeto está diretamente relacionado ao tratamento de dados pessoais e dados pessoais sensíveis, sem a adoção de uma das hipóteses legais, ou com a adoção equivocada, das previstas na LGPD e do cumprimento de boas práticas, princípios e outras determinações previstas na Lei, que pode acarretar sanções aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD), ações judiciais e até mesmo sanções de outros órgãos como PROCON, SENACON, quando há a relação de consumo ou o próprio Ministério Público (MP), além de outras entidades fiscalizadoras, como os órgãos de proteção ao trabalhador MPT, MPF, dentre outros (Luz, 2022).

A motivação deste trabalho emerge da necessidade crescente de gerenciar a privacidade e proteção de dados pessoais e dados pessoais sensíveis em um mundo cada vez mais digitalizado e interconectado. Com a adoção generalizada de tecnologias para a Saúde Digital, e a implementação de normativas como a LGPD, surge um imperativo para as organizações de adequarem suas operações às novas exigências legais e às expectativas dos cidadãos quanto à privacidade e a segurança da informação.

No contexto dos temas discutidos, como Telessaúde, privacidade e a LGPD, a IA surge como um instrumento potencialmente poderoso para auxiliar os agentes de tratamento[7] a alcançarem a conformidade com a legislação.

Existe uma variedade de outros sistemas no mercado, contudo eles adotam controles de normas técnicas, com destaque para as normas técnicas da ABNT e da ISO e a partir de avaliação booleana, o risco é medido.

Atualmente, diante do cenário de conformidade com a LGPD, observa-se uma diversidade de ferramentas disponíveis. No entanto, é evidente uma lacuna significativa e consequente escassez de aplicações no mercado em relação a aplicações que adotem sistemas de Gestão de Risco ancorados em dados quantitativos e fundamentados na Lógica Fuzzy, em contraposição à tradicional lógica booleana. Ao contrário, a disponibilidade fica a cargo de aplicações que se baseiam em controles de normas técnicas internacionais para garantir a confiabilidade de seus resultados. Ou seja, estas aplicações verificam se aquele agente de tratamento atendeu ou não aquele controle, em um universo de diferentes controles, e calcula o risco, considerando a probabilidade. Ou seja, não é utilizada a IA, e consequentemente a Lógica Fuzzy e nem tão pouco dados quantitativos associados, como, por exemplo, número de titulares, número de dados pessoais e dados pessoais sensíveis que estão sendo tratados, número de dados pessoais e dados pessoais fora do território brasileiro ou sem uma hipótese de tratamento ou fora dos seus ciclos de vida.

7 Agentes de tratamento: são definidos no Art. 5º, IX como o controlador e o operador. O Art. 5º da LGPD também detalha conceitos-chave para a compreensão dos termos supracitados. Conforme os incisos VI e VII deste artigo: O Controlador é a pessoa natural ou jurídica, de direito público ou privado, que tem a autoridade para tomar as decisões relativas ao tratamento de dados pessoais, incluindo os dados pessoais sensíveis; O Operador, por outro lado, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador age sob as determinações do controlador, executando as ações práticas de tratamento destes dados, mas sem tomar decisões sobre este tratamento.

Objetivos

A Gestão de Risco com o emprego da Lógica Fuzzy não é algo inovador, e já vendo sendo amplamente abordado na literatura acadêmica. Contudo, as empresas vêm tentando disponibilizar ferramentas no mercado que auxiliem as adequações de outras empresas na mitigação de riscos relacionados ao descumprimento da LGPD. Este risco tende a ser maior na área da Saúde, com destaque para a Saúde Digital pela criticidade dos dados pessoais sensíveis. Este argumento é corroborado por Projetos de Lei, Deliberações, Pareceres, Recomendações e Resoluções de Conselhos de Classes, federais e regionais, com destaque para o Conselho Federal de Medicina (CFM). Sendo assim, a seguir, são apresentados os objetivos geral e específicos deste trabalho.

Objetivo geral

No presente trabalho, propõe-se o desenvolvimento de um sistema computacional inovador que emprega a Lógica Fuzzy para a Identificação de Riscos em conformidade com as normativas da LGPD no contexto da Saúde Digital. Esta dissertação visa explorar tanto os benefícios quanto os desafios inerentes à adoção dessa tecnologia na sociedade, abordando também as questões legais relacionadas à implementação de soluções tecnológicas no setor de saúde. Para embasar este estudo, foi realizada uma extensa pesquisa bibliográfica, a fim de oferecer uma análise crítica e holística sobre o tema. Espera-se que os achados desta pesquisa contribuam significativamente para o entendimento do papel das tecnologias emergentes na área da saúde e auxiliem na formulação de decisões estratégicas por profissionais e entidades do setor, garantindo a aderência às exigências da LGPD.

É importante ressaltar que, para fundamentar o processo de desenvolvimento do sistema computacional proposto na dissertação, foram utilizadas normas de Gestão de Riscos reconhecidas internacionalmente. Essa abordagem visa assegurar que o sistema esteja alinhado com as melhores práticas globais, garantindo uma implementação eficaz e segura. A adoção desses padrões internacionais de Gestão de Riscos não apenas fortalece o embasamento teórico do projeto, mas também contribui para a robustez e confiabilidade da solução proposta, especialmente no que tange à conformidade com a LGPD e às especificidades da Saúde Digital. Dessa forma, o projeto se beneficia de uma perspectiva global, integrando conhecimentos e práticas

testadas e aprovadas no cenário internacional para aprimorar a Gestão de Riscos em tecnologias aplicadas à saúde.

Objetivos específicos

Dentre os objetivos secundários desta pesquisa, destacam-se os seguintes pontos fundamentais:

a) Foco na identificação de variáveis linguísticas que são pertinentes ao tratamento de dados pessoais. Este passo é crucial para a elaboração de um modelo de Lógica Fuzzy que reflita com precisão as nuances do tratamento de dados na realidade prática;
b) Desenvolvimento de um Conjunto de Regras Fuzzy: Proposição de um conjunto de regras Fuzzy destinadas à inferência de riscos relacionados a possíveis sanções aplicadas pela ANPD. Essa construção é essencial para o processo de tomada de decisão no sistema proposto;
c) Criação de Casos de Teste Artificiais: Desenvolvimento de cenários de teste artificiais para a avaliação preliminar do modelo proposto. Estes casos servirão para testar a eficácia do sistema em condições controladas;
d) Avaliação do Modelo com Caso Real: Aplicação do modelo em um contexto real para verificar sua efetividade e precisão em um ambiente prático. Esta etapa é vital para validar a aplicabilidade do sistema no mundo real;
e) Estabelecimento de um Protocolo de Avaliação de Risco: Formulação de um protocolo específico para a Avaliação de Riscos. Este protocolo visa estabelecer um procedimento padrão para a identificação e Gestão de Riscos potenciais;
f) Comparação entre o modelo proposto nesta Dissertação e o Modelo de Avaliação de Riscos de Segurança e Privacidade, da SGD;
g) Investigação dos tipos de risco aos quais clínicas da área da Saúde, incluindo Medicina/Telemedicina e Nutrição/Telenutrição, podem estar expostas, por meio de um questionário *online*;
h) Análise de trabalhos correlatos, a fim de apurar os fundamentos e similaridades com o presente estudo.

Esses objetivos secundários são fundamentais para a consolidação do modelo proposto, assegurando sua relevância prática e eficácia na Gestão de Riscos no contexto da LGPD e da Saúde Digital.

A adoção de sistemas de IA baseados em Lógica Fuzzy pode ser particularmente benéfica, uma vez que esta técnica permite o manejo de incertezas e a modelagem de decisões em ambientes complexos e imprecisos, como é o caso da interpretação da legislação e a tomada de decisões referentes à privacidade e proteção de dados pessoais. A Lógica Fuzzy pode ser utilizada para avaliar riscos, e garantir que as decisões tomadas em relação ao tratamento de dados sejam assertivas e alinhadas com os princípios e diretrizes da LGPD.

Organização do trabalho

A organização desta dissertação foi planejada para oferecer coerência e lógica através dos diferentes aspectos do estudo, garantindo uma compreensão abrangente do tema e dos objetivos propostos. A dissertação inicia-se com uma introdução que contextualiza o tema central do estudo, destacando sua relevância e oferecendo uma visão geral do conteúdo subsequente. A motivação por trás da escolha do tema é discutida, juntamente com a contribuição esperada para a área de conhecimento em questão. Além disso, um resumo da organização da dissertação é fornecido, delineando o que será abordado em cada seção.

Em seguida, os objetivos da pesquisa são claramente definidos, tanto o específico quanto os objetivos gerais, a fim de orientar as expectativas em relação aos resultados esperados.

A seção de Material e Método é fundamental para embasar o estudo. Ela inclui uma análise detalhada dos conceitos-chave e do estado da arte relacionados ao tema, abrangendo áreas como Telemedicina, Teleconsulta, mHealth, eHealth e Saúde Digital. Além disso, explora a literatura sobre Gestão de Riscos, privacidade e proteção de dados, com destaque para a Lei Geral de Proteção de Dados. A introdução à Inteligência Artificial, com ênfase na Lógica Fuzzy, regras de modelagem e o Modelo de Inferência de Mamdani é apresentada, juntamente com uma revisão de trabalhos correlatos. A metodologia adotada para o desenvolvimento do sistema computacional proposto é detalhada, incluindo a modelagem do problema, a formulação da pergunta de pesquisa e a definição das variáveis linguísticas pertinentes à Lógica Fuzzy.

Os resultados obtidos são apresentados na seção subsequente, incluindo comparações entre o modelo proposto e outros modelos existentes, bem como análises dos parâmetros relacionados às variáveis linguísticas.

Na seção de Discussão, são apresentados trabalhos correlatos, comparados entre si por meio de uma tabela. Também são detalhadas as normas adotadas pela Secretaria de Governo Digital (SGD) para a elaboração de seu modelo. As origens e implicações dos resultados obtidos são examinadas, proporcionando uma análise aprofundada dos achados.

A seção de Conclusão fornece uma síntese dos resultados até o momento, discutindo suas implicações práticas e teóricas, além de delinear possíveis trabalhos futuros que possam estender o estudo atual.

A lista de Referências é apresentada para garantir a credibilidade acadêmica, compilando todas as fontes citadas ao longo da dissertação.

Por fim, a seção de Apêndice inclui material suplementar que oferece suporte adicional ao conteúdo principal do trabalho, como dados brutos e instrumentos de pesquisa.

Esta estrutura foi pensada para facilitar a leitura do documento, promovendo um fluxo lógico e sistemático que apoia a argumentação central do trabalho e destaca a originalidade e relevância da pesquisa realizada.

1 MATERIAIS E MÉTODOS

1.1 Fundamentação teórica

1.1.1 Telemedicina, Teleconsulta, mHealth, eHealth e Saúde Digital

O termo telemedicina começou a ter maior relevância no início dos anos 90. Uma rápida busca na base PubMed®, pelo termo em inglês *telemedicine*, mostra que no ano de 1990, houve a publicação de 7 artigos e em 1999, houve a publicação de 82 artigos. De 1962 a 2024, 60.656 artigos foram publicados (PubMED, 2024).

Segundo a Organização Mundial da Saúde (OMS, 1997), o termo telemedicina pode ser definido como:

> Serviços e sistemas relacionados à saúde, realizados à distância por meio de Tecnologias de Informação e Comunicação (TIC), para fins de promoção global da saúde, controle de doenças e assistência à saúde, bem como educação, gestão, e pesquisa para a saúde. É importante ressaltar que, em muitos casos, a distância é um fator crítico.

O Conselho Federal de Medicina (CFM) define a telemedicina como o exercício da medicina mediado por Tecnologias Digitais, de Informação e de Comunicação (TDICs), para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde (Conselho Federal de Medicina, 2022a).

Segundo Plazzotta e Sommer (2020), podemos definir a telemedicina de maneira simples, comum e globalmente aceita como: “a assistência médica ou cuidados de saúde quando os participantes estão separados por distância ou tempo e a tecnologia de telecomunicações é usada”.

Na visão destes autores, caso seja utilizada as telecomunicações ou as tecnologias da informação para o cuidado de saúde, de algum modo, se emprega a telemedicina.

O termo telemedicina restringe os cuidados de saúde à Medicina e aos médicos, com o emprego de sistemas de Tecnologia da Informação e Comunicação (TIC). Entretanto, outras profissões, incluindo a psicologia e a odontologia, podem recorrer a sistemas de TIC para o atendimento a sujeitos de cuidado, neste caso podemos adotar o termo teleconsulta, o qual é

mais abrangente. Este termo também engloba a medicina, e consequentemente a telemedicina, as já citadas psicologia e odontologia, além de outras disciplinas, como a nutrição, a enfermagem, e outras mais, relacionadas à saúde (Plazzotta; Sommer, 2020).

Sendo assim, é importante reiterar que telemedicina e telessaúde não têm o mesmo significado. De fácil dedução, o termo telessaúde é mais amplo e inclui, além da consulta e atenção sanitária, outras ferramentas, como o telemonitoramento, a telereabilitação, mas também engloba a capacitação e educação de equipes de saúde e de sujeitos de cuidado, à distância, com o emprego de sistemas de TIC. A telessaúde permite o contato remoto, atendimento, aconselhamento, lembretes, educação, intervenção, supervisão e encaminhamentos para pacientes e médicos, e outros profissionais da saúde, à distância (Plazzotta; Sommer, 2020).

Segundo a Organização Pan-Americana da Saúde 2015), no início dos anos 2000, projetos de telemedicina e telessaúde, envolvendo a União Europeia (UE) e a América Latina, foram iniciados, dentre os quais, cabe citar:

a) Programa @lis Alliance *for the Information Society,* com destaque para o E-México, que avançou o Programa Nacional de Telemedicina do México;
b) T@lemed, que influenciou a criação da Rede Universitária de Telemedicina (RUTE) sob a coordenação da Rede Nacional de Ensino e Pesquisa (RNP), no Brasil, com recursos do Ministério da Ciência, Tecnologia e Inovação (MCTI). Esta rede já está presente em mais de 140 hospitais universitários e de ensino no Brasil;
c) eHAS *Enlaces Hispano Americano de Salud*, que demonstrou a viabilidade em comunidades na selva sem energia;
d) HCN *Health Care Network*, que inspirou o Tele Minas Saúde; e
e) RedClara, também conhecida como Cooperação Latino-Americana de Redes Avançadas, sendo a rede de fibra ótica dedicada ao ensino e à pesquisa conectando as redes acadêmicas nos países da América Latina.

Em 2006, houve diálogo entre a RUTE, o Ministério da Saúde e o Ministério da Educação, resultando na articulação entre a RUTE, o Programa Telessaúde Brasil, e a Universidade Aberta do SUS (UNASUS). Essas três redes, de caráter público, impulsionaram a atuação em rede no setor saúde, incluindo a atenção, a formação, a pesquisa e a gestão em saúde (Organização Pan-Americana da Saúde, 2015.

A adoção da telessaúde, na teletriagem, reduziu filas de espera por especialidades. Além de qualificar os atendimentos e torná-los mais eficazes, a telessaúde tornou-se uma estratégia de fortalecimento da atuação em rede – apoiando a referência e contrarreferência de paciente -

e ampliação do acesso ao atendimento humanizado. Em média, 60% das teleconsultorias levou a uma mudança na conduta inicialmente planejada, reduzindo custos, em especial com o tratamento fora de domicílio, resultando em maior resolubilidade dos casos (Organização Pan-Americana da Saúde, 2015).

Visto o exposto, a telessaúde destina-se não só aos sujeitos de cuidado, mas também aos profissionais de saúde, permitindo educação à distância, reuniões, supervisões, apresentações entre profissionais; informação *online*, gestão da informação de saúde, e integração do sistema de saúde. Neste contexto, uma das distinções-chave da telemedicina surge: a amplitude da telessaúde vai além do atendimento clínico tradicional, abraçando iniciativas que incluem educação contínua, programas de teleducação, telementoria e serviços de saúde móvel, também referidos como mHealth (Plazzotta; Sommer, 2020).

Em 27 de dezembro de 2022 foi sancionada a Lei Federal n.º 14.510 que:

a) alterou a Lei n.º 8.080/1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional;
b) alterou a Lei n.º 13.146/2015, e incluiu no Art. 19, a alínea V - aprimoramento do atendimento neonatal, com a oferta de ações e serviços de prevenção de danos cerebrais e sequelas neurológicas em recém-nascidos, inclusive por telessaúde; e
c) revogou a Lei n.º 13.989/2020, que dispunha sobre o uso da telemedicina durante a crise causada pelo coronavírus (SARS-CoV-2).

A Lei n.º 8.080/1990 passou a vigorar acrescida do Título III-A: Da Telessaúde e definiu a telessaúde como:

> A modalidade de prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação, que envolve, entre outros, a transmissão segura de dados e informações de saúde, por meio de textos, de sons, de imagens ou outras formas adequadas (Brasil, 2022).

As inovações tecnológicas são uma realidade constante, quando pensamos na saúde. Estas tendem a extrapolar as tecnologias, o que pode acarretar uma inovação incremental em processos, serviços e métodos. E, a fim de acompanhar tais evoluções, surgiu o conceito de mHealth, também conhecido como Cibersaúde, mSaúde ou Saúde Móvel. Este conceito pode ser entendido como práticas relacionadas à saúde, realizadas, por meio de dispositivos móveis, como, por exemplo, *smartphones*, assistentes digitais e dispositivos de monitoramento, com destaque para os *smartwatches* e *smartbands*.

A Saúde Eletrônica, também conhecida como e-Saúde ou e-Health, é centrada ao redor do provedor de saúde e embora, às vezes, seja utilizada como sinônimo de telemedicina e telessaúde, o termo é mais abrangente. Segundo (Shaw *et al*., 2017), podemos definir Saúde Eletrônica como:

> Forma de incorporar a tecnologia nos cuidados de saúde para promover a saúde e o bem-estar. Pode ser tão simples quanto usar alguma forma de tecnologia para automonitorar sua atividade, comunicar-se com diferentes pessoas sobre saúde e condições de saúde, coordenar os cuidados no sistema de saúde e usar ativamente a tecnologia para fornecer intervenção.

Mais abrangente do que o conceito de eHealth, há o termo Saúde Digital, que lida com inúmeras soluções digitais que têm como finalidade, a melhoria da saúde e da qualidade de vida dos sujeitos de cuidado. Englobadas pelo termo Saúde Digital, temos a tecnologia, a robótica, a inteligência artificial, a internet das coisas, termo originado da língua inglesa, *Internet of Things* (IoT), a telessaúde, a mHealth e a eHealth. Cabe destacar que não foram exauridas as demais disciplinas que podem ser englobadas pelo referido termo, Saúde Digital. Além das mencionadas, inclui-se também a análise de dados de saúde, a realidade virtual na medicina, a biotecnologia aplicada à saúde, entre outras áreas em constante evolução. A Saúde Digital é um campo diversificado e em expansão, que incorpora uma ampla gama de tecnologias e abordagens para promover o bem-estar e a gestão da saúde (Plazzotta; Sommer, 2020).

A Saúde Digital está revolucionando o conceito de assistência médica, já que coloca os sujeitos de cuidado no cerne do conceito, e não os provedores, e assim permite, desta forma, que estes pacientes acompanhem, gerem e melhorem os seus tratamentos, tornando-os mais participativos, informados, independentes e exigentes (Deetjen *et al*., 2020).

O Ministério da Saúde (MS) define Saúde Digital como:

> O uso de recursos de TIC para produzir e disponibilizar informações confiáveis sobre o estado de saúde para os cidadãos, profissionais de saúde e gestores públicos. O termo Saúde Digital é mais abrangente do que e-Saúde e incorpora os recentes avanços na tecnologia, como novos conceitos, aplicações de redes sociais, Internet das Coisas (IoT), Inteligência Artificial (IA), entre outros (Ministério da Saúde, 2023).

Em 2005, a OMS já compartilhava com os países membros desta organização a urgência e a necessidade de estes considerarem a elaboração de um plano estratégico de longo prazo para o desenvolvimento e implementação de serviços de e-Saúde, nas diversas áreas do setor da saúde, incluindo a administração da saúde, que incluiria uma estrutura jurídica e infraestrutura adequadas e incentivaria parcerias públicas e privadas (Organização Mundial da Saúde, 2005).

A OMS define uma intervenção de saúde digital como uma funcionalidade discreta da tecnologia digital aplicada para alcançar objetivos de saúde e é implementada em aplicativos de saúde digital e sistemas de TIC, incluindo canais de comunicação como mensagens de texto (Organização Mundial da Saúde, 2019b).

Em 2019, a OMS deu início à Estratégia Global de Saúde Digital, tradução livre do nome em inglês *Global Strategy on Digital Health*. A Estratégia Global de Saúde Digital enfatiza que os dados de saúde devem ser classificados como dados pessoais sensíveis, ou informações de identificação pessoal, que requerem um alto padrão de segurança e proteção. Portanto, enfatiza a necessidade de uma forte base legal e regulatória para proteger a privacidade, confidencialidade[8], integridade[9] e disponibilidade[10] (CID)[11] de dados e o processamento de dados pessoais de saúde, e lidar com segurança cibernética, construção de confiança, responsabilidade e governança, ética, equidade, capacidade construção e alfabetização, garantindo que dados de boa qualidade sejam coletados e posteriormente compartilhados para apoiar o planejamento, comissionamento e transformação dos serviços (Organização Mundial da Saúde, 2019a).

Um aspecto muito significativo da proposta de Estratégia Global de Saúde Digital é que ela unifica, sob o termo Saúde Digital, todos os conceitos de aplicação das TICs em Saúde, incluindo e-Saúde, Telemedicina, Telessaúde e Saúde Móvel. Além de reduzir a fragmentação das aplicações da tecnologia em saúde, a Saúde Digital amplia o seu entendimento, em que se caracteriza como área de conhecimento e prática, e absorve os conceitos da utilização avançada da tecnologia, incluindo o uso de dispositivos pessoais e de tecnologias emergentes (Organização Mundial da Saúde, 2019a).

A vasta gama de possibilidades pelas quais as tecnologias digitais podem ser usadas para atender às necessidades dos sistemas de saúde é ampla e essas tecnologias continuam a evoluir devido à natureza inerentemente dinâmica do campo. Um ponto de partida para categorizar as diferentes maneiras pelas quais as tecnologias digitais estão sendo usadas para superar

[8] Confidencialidade: a propriedade de que a informação não está disponível ou divulgada a indivíduos, entidades ou por meio de processos não autorizados.
[9] Integridade: a propriedade de precisão e completude dos ativos, garantindo que a informação não esteja sujeita a alterações impróprias.
[10] Disponibilidade: a propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.
[11] CID: São os três critérios primários da segurança da informação: Confidencialidade, Integridade e Disponibilidade. Esses conceitos foram formalizados e popularizados ao longo das décadas. Atualmente, há mais dois elementos que fazem parte dos 5 Pilares da Segurança da Informação. Esses dois novos membros também são relevantes para os esforços de proteção do conhecimento: Autenticidade, que garante que, em um processo de comunicação, os remetentes não se façam passar por terceiros e que a mensagem não seja alterada durante a transmissão, com sua fonte anunciada; e Legalidade, que assegura que a informação foi produzida em conformidade com a legislação atual.

os desafios definidos do sistema de saúde é fornecido pela OMS através do *WHO's Classification of digital health interventions v1.0* (Organização Mundial da Saúde, 2018).

De acordo com Jandoo (2019), a OMS enfatizou a avaliação da privacidade e da segurança da informação, dos aplicativos digitais, incluindo a possibilidade de quaisquer consequências não intencionais, como uma lacuna fundamental na pesquisa para a saúde digital. As preocupações com a privacidade e a segurança da informação dos dados pessoais e dados pessoais sensíveis impactam a escolha das tecnologias digitais e os projetos relacionados a estas tecnologias.

Ainda, segundo a OMS, as ferramentas digitais devem atender aos padrões da Lei norte-americana 104-191, conhecida como *Health Insurance Portability and Accountability Act of 1996*[12], o *General Data Protection Regulation (GDPR)*[13], regulamento europeu que substituiu a Diretiva 46/ CE[14], de 1995, e a norma técnica *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. E, ainda, determina que os dados pessoais e dados pessoais sensíveis, consequentemente, devem ser pseudonimizados, coletados, armazenados e transferidos, conforme os regulamentos locais aplicáveis (Jandoo, 2019). No que se refere a regulamentos locais aplicáveis, a LGPD é evidenciada, além das leis supracitadas n.º 8.080/1990, n.º 13.146/2015 e n.º 14.510/2022, e dos padrões normativos disciplinados pelos conselhos federais, como, por exemplo, a Resolução do CFM n.º 2.314/2022[15].

Independente da definição ou do termo, um ponto indiscutível, que demanda atenção, é o tratamento de dados pessoais e dados pessoais sensíveis dos sujeitos de cuidado por meio de soluções digitais. Indiscutivelmente, a digitalização pode capacitar e tornar viável que tanto os indivíduos sob cuidados quanto os profissionais de saúde alcancem seus objetivos relacionados

---

[12] *Health Insurance Portability and Accountability Act of 1996*: esta lei foi sancionada para alterar o *Internal Revenue Code de 1986* para melhorar a portabilidade e a continuidade da cobertura de seguro saúde nos mercados de grupo e individual, para combater o desperdício, fraude e abuso no seguro saúde e na prestação de cuidados de saúde, para promover o uso de contas de poupança médicas, para melhorar o acesso a serviços e coberturas de cuidado de longo prazo, para simplificar a administração do seguro de saúde e para outros fins (Assistant Secretary for Planning and Evaluation, 1996).

[13] *General Data Protection Regulation (GDPR)*: também conhecido como Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e revoga a Diretiva 95/46/CE (Parlamento Europeu; Conselho, 2016).

[14] Diretiva 95/46/CE: diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Parlamento Europeu; Conselho, 1995).

[15] Resolução CFM n.º 2.314/2022: Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação (Conselho Federal de Medicina, 2022a).

à saúde. Todavia, há a necessidade de estar em *compliance* com os documentos jurídicos vigentes, sejam nos âmbitos legislativos, jurisprudentes ou doutrinários.

1.1.2 Gestão de Riscos

Nesta subseção, torna-se necessário simplificar certos termos e conceitos relativos à gestão de risco no contexto da segurança da informação e privacidade, devido à complexidade abrangente destes tópicos.

O GDPR impõe requisitos aos responsáveis pelo tratamento[16], que se envolvem em atividades de alto risco. Especificamente, antes de se envolver em uma atividade de alto risco, uma organização pode ser obrigada a consultar uma autoridade de proteção de dados e, em seguida, realizar uma avaliação detalhada do impacto na privacidade. Caso haja um incidente de segurança da informação ou privacidade, pode ser necessário notificar os indivíduos potencialmente afetados (Maldoff, 2016).

Para as atividades que não se qualificam como de alto risco, aqueles responsáveis pelo tratamento de dados pessoais devem ainda adotar medidas proporcionais ao nível de risco associado à atividade. Isso ocorre porque esses responsáveis devem assegurar um nível adequado de segurança de dados, conforme o risco envolvido, e implementar medidas baseadas na avaliação de risco, visando cumprir as obrigações gerais estabelecidas pelo GDPR. No entanto, quando o risco para os titulares de dados é considerado baixo, um responsável pelo tratamento de dados pessoais, geralmente, está isento da obrigação de notificar as autoridades em caso de violação de dados, e um responsável pelo tratamento estrangeiro pode ser dispensado da exigência de nomear um representante dentro da UE (Maldoff, 2016).

Embora o GDPR seja omisso sobre como os responsáveis pelo tratamento devem avaliar e quantificar o risco, certas tendências emergem das seções em que o risco é citado e que orientam, em parte, os responsáveis pelo tratamento na implementação de uma abordagem baseada em risco (Maldoff, 2016).

[16] Responsável pelo tratamento: o Art. 4.º, 7), do GDPR - a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União, ou de um Estado-Membro.

Ao realizar uma busca pelo termo “risco” no texto do GDPR, são apresentados 74 resultados. Da mesma forma, ao realizar uma busca com o mesmo termo no texto da LGPD, são exibidos 11 resultados. Isso evidencia que ambas as normas adotam uma abordagem baseada no risco, também conhecida como *risk-based approach*. Essa abordagem significa que as regulamentações consideram o nível de risco associado ao tratamento de dados pessoais e estabelecem requisitos proporcionais ao risco, almejando proteger a privacidade e os direitos dos titulares de dados conforme a gravidade das ameaças potenciais.

Os caminhos para cumprir com a obrigação legal de estar *compliant* com a LGPD nem sempre são claros. Embora a LGPD tenha sido resultado de consultas públicas conduzidas pelo Ministério da Justiça e Segurança Pública (MJSP), anteriormente conhecido como Ministério da Justiça (MJ), em 2010 (Santos, 2011), é evidente que o seu texto foi significativamente influenciado pelo GDPR. Além disso, documentos como Avaliação de Impacto sobre a Proteção de Dados (GDPR) e Relatório de Impacto sobre a Proteção de Dados Pessoais (LGPD) reforçam a preocupação com a gestão do risco.

Visto o exposto, não é possível tratar risco sem gerir risco. E, para a busca das melhores práticas, recorre-se às normas técnicas da ABNT e da ISO. A norma técnica *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, já citada, foi adotada, de forma idêntica, em conteúdo técnico, estrutura e redação, no Brasil, pelo Comitê Brasileiro de Tecnologias da Informação e Transformação Digital (ABNT/CB-021), e pela Comissão de Estudo e Segurança da Informação, Segurança Cibernética e Proteção da Privacidade (CE-021:004.027). Este Projeto de Revisão seguiu para Consulta Pública, conforme o Edital n.º 10, de 19 de outubro de 2022 a 17 de novembro de 2022 (Associação Brasileira de Normas Técnicas, 2022).

A busca pelo termo risco, na norma NBR ISO/ IEC 27001, retorna 55 resultados. Esta norma inclui: Ações para abordar riscos e oportunidades; Avaliação de riscos de segurança da informação; e Tratamento de riscos de segurança da informação. E, em sua bibliografia, outras normas técnicas, relacionadas a risco, são citadas, como, por exemplo, a norma ABNT NBR ISO/ IEC 27005:2019 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação e a norma ABNT NBR ISO 31000:2018 – Gestão de Riscos - Diretrizes (Associação Brasileira de Normas Técnicas, 2022).

As normas NBR 27001 e 27005 são mais específicas para a segurança da informação. Sendo necessário consultar outras normas técnicas que deem ênfase à privacidade. Neste caso, as normas técnicas que cumprem esse papel são:

a) a ABNT NBR ISO/ IEC 27701 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes. A busca pelo termo risco, nesta norma, retorna 68 resultados (Associação Brasileira de Normas Técnicas, 2019);
b) ABNT NBR ISO/IEC 27557:2023 – Segurança da Informação, segurança cibernética e proteção da privacidade — Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional. A busca pelo termo risco, nesta norma, retorna 146 resultados (Associação Brasileira de Normas Técnicas, 2023).

Para este trabalho, também foi necessário adotar uma norma de riscos mais abrangente, e aplicável a qualquer atividade, a norma ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes, citada na norma ABNT NBR ISO/IEC 27557:2023, como a norma de aplicação. Esta norma define risco como efeito[17] da incerteza[18] nos objetivos. E define Gestão de Riscos como atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (Associação Brasileira de Normas Técnicas, 2018).

O Decreto n.º 9.203[19], de 22 de novembro de 2017, define em seu Art. 2º, inciso IV, Gestão de Riscos como:

> Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (Brasil, 2017).

O Decreto supracitado ressalta que uma das diretrizes da governança pública é a implementação de controles internos fundamentados na gestão de risco, que privilegiará ações estratégicas de prevenção antes de processos sancionadores, conforme o Art. 4º, inciso VI (Ministério da Gestão e da Inovação em Serviços Públicos; Governo Digital, 2022).

A Gestão de Riscos é amplamente difundida na administração pública federal, como exemplo, há as **Assessorias Especiais de Controle Interno (AECI), a Controladoria-Geral**

[17] Efeito: é um desvio em relação ao esperado, positivo ou negativo (Associação Brasileira de Normas Técnicas, 2018).
[18] Incerteza: A incerteza é o estado, mesmo parcial, de deficiência de informações relacionadas com a compreensão ou conhecimento de um evento, sua consequência ou probabilidade (International Organization for Standardization, 2022).
[19] Decreto n.º 9.203: dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

da União (CGU), o Tribunal de Contas da União (TCU) e a Rede GIRC (Ministério Da Gestão e da Inovação em Serviços Públicos; Governo Digital, 2022)**.**

Além das normas técnicas da ABNT e ISO, também há outros *frameworks*[20] que podem ser consultados para uma Gestão de Riscos bem fundamentada (Controladoria-Geral da União, 2021), com destaque para:

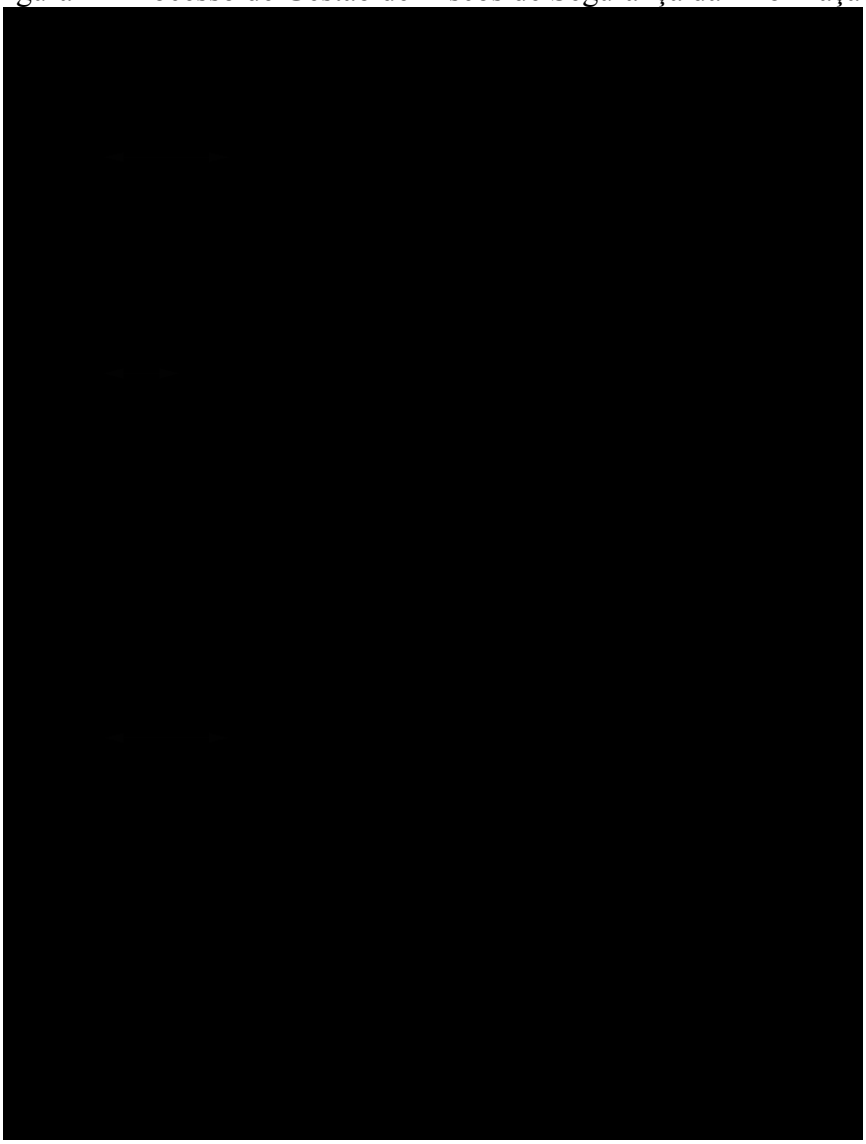
a) COSO *Report. Internal Control: Integrated Framework*, 1992;
b) COSO - ERM - *Enterprise Risk Management*, 2004;
c) Instrução Normativa Conjunta CGU/MP n.º 01, de 10 de maio de 2016.

O Risco é normalmente expresso em termos de fontes de risco, ou seja, de elementos que, individualmente ou combinados, têm o potencial para dar origem ao risco. Além das fontes de riscos, também são considerados os eventos potenciais, suas consequências e suas probabilidades (*International Organization for Standardization*, 2022).

O processo de Gestão de Riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de Identificação de Riscos, comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos, dentre outros, conforme a Figura 1 – Processo de Gestão de Riscos de Segurança da Informação (Associação Brasileira de Normas Técnicas, 2018).

[20] *Framework*: Um framework é uma estrutura ou modelo conceitual que fornece diretrizes, padrões e componentes pré-definidos para auxiliar no desenvolvimento, organização e solução de problemas em um determinado contexto.

Figura 1 - Processo de Gestão de Riscos de Segurança da Informação



Fonte: Associação Brasileira de Normas Técnicas, 2023

Contudo, para este trabalho, a ênfase da Gestão de Riscos será dada apenas à Identificação de Riscos. A intenção desta etapa é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Nesta etapa, é importante definir organização, que pode ser entendida como pessoa ou grupo de pessoas que tem suas próprias funções, responsabilidades, autoridades e relacionamentos para alcançar os seus objetivos (*International Organization for Standardization*, 2022).

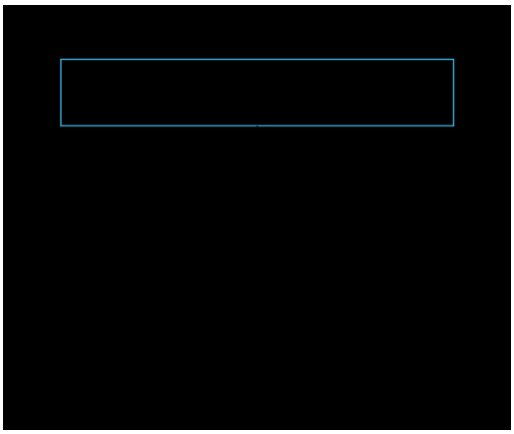
O conceito de organização também pode ser estendido ao empreendedor individual, além de abranger companhias, públicas ou privadas (Associação Brasileira de Normas Técnicas, 2020b).

A organização pode fazer uso de uma variedade de técnicas para identificar incertezas que podem afetar um ou mais objetivos. Convém que, os seguintes fatores e o relacionamento entre estes fatores sejam considerados:

a) fontes tangíveis e intangíveis de risco;
b) causas e efeitos;
c) ameaças e oportunidades;
d) vulnerabilidades e capacidades;
e) mudanças nos contextos externo e interno;
f) indicadores de riscos emergentes;
g) natureza e valor dos ativos e recursos;
h) consequências e seus impactos nos objetivos;
i) limitações de conhecimento e de confiabilidade da informação;
j) fatores temporais;
k) vieses, hipóteses e crenças dos envolvidos.

É importante ressaltar que a Identificação de Riscos é apenas uma das etapas do Processo de Avaliação de Riscos, que engloba: Identificação de Riscos; Análise de Riscos e Avaliação de Riscos, conforme Figura 2, a seguir.

Figura 2 - Processo de Avaliação de Risco



Fonte: O autor, 2023.

Quando se ressalta a Identificação de Riscos, refere-se aos riscos legais, que podem ser entendidos como riscos relacionados a questões legais, regulamentares e contratuais, e de direitos e obrigações extracontratuais (Associação Brasileira de Normas Técnicas, 2020b). No âmbito do presente trabalho, a referência a risco, está relacionado aos riscos legais relacionados às exigências da LGPD.

Conforme já abordado, o processo de gerenciamento de riscos em projetos é um processo iterativo, cíclico e dinâmico, que envolve a aplicação sistemática de políticas, procedimentos e práticas para atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, registro e relato de riscos. Contudo, a restrição do objetivo deste trabalho à Identificação de Riscos legais relacionados ao não cumprimento da LGPD é encontrar riscos que possam prevenir sanções previstas nesta Lei. Contudo, vai além, pois se busca mitigar o risco da operação de tratamento[21] de dados pessoais e dados pessoais sensíveis, em respeito aos reais donos destes dados, os titulares[22]. A Identificação de Riscos faz parte da Etapa de Planejamento do Processo de gerenciamento de riscos (Luz, 2022).

O cerne da LGPD é o titular e o texto desta Lei enfatiza as operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais destes titulares, conforme o Art. 5º, inciso XVII, descrito a seguir:

[21] Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

[22] Titular: pessoa natural a quem os dados pessoais dizem respeito, que pode ser desde um cliente/consumidor, até um visitante, prestador de serviços, paciente, colaborador e dependentes (Luz, 2022).

> Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Brasil, 2018).

Conforme (Luz, 2022), a adequação à LGPD com influência de um processo robusto de gestão de risco ou até mesmo, apenas parte dele, pode representar significativo ganho para os agentes de tratamento[23], controlador e operador, previstos nesta Lei. Contudo, muito mais do que o simples cumprimento de uma imposição legal, é a oportunidade de Identificação de Riscos e dar soluções a tais vulnerabilidades.

1.1.3 Lei Geral de Proteção de Dados

O tema privacidade e proteção de dados começou a ser discutido no Brasil, em 2010, em um debate público, via internet. Já em junho de 2012, foi proposto pelo, na época deputado, o Sr. Milton Monti (PR-SP), o Projeto de Lei (PL) n.º 4.060/2012. Houve um segundo debate público em 2015, também pela internet, contando com mais de duas mil contribuições dos setores público e privado, academia e organizações não governamentais. Ainda em 2015, a Secretaria Nacional do Consumidor do Ministério da Justiça (SENACON), em conjunto com a Secretaria de Assuntos Legislativos (SAL), do mesmo Ministério, elaborou o Anteprojeto de Lei de Proteção de Dados Pessoais (Ministério da Justiça e Segurança Pública, 2015).

No Brasil, a pressão para a criação de uma legislação referente à proteção de dados aumentou após a entrada em vigor das novas regras estabelecidas pelo GDPR, em maio de 2018. Isto ocorreu devido às dificuldades do país em celebrar contratos e acordos e tratados bilaterais, por não possuir os requisitos que exigiam o consentimento dos usuários. Com isso, o Brasil não era reconhecido pela UE como um Estado com o qual poderia haver transações de transferências internacionais de dados pessoais (Sombra, 2018).

Cabe ressaltar que, embora o Brasil tenha tomado como base o arcabouço jurídico-regulatório da UE, isto não significou que outros países não tenham se precavido e criado outros arcabouços jurídicos-regulatórios de proteção e privacidade de dados. Atualmente, mais de 120 países possuem arcabouços regulatórios de proteção de dados pessoais (Dias, 2020). A LGPD acaba por complementar o marco regulatório brasileiro de aspectos relacionados ao tratamento

[23] Agente de tratamento: o controlador e o operador.

e proteção da informação, com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor (Klee; Pereira Neto, 2019).

Torna-se importante para uma empresa, pública ou privada, estar em *compliance* com o arcabouço jurídico-regulatório da LGPD, considerando diferentes condições de contorno, como, por exemplo: contexto da organização, cenário econômico, viabilidade de investimentos em tecnologia, treinamento, em suporte jurídico e aspectos relacionados à maturidade da organização.

Por mais que a LGPD ainda seja novidade para a grande maioria da população, o assunto, não é tão recente assim, conforme já foi mencionado. Já que o tema privacidade e proteção de dados vem sendo discutido há mais de dez anos. De lá para cá, muitos instrumentos foram publicados, cabendo citar:

a) Projeto de Lei n.º 4.060, de 13 de junho de 2012;
b) Projeto de Lei de Conversão n.º 53, de 14 de agosto de 2018;
c) Lei n.º 13.709 (LGPD), de 14 de agosto de 2018;
d) Medida Provisória n.º 869, de 28 de dezembro de 2018;
e) Projeto de Emenda Constitucional n.º 17, de 03 de julho de 2018;
f) Lei n.º 13.853, de 08 de julho de 2019;
g) Projeto de Lei n.º 1.179, de 13 de abril de 2020;
h) Medida Provisória n.º 959, de 29 de abril de 2020;
i) Lei n.º 14.010, de 10 de junho de 2020;
j) Projeto de Lei de Conversão n.º 34, de 26 de agosto de 2020;
k) Decreto n.º 10.474, de 26 de agosto de 2020;
l) Lei n.º 14.058, de 18 de setembro de 2020; e
m) Projeto de Lei de Conversão n.º 34/2020;
n) Emenda Constitucional 115/2022[24].

[24] Emenda Constitucional n.º 115, de 10 de fevereiro de 2022: Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A Lei n.º 13.709, de 14 de agosto de 2018, mais conhecida como LGPD, dispõe sobre o tratamento[25] de dados pessoais[26] e dados pessoais sensíveis[27], inclusive nos meios digitais[28], por pessoa natural[29], com fins comerciais, ou seja, a atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional; ou por pessoa jurídica de direito público, ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, e tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei n.º 13.853/2019 deu nova redação à Lei n.º 13.709/2018 e fez com que essa passasse a ser conhecida como a LGPD, e criou a ANPD (Brasil, 2018).

A aplicação da LGPD é fundamentada em seu Art. 3º, descrito, a seguir:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público, ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens, ou serviços, ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional. (Brasil, 2018).

O Art. 2º, da LGPD, apresenta os fundamentos da lei (Brasil, 2018), descritos, a seguir:

I. o respeito à privacidade;
II. a autodeterminação informativa;
III. a liberdade de expressão, de informação, de comunicação e de opinião;
IV. a inviolabilidade da intimidade, da honra e da imagem;

---

[25] Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).
[26] Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável (Brasil, 2018).
[27] Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018).
[28] A LGPD estende seu alcance não apenas aos ambientes digitais, mas também às esferas físicas. Esta abrangência é explicitamente delineada no Artigo 1º da referida lei, e reflete uma compreensão ampla sobre a natureza da proteção de dados, reconhecendo que a privacidade e a segurança das informações pessoais transcendem a barreira entre o digital e o físico.
[29] Pessoa natural: A existência da pessoa natural termina com a morte; presume-se esta, quanto aos ausentes, nos casos em que a lei autoriza a abertura de sucessão definitiva (Brasil, 2002).

V. o desenvolvimento econômico e tecnológico e a inovação;
VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

1.1.3.1 Boa-fé

Sobre a LGPD, além dos fundamentos, já citados, é importante observar a boa-fé, abordada a seguir, e os princípios desta Lei. Ambos previstos em seu Art. 6º.

Cabe aqui discorrer sobre o princípio da boa-fé, no *caput* do Art. 6º. Este é um dos princípios fundamentais do Direito Civil brasileiro, e é mencionado em diversos artigos e seu objetivo precípuo é ajustar um padrão ético de conduta para as partes interessadas, nas relações obrigacionais, e pode ser dividido em:

- **boa-fé subjetiva**: é relacionada com a intenção do sujeito de direito (Helton, 2019). Para fins meramente históricos, o Código Civil brasileiro, de 1916, se referia à boa-fé subjetiva, mediante cláusulas genéricas e imposições de parâmetros de conduta para as relações sociais, criando direitos e obrigações anexas àquelas existentes em relações contratuais, visando alcançar a mútua e leal cooperação entre as partes (Diniz, [s.d.]);
- **boa-fé objetiva**: pode ser entendida como um dos parâmetros-base para equilibrar a relação entre agentes de tratamento e titulares. No Código Civil, este princípio está presente no Art. 422, da seção I, do Capítulo: Disposições Gerais, sob o Título V - Dos Contratos em Geral: Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé (Brasil, 2002).

Esta percepção representa uma transformação substancial no âmbito do direito das obrigações. Sob a égide do regime jurídico antecedente, predominava exclusivamente a dimensão subjetiva da boa-fé. O reconhecimento atual de duas facetas tanto subjetivas quanto objetivas constitui, portanto, uma evolução significativa na compreensão e aplicação deste princípio jurídico fundamental.

Segundo Diniz (2012), a boa-fé objetiva, também conhecida como boa-fé contratual, foi desenvolvida pela doutrina e jurisprudência alemãs, por volta de 1896, com base no § 242 do BGB, onde se lê: “O devedor está adstrito a realizar a prestação tal como o exija a boa-fé, com consideração pelos costumes do tráfego”.

1.1.3.2 Dos requisitos para o tratamento de dados pessoais

Mesmo para alguns estudiosos do tema privacidade e proteção, com ênfase na LGPD, o termo tratamento acarreta um conceito genérico e, às vezes, até mesmo abstrato. À luz da LGPD, o termo tratamento prevê cerca de vinte operações e, é definido em seu Art. 5º, Inciso X:

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018);

O Governo Digital definiu, de forma clara, cada uma dessas operações, a fim de melhorar o entendimento dos conceitos envolvidos (Governo Digital, 2020).

É essencial reconhecer a necessidade de categorizar o tratamento de dados sob duas distintas vertentes, conforme estabelecido pela LGPD:

- o tratamento de dados pessoais; e
- o tratamento de dados pessoais sensíveis.

A LGPD, em sua estrutura normativa, contempla artigos específicos que delineiam as condições e diretrizes para o tratamento de ambas as categorias de dados. Neste contexto, é imperativo sublinhar que a obtenção de consentimento, não se configura como a única hipótese legal para o tratamento de dados conforme a LGPD. Existem, de fato, outras dez hipóteses legais previstas nesta Lei, demonstrando a complexidade e a abrangência do regime jurídico de proteção de dados no Brasil. Esta pluralidade de hipóteses legais para o tratamento de dados reflete a necessidade de um equilíbrio entre a proteção da privacidade dos titulares dos dados e a flexibilidade necessária para o tratamento de dados em diversos contextos socioeconômicos.

Conforme previsto no Art. 7º, da LGPD, o tratamento de dados pessoais somente poderá ser realizado nas hipóteses previstas neste artigo. Já o tratamento de dados pessoais sensíveis, somente poderá ser realizado, com base nas hipóteses de tratamento previstas no Art. 11. O § 1º deste artigo determina que se aplica o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica (Brasil, 2018).

A Tabela 1 – Hipóteses de tratamento de dados pessoais apresenta as hipóteses de tratamento desta Lei e os dispositivos legais previstos nos Arts. 7º (tratamento de dados pessoais) e 11 (tratamento de dados pessoais sensíveis) (Governo Digital, 2020).

Tabela 1 - Hipóteses de tratamento de dados pessoais e dados pessoais sensíveis

HIPÓTESES DE TRATAMENTO	DISPOSITIVOS LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS (Art. 7º)	DISPOSITIVOS LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS (Art. 11)
Hipótese 1: Mediante consentimento do titular	LGPD, Art. 7º, I	LGPD, Art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, Art. 7º, II	LGPD, Art. 11, II, “a”
Hipótese 3: Para a execução de políticas públicas	LGPD, Art. 7º, III	LGPD, Art. 11, II, “b”
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, Art. 7º, IV	LGPD, Art. 11, II, “c”
Hipótese 5: Para a execução ou preparação de contrato	LGPD, Art. 7º, V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, Art. 7º, VI	LGPD, Art. 11, II, “d”
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular, ou de terceiro	LGPD, Art. 7º, VII	LGPD, Art. 11, II, “e”
Hipótese 8: Para a tutela da saúde do titular	LGPD, Art. 7º, VIII	LGPD, Art. 11, II, “f”
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, Art. 7º, IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, Art. 7º, X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, Art. 11, II, “g”

Fonte: Governo Digital, 2020.

Convém que antes de um agente de tratamento iniciar qualquer operação de tratamento de dados pessoais, ele se certifique de que esta operação seja registrada, para fins de trilha de auditoria e prestação de contas. A compreensão das hipóteses previstas na LGPD e que possam

fundamentar as operações de tratamento é fundamental para a mitigação de riscos associados ao descumprimento da LGPD (Governo Digital, 2020).

Cabe ressaltar que o desconhecimento de determinada lei, ou conjunto delas, não é pressuposto para o seu não cumprimento. O Decreto-Lei n.º 2.848, de 7 de dezembro de 1940, mais conhecido como Código Penal, prevê em seu Art. 21 que o desconhecimento da lei é inescusável (Brasil, 1940). Já o Decreto-Lei n.º 4.657, de 4 de setembro de 1942, mais conhecido como Lei de Introdução as Normas do Direito Brasileiro, determina no seu Art. 3º que ninguém se escusa de cumprir a lei, alegando que não a conhece (Brasil, 1942). A exceção fica por conta do Decreto-Lei n.º 3.688, de 3 de outubro de 1941, mais conhecido com Lei das Contravenções Penais, que em seu Art. 8º determina que no caso de ignorância ou de errada compreensão da lei, quando escusáveis, a pena pode deixar de ser aplicada (Brasil, 1941).

Há um verbete, em Latim, "*Dura Lex Sed Lex*", que em tradução livre, pode ser entendido como A lei é dura, mas é a lei. Apesar de exigir sacrifícios, a lei deve ser cumprida (Vade Mecum Brasil, 2023).

A LGPD determina, em seu Art. 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. Ainda sobre o tratamento de dados pessoais de crianças e adolescente:

a) este deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, e os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei (Direito dos Titulares);
b) poderão ser coletados dados pessoais de crianças sem o consentimento a que se, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento;
c) os controladores não deverão condicionar a participação dos titulares em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade;
d) o controlador deve realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis;

e) as informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, para proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

A LGPD, em seu Artigo 14, estabelece diretrizes específicas para o consentimento no contexto do tratamento de dados pessoais. Esta forma de consentimento, conforme delineado pela LGPD, apresenta características distintas quando comparada aos consentimentos utilizados nos termos de consentimento livre e esclarecido, tradicionalmente empregados em outras áreas, conforme já abordado neste trabalho. Sendo assim, é crucial, portanto, reconhecer que, embora ambos os tipos de consentimento busquem a proteção e a autonomia do indivíduo, eles operam sob diferentes premissas e objetivos.

Prosseguindo na análise acerca das outras hipóteses de tratamento de dados pessoais previstas na LGPD, é imperioso reafirmar a interpretação de que não se estabelece uma hierarquia entre as diferentes hipóteses legais para o tratamento de dados pessoais. E, no que se refere ao tratamento de dados pessoais de crianças e adolescentes, torna-se relevante a consideração do Enunciado CD/ANPD n.º 1, datado de 22 de maio de 2023. Este enunciado esclarece que o tratamento de dados pessoais de crianças e adolescentes é viável sob as disposições legais estipuladas tanto no artigo 7º quanto no artigo 11 da LGPD. Contudo, é fundamental que tal tratamento seja efetuado com a preponderância do princípio do melhor interesse, conforme determina o artigo 14 da referida Lei (Autoridade Nacional De Proteção De Dados, 2023).

A análise da LGPD sugere a necessidade de uma adaptação ou harmonização dos termos de consentimento livre e esclarecido com as exigências específicas impostas pela legislação em matéria de dados pessoais. Essa adaptação é imperativa para assegurar a conformidade legal e ética, especialmente no que tange ao tratamento de informações em contextos que envolvem sujeitos de cuidado. Tal harmonização implicaria que em determinado termo de consentimento livre e esclarecido houvesse a adoção de uma das 11 hipóteses de tratamento de dados pessoais apresentadas na Tabela 1, não se restringindo apenas aos consentimentos previstos nos incisos I, dos Artigos 7º e 11 desta Lei.

1.1.3.3 Das Sanções Administrativas

A LGPD, em seu Art. 52, determina que os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos a sanções administrativas aplicáveis pela ANPD.

No contexto normativo imposto pela LGPD, em seu Artigo 52, observa-se uma distinção específica no que tange à aplicabilidade das sanções administrativas em relação ao Poder Público. Enquanto as multas simples e diárias estão explicitamente previstas como penalidades aplicáveis às pessoas jurídicas de direito privado e pessoas físicas que tratem dados pessoais com fins comerciais, as demais sanções delineadas no referido artigo recaem sobre todos os agentes de tratamento (Autoridade Nacional de Proteção de Dados; Ministério da Justiça e Segurança Pública, 2023).

As sanções poderão ser aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, conforme as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

a) a gravidade e a natureza das infrações e dos direitos pessoais afetados;
b) a boa-fé do infrator;
c) a vantagem auferida ou pretendida pelo infrator;
d) a condição econômica do infrator;
e) a reincidência;
f) o grau do dano;
g) a cooperação do infrator;
h) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
i) a adoção de política de boas práticas e governança;
j) a pronta adoção de medidas corretivas; e
k) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As sanções aplicáveis pela ANPD não substituem as aplicações de sanções administrativas, civis ou penais definidas na Lei n.º 8.078, de 11 de setembro de 1990, e em legislação específica (Brasil, 2018).

O Conselho Diretor da ANPD aprovou, em 24 de fevereiro de 2023, a Resolução CD/ANPD n.º 4, que aprova o Regulamento de Dosimetria[30] e Aplicação de Sanções Administrativas (Autoridade Nacional de Proteção de Dados; Ministério da Justiça e Segurança Pública, 2023).

Em 27 de fevereiro de 2023, a ANPD publicou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas por esta Autoridade, que também ficou conhecido como Norma de Dosimetria. Este Regulamento almeja a garantia da proporcionalidade entre a sanção aplicada e a gravidade da conduta do agente de tratamento, além de proporcionar segurança jurídica aos processos fiscalizatórios e a garantia do direito ao devido processo legal e ao contraditório (Autoridade Nacional de Proteção de Dados, 2023).

Os principais objetivos deste Regulamento são:

a. Regulamentar os artigos 52 e 53 da LGPD e definir os critérios e parâmetros para as sanções pecuniárias e não pecuniárias pela ANPD, bem como as formas e dosimetrias para o cálculo do valor-base das multas;
b. Alterar os artigos 32, 55 e 62 da Resolução n.º 1º CD/ANPD, com vistas a aprimorar o processo administrativo sancionador e de fiscalização, permitindo-se que a ANPD evolua na atividade repressiva, respeitados o devido processo legal e o contraditório, de modo a proporcionar segurança jurídica e transparência para todos os envolvidos.

1.1.4 Tratamento de Dados Pessoais na Saúde

Para estabelecermos uma conexão entre a LGPD e as relações médico-paciente, que têm suas raízes na tradição de Hipócrates[31], no Código de Nuremberg[32], no Termo de Consentimento Livre e Esclarecido (TCLE), e em outras regulamentações, será preciso explorar mais detalhadamente alguns desses tópicos nos parágrafos subsequentes.

[30] Dosimetria: é o método que orienta a escolha da sanção mais apropriada para cada caso concreto em que houver violação à LGPD e permite calcular, quando cabível, o valor da multa aplicável ao infrator (Autoridade Nacional de Proteção de Dados; Ministério da Justiça e Segurança Pública, 2023).
[31] Tradição de Hipócrates: se refere ao conjunto de princípios éticos e de conduta associados ao médico grego Hipócrates, que é frequentemente considerado o "pai da medicina ocidental". Hipócrates viveu por volta de 460 a.C. a 370 a.C. e fundou uma escola de medicina na Grécia antiga. Ele é conhecido por suas contribuições significativas para o campo da medicina e também por estabelecer um código de ética que influenciou profundamente a prática médica ao longo da história.
[32] Código de Nuremberg: também conhecido como Código de Nuremberga (em português europeu), é um conjunto de princípios éticos que estabelece as diretrizes para a pesquisa médica envolvendo seres humanos.

Quando a relação médico-paciente é estabelecida, este relacionamento é inspirado pela tradição de Hipócrates. Contudo, há outros influenciadores nesta relação, como o Código de Nuremberg, que teve origem no Tribunal Militar de Nuremberg (1945 a 1946), e que estabeleceu que um sujeito de cuidado falante, com autonomia para decisão do que é melhor para ele e agindo em consequência, tem a garantia de que seus melhores interesses serão garantidos. Os juízes de Nuremberg elaboraram um conjunto de dez princípios centrados nos sujeitos participantes de pesquisas, com destaque para o primeiro princípio, que diz que o consentimento voluntário do ser humano é absolutamente essencial (Ghool, 2011).

Os principais princípios do Código de Nuremberg incluem:

a) Consentimento voluntário e informado: Os participantes da pesquisa médica devem dar seu consentimento voluntário, livre e informado para participar, após serem devidamente informados sobre os objetivos, métodos e riscos da pesquisa;
b) Benefícios para a sociedade devem superar os riscos: A pesquisa médica deve ter um propósito valioso para a sociedade e os benefícios esperados devem superar qualquer risco potencial para os participantes;
c) Evitar danos: Os pesquisadores têm a obrigação de minimizar o risco de danos aos participantes da pesquisa e garantir que os procedimentos sejam realizados com segurança;
d) Escolha do participante: A seleção de participantes não deve ser arbitrária, e os grupos mais vulneráveis, como crianças e prisioneiros, devem receber proteções especiais; e
e) Liberdade de interrupção: Os participantes têm o direito de interromper sua participação na pesquisa a qualquer momento, sem penalidades.

O Código de Nuremberg desempenhou um papel crucial no desenvolvimento da ética na pesquisa médica e serviu de base para a criação de diretrizes éticas mais amplas, como a Declaração de Helsinque[33], que continua a guiar a pesquisa clínica em todo o mundo. Estas

[33] A Declaração de Helsinque, elaborada pela Associação Médica Mundial em 1964, constitui um marco na ética da pesquisa envolvendo seres humanos. Este documento seminal estabelece princípios éticos reconhecidos internacionalmente no campo da pesquisa biomédica. A premissa central da Declaração é que o bem-estar do ser humano deve prevalecer sobre os interesses da ciência e da sociedade, sublinhando a primazia da ética humanista na

diretrizes buscam garantir que a pesquisa médica seja conduzida com o máximo respeito pelos direitos e bem-estar dos participantes.

Na área da saúde, o Termo de Consentimento Informado Livre e Esclarecido (TCLE), amplamente utilizado nos comitês de ética, também é um documento amplamente utilizado na relação entre cuidador e sujeito de cuidado. Sendo assim, não necessariamente o TCLE[34], da área da saúde ou de outra base legal, estará automaticamente adequado à LGPD. Desta forma, normas constitucionais, codificadas, esparsas[35], ou consolidadas, que exijam um TCLE, que inclusive podem ser anteriores à LGPD, continuarão a ser atendidas. Contudo, pode ser necessário, além do TCLE, outro documento que respalde a evidência da hipótese de tratamento, à luz da LGPD, ou até mesmo um documento que combine o conteúdo de um TCLE com a ciência de uma hipótese de tratamento, prevista pela LGPD e adotada por determinado agente de tratamento (Sedlmaier; Hernandez, 2019).

O TCLE é definido por como:

> Documento de caráter explicativo, onde são abordadas todas as questões relativas ao estudo clínico que possam estar relacionadas à decisão do sujeito da pesquisa e, assim, garantir sua participação voluntária. A participação voluntária em estudos humanos é baseada no direito de ser informado de todos os aspectos do estudo, bem como ter respostas para questões em linguagem clara e de fácil entendimento (Souza *et al*., 2013).

O Código de Ética Médica vigente, Resolução CFM n.º 1.931, retificado em 13 de outubro de 2009, em seu Capítulo IV – Direitos humanos, é claro em vedar ao médico deixar de obter consentimento do paciente ou de seu representante legal após esclarecê-lo sobre o procedimento a ser realizado, salvo em caso de risco iminente de morte. No referido Código, em seu Art. 73, do Capítulo IX – Sigilo profissional, ele é explicito ao determinar que é vedado ao médico revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente. O termo sigilo é citado outras nove vezes, com destaque para o Art. 101, que informa que é vedado ao médico Deixar de obter do paciente ou de seu representante legal o termo de consentimento livre e esclarecido

pesquisa. Um dos pilares da Declaração é a ênfase na necessidade de consentimento livre e informado dos participantes da pesquisa, assegurando sua autonomia e proteção (Diniz; Corrêa, 2001).

[34] O TCLE também pode ter sinônimos, como, por exemplo, Termo de Consentimento Informado (TCI).

[35] Normas esparsas (ou extravagantes) são aquelas editadas de modo isolado, e que tratam de específica matéria jurídica, não estando, portanto, codificadas. Como exemplo, a Lei Ambiental (Lei n.º 9.605/98), cujo conteúdo abarca um amplo leque de normas jurídicas (de natureza penal, administrativa, civil etc.) relativas à preservação do meio ambiente (Friede, 2021).

para a realização de pesquisa envolvendo seres humanos, após as devidas explicações sobre a natureza e as consequências da pesquisa (Conselho Federal de Medicina, 2009).

É indiscutível que estas referências de consentimento supracitadas não estejam prevendo diálogo com os Arts. 7º ou 11, da LGPD, já que a Resolução CFM n.º 1.931 foi publicada em data que precede cronologicamente a LGPD, de 2018.

A Lei n.º 14.510, de 27 de dezembro de 2022, autoriza e disciplina a prática da telessaúde em todo o território nacional. O seu Art. 2º acrescentou à Lei n.º 8.080/90 o Art. 26-G que exige que a prática da telessaúde deve ser realizada por consentimento livre e esclarecido do paciente, ou de seu representante legal, e sob responsabilidade do profissional de saúde (Brasil, 2022).

O Decreto do CFM n.º 2.314, de 20 de abril de 2022, determina em seu Art. 15 que:

> O paciente ou seu representante legal deverá autorizar o atendimento por telemedicina e a transmissão das suas imagens e dados por meio de (termo de concordância e autorização) consentimento, livre e esclarecido, enviado por meios eletrônicos ou de gravação de leitura do texto com a concordância, devendo fazer parte do SRES do paciente (Conselho Federal de Medicina, 2022b).

Salienta-se a relevância de considerar que, embora os instrumentos mencionados estejam vinculados ao CFM, é necessário atentar para situações específicas relacionadas a outras disciplinas do campo da saúde, abarcando, mas não se limitando, a Nutrição, Enfermagem, Psicologia, Farmácia, Fisioterapia, Biologia e Biomedicina. Nesses contextos, é imprescindível observar os instrumentos éticos elaborados pelos respectivos Conselhos Federais de cada área profissional.

1.1.5 Privacidade de Dados Pessoais

Será que o homem comum tem ideia do que é privacidade? É importante a reflexão sobre a amplitude do conceito associado a esta palavra, como ela é definida, quais direitos estão associados e o que se pode esperar de todos os temas relacionados a ela. Contudo, de certa forma, na Sociedade, a privacidade acaba ficando esquecida, em meio a tantos assuntos relacionados à LGPD. Torna-se imprescindível que a privacidade dos Titulares de Dados Pessoais (DP) sejam sempre o elemento mais importante nos processos relacionados à LGPD, e até mesmo em arcabouços jurídicos-regulatórios equivalentes.

A privacidade é considerada, no Brasil e ao redor do mundo, como um direito fundamental, essencial à autonomia e proteção da dignidade humana, e a partir dela, muitos outros direitos foram, são e serão construídos. Uma das primeiras citações públicas sobre a definição de privacidade foi feita em 15 de dezembro de 1890, pelos advogados, Samuel Warren e Louis Brandeis, quando publicaram na Harvard Law Review, um artigo jurídico intitulado: "*The Right to Privacy*". Neste artigo, os autores discutem sobre o direito de ser deixado só e definem privacidade com esta mesma frase, ou seja, a definição de privacidade nesta época era: o direito de ser deixado sozinho (Warren; Brandeis, 1890). É relevante destacar um trecho deste artigo que não apenas reflete uma coincidência com o que vemos atualmente, mas também demonstra como cidadãos ainda buscam esse direito, com base em um conceito que tem mais de um século de existência:

> Invenções e métodos de negócios recentes chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para garantir ao indivíduo o que o Juiz Cooley chama de direito de "ser deixado em paz". Os recintos sagrados da vida privada e doméstica, e numerosos dispositivos mecânicos ameaçam confirmar a previsão de que "o que é sussurrado no armário será proclamado dos telhados". Durante anos, houve um sentimento de que a lei deveria fornecer algum remédio para a circulação não autorizada de retratos de pessoas privadas; e o mal da invasão de privacidade pelos jornais, há muito sentido, foi discutido recentemente por um hábil escritor. Os alegados fatos de um caso um tanto notório, levado a um tribunal inferior em Nova York há alguns meses, envolveu diretamente a consideração do direito de circular retratos; e a questão de saber se nossa lei reconhecerá e protegerá o direito à privacidade neste e em outros aspectos deve em breve ser levada aos nossos tribunais para consideração (Warren; Brandeis, 1890).

Warren e Brandeis descreveram originalmente o direito à privacidade ("*The Right to Privacy*") como um direito comum já existente que incorporava proteções para a "personalidade inviolável" de cada indivíduo. A legislação comum, dos EUA, garante, para cada indivíduo, o direito de determinar em que medida os pensamentos, sentimentos e emoções, dos cidadãos norte-americanos, podem ser divulgados a outras pessoas, fixando os limites da publicidade que pode ser dado a eles. Para Warren e Brandeis, o direito à privacidade, na época, significava que cada indivíduo tinha o direito de escolher compartilhar ou não com os outros, informações sobre sua "vida privada, hábitos, atos e relações" (Warren; Brandeis, 1890).

Tais autores argumentaram que era necessário o sistema legal norte-americano reconhecer o direito à privacidade, porque, **quando a informação sobre a vida privada de um indivíduo é disponibilizada para os outros, tende a influenciar e até mesmo ferir o próprio cerne da personalidade de um indivíduo – "sua avaliação de si mesmo".** O conceito original de Warren e Brandeis do direito à privacidade, portanto, incorporou um *insight* psicológico, que naquele tempo era relativamente inexplorado, ou seja, que:

> a personalidade de um indivíduo, especialmente a sua autoimagem, pode ser afetada e, às vezes, distorcida ou ferida, quando a informação sobre a vida privada desse indivíduo é tornada disponível para outras pessoas (Warren; Brandeis, 1890).

Em termos mais simples, para os referidos autores, o direito à privacidade era o direito de cada indivíduo de proteger a sua integridade psicológica, exercendo controle sobre as informações que refletiu e afetou a personalidade daquele indivíduo (Warren; Brandeis, 1890).

No conceito moderno e atual, podemos entender privacidade como direito fundamental, essencial para a autonomia e a proteção da dignidade humana, servindo como o fundamento sobre o qual muitos outros direitos humanos são construídos.

A privacidade é um direito humano fundamental e qualificado. O direito à privacidade está articulado em todos os principais instrumentos internacionais e regionais de direitos humanos, incluindo a Declaração dos Direitos Humanos das Nações Unidas (1948), que em seu 12º Artigo consagra o Direito à Privacidade como direito fundamental:

> Ninguém será sujeito a interferência arbitrária em sua privacidade, família, casa ou correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques (NAÇÕES UNIDAS, 1948).

Com a aceleração dos avanços tecnológicos, também evoluíram os marcos legais de proteção de dados. Em 1980, a Organização para Cooperação e Desenvolvimento Econômico emitiu diretrizes sobre proteção de dados em resposta direta ao aumento do uso e poder dos computadores para processar dados. Um ano depois, o Conselho da Europa adotou a Convenção de Proteção de Dados – Convenção 108 – que foi a primeira vez que o direito à privacidade foi consagrado na lei dos países europeus.

No final de 1983, o Tribunal Constitucional Federal da Alemanha chegou a uma decisão fundamental sobre o chamado julgamento do censo. O veredicto foi considerado um marco da proteção de dados, por moldar o direito à autodeterminação informativa, também conhecida como autodeterminação informacional. A decisão do Tribunal alemão continuaria a influenciar o aumento da proteção de dados nas próximas décadas (Organização Mundial da Saúde, 2021).

Em 1995, foi criada a Diretiva Europeia de Proteção de Dados 46/EC, refletindo os avanços tecnológicos e introduzindo novos termos, incluindo processamento, dado pessoal sensível, consentimento, dentre outros. Esta Diretiva deu ênfase ao crescente desequilíbrio de poder entre empresas privadas e cidadãos, esclarecendo que o direito à autodeterminação informativa é de fato universal (Organização Mundial da Saúde, 2021).

Em 2016, o GDPR foi aprovado pelo Parlamento Europeu após quatro anos de discussão. O GDPR serve como um modelo para várias leis de proteção de dados em todo o mundo. Em 2018, as Nações Unidas promulgaram os Princípios de Proteção de Dados Pessoais e Privacidade como a principal fonte para a proteção de dados pessoais por todas as instituições das Nações Unidas (Organização Mundial da Saúde, 2021).

Segundo as leis de proteção de dados em todo o mundo, em linhas gerais, dados pessoais significam qualquer informação relacionada a um indivíduo identificado ou identificável. Uma pessoa identificável é aquela que pode ser identificada, direta ou indiretamente – em particular, por referência a um número de identificação ou por um, ou mais fatores específicos de sua condição física, fisiológica, mental, econômica, cultural ou identidade (como sobrenome e nome, data de nascimento, dados biométricos, incluindo impressões digitais) (Organização Mundial da Saúde, 2021).

O rápido avanço das tecnologias no âmbito das comunicações, tornou o mundo muito mais conectado. Até pouco tempo atrás, conceitos como plataformas de mídia social, *smartphones*, dispositivos *wearable*s, também conhecidos como dispositivos vestíveis, inteligência artificial (AI), que pareciam distantes, passaram a guiar o mundo para metodologias mais eficazes para extração de benefícios, a partir da obtenção e processamento de DP. Na época que essas tecnologias e tendências surgiram não se considerava como elas deveriam ser reguladas. Consequentemente, poderes legislativos, judiciários e executivos, englobando autoridades regulatórias, esforçam-se diariamente para adaptar instrumentos normativos obsoletos para se adequarem a um mundo que segue a passos largos e mudança exponencial, para os quais estes simplesmente não foram projetados.

Desde o artigo de Warren e Brandeis (1890) para cá, o conceito de privacidade evoluiu significativamente. E, até mesmo, pode-se afirmar que o termo gera uma expectativa de que DP compartilhados em um local privado, não serão divulgados a terceiros ou não terão usos secundários. Infelizmente, na prática, a realidade não condiz com a expectativa.

Em linhas gerais, privacidade era definida como o direito de ser deixado em paz, direito de liberdade de interferência ou intrusão, ou seja, um direito de ter algum controle sobre como os seus DP são tratados (Warren e Brandeis, 1890). No conceito moderno e atual, entende-se privacidade como direito fundamental, essencial para a autonomia e a proteção da dignidade humana, servindo como o fundamento sobre o qual muitos outros direitos humanos são construídos. A privacidade nos permite criar barreiras de proteção e gerenciar limites que protegem o cidadão de interferências injustificadas em suas vidas. Sendo assim, a privacidade garante a oportunidade aos cidadãos de negociarem quem são e como querem interagir com o mundo real

ou virtual, ao seu redor. A privacidade ajuda a estabelecer limites, para que o cidadão possa determinar quem pode acessar seus corpos, lugares e coisas, bem como às suas comunicações (TIC) e informações (Privacy International, 2017).

Regulamentos e leis, como a LGPD, que protegem a privacidade, dão aos cidadãos a oportunidade de fazerem valer seus direitos em face a desequilíbrios desproporcionais de poderes significativos. Em outras palavras, a privacidade desempenha um papel fundamental na capacidade dos cidadãos de se protegerem a si e à sociedade em que vivem contra o uso indiscriminado e injustificado do poder, reduzindo o escopo do que pode ser conhecido e realizado em relação a eles. Isso se torna crucial ao proporcionar um espaço onde esses cidadãos podem se expressar sem julgamentos, cultivando pensamentos livres e promovendo a ausência de discriminação.

As pessoas, tecnicamente conhecidas como titulares[36] de DP, compartilham os seus dados por vários motivos, dentre os quais, cabe enumerar os seguintes:

a) para serem ativos em suas mídias sociais, divulgando, imagens, vídeos, textos, e locais que frequentam, seja no âmbito pessoal ou até mesmo profissional;
b) para obter assistência social, financiamentos ou cartões de crédito, há necessidade de divulgar seus nomes, endereços, CPF, histórico de empregos e salário;
c) para obter alívio, pessoas contam ao clero, médicos e advogados alguns dos detalhes mais íntimos de suas vidas; e
d) para permitir ou esperar que a vigilância mantenha a ordem social (por exemplo, quando se permite câmeras no saguão de um banco para dissuadir os criminosos).

Ao abordar temas relacionados à privacidade, como o desenvolvimento de um aplicativo, inclusive, torna-se necessário visitar os conceitos de *Privacy by Design* e *Privacy by Default*. O conceito de *Privacy by Design* foi desenvolvido na década de 90, por Ann Cavoukian, Ph.D., para abordar os efeitos sistêmicos e crescentes das tecnologias de informação e comunicação e sistemas de dados em redes. O conceito de *Privacy by Design* promove a visão de que o futuro da privacidade não pode ser assegurado apenas pela conformidade com as estruturas regulatórias; em vez disso, a garantia de privacidade deve, idealmente, tornar-se o padrão de uma organização, o seu modo de operação. (Cavoukian, 2009).

[36] Titular: Conforme o inciso V, do Art. 5 º, da LGPD, pode ser definido como pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

A privacidade desde a concepção se estende a uma "trilogia" de aplicativos abrangentes: sistemas de Tecnologia da Informação; práticas de negócios responsáveis; e projeto físico e infraestrutura de rede. Os princípios de *Privacy by Design* podem ser aplicados a todos os tipos de informações pessoais, mas devem ser aplicados com esforço especial a dados confidenciais, como informações médicas, consideradas dados pessoais sensíveis, à luz da LGPD, e dados financeiros. A força das medidas de privacidade tende a ser proporcional à sensibilidade dos dados (Cavoukian, 2009).

Segundo Ana Cavoukian, os objetivos do *Privacy by Design* podem ser alcançados praticando os seguintes sete Princípios Fundamentais:

a) Proativo e não reativo; Preventiva não Remediadora: A abordagem *Privacy by Design* é caracterizada por medidas proativas em vez de reativas. Ela antecipa e previne eventos invasivos de privacidade antes que eles aconteçam. A *Privacy by Design* não espera que os riscos à privacidade se materializem, nem oferece remédios para resolver as infrações à privacidade depois que elas ocorrem - visa impedir que ocorram. Resumindo, *Privacy by Design* vem antes do fato, não depois;
b) Privacidade como configuração padrão: A *Privacy by Design* visa fornecer o grau máximo de privacidade, garantindo que os dados pessoais sejam automaticamente protegidos em qualquer sistema de TI ou prática comercial. Se um indivíduo não fizer nada, sua privacidade ainda permanecerá intacta. Nenhuma ação é necessária por parte do indivíduo para proteger sua privacidade, ou seja, ela é incorporada ao sistema, por padrão;
c) Privacidade incorporada ao design: O conceito *Privacy by Design* está incorporado no design e na arquitetura dos sistemas de TI e nas práticas de negócios. Não é utilizado como um complemento, após o fato. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade;
d) Funcionalidade total: Soma positiva, não soma zero da *Privacy by Design*, sendo assim, tem em vista todos os interesses e objetivos legítimos de uma maneira "ganha-ganha" de soma positiva, não por meio de uma abordagem datada de soma zero, em que trocas desnecessárias. O *Privacy by Design* evita a pretensão de falsas dicotomias, como privacidade *versus* segurança, demonstrando que é possível ter os dois;

e) Segurança de ponta a ponta - ciclo de vida de proteção dos dados completo: A *Privacy by Design*, tendo sido incorporada ao sistema antes do primeiro elemento de informação ser coletado, estende-se com segurança por todo o ciclo de vida dos dados envolvidos, ou seja, fortes medidas de segurança são essenciais para a privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e destruídos também com segurança, no final do processo, em tempo hábil. Assim, o *Privacy by Design* garante o gerenciamento seguro do ciclo de vida completo das informações, de ponta a ponta;
f) Visibilidade e Transparência: A *Privacy by Design* visa garantir a todos os *stakeholders* que, seja qual for a prática comercial ou tecnologia envolvida, ela está de fato operando conforme as promessas e objetivos declarados, sujeito a verificação independente. Seus componentes e operações permanecem visíveis e transparentes, tanto para usuários quanto para provedores. Lembre-se, confie, mas verifique; e
g) Respeito pela privacidade do usuário: O titular deve ser o centro das atenções, ou seja, acima de tudo, a *Privacy by Design* exige que arquitetos e operadores mantenham os interesses do indivíduo em primeiro lugar, oferecendo medidas como fortes padrões de privacidade, aviso apropriado e capacitando opções fáceis de usar. Mantenha-o centrado no usuário.

Um dos motivos de os sete princípios do conceito *Privacy by Design* ser chamado de Princípios Fundamentais é que eles podem ser atualizados e personalizados de várias maneiras, a depender dos requisitos particulares de uma organização. Embora amplamente aceita como um divisor de águas para a proteção da privacidade, o conceito *Privacy by Design* também desenvolveu uma reputação de ser um desafio de implementar para as empresas. A realidade é muito diferente. O *Privacy by Design* foi adotado, com sucesso, por empresas em todo o mundo, em uma variedade de indústrias e mercados, incluindo telecomunicações e serviços de autenticação. Essas empresas, que operam em setores distintos da economia, têm uma coisa em comum: optaram por colocar a privacidade no centro do desenvolvimento de seus produtos e serviços e descobriram que isso lhes dá uma vantagem competitiva. (Cavoukian, 2020).

O termo *Privacy by Design* foi adotado na norma ISO 31700-1:2023 - *Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*. Esta norma estabelece requisitos de alto nível para privacidade por *design,* para proteger a privacidade durante todo o ciclo de vida de um produto de consumo, incluindo dados processados pelo consumidor (*International Organization for Standardization*, 2023).

A norma técnica ISO 31700 apresenta trinta requisitos para serem cumpridos por organizações que queiram estar em conformidade com esta norma. De maneira geral, ela inclui orientações gerais sobre como projetar recursos para permitir que os consumidores façam valer seus direitos de privacidade, atribuindo funções e autoridades relevantes, fornecendo informações de privacidade aos consumidores, conduzindo avaliações de risco de privacidade, estabelecendo e documentando requisitos para controles de privacidade, como projetar controles de privacidade, gerenciamento de dados do ciclo de vida, e preparando e gerenciando uma violação de dados. Segundo Ann Cavoukian compartilhou:

> A incorporação deste conceito pela ISO dá vida à operacionalização dessa ideia, auxiliando as organizações a entenderem como efetivamente implementá-lo. O projeto desta norma foi elaborado visando sua aplicação por uma ampla variedade de empresas, incluindo *startups*, empresas multinacionais, organizações de todos os tamanhos. Com qualquer produto, você pode fazer esse padrão funcionar porque é fácil de adotar. Esperamos que a privacidade seja incorporada proativamente no *design* das operações de uma organização e complemente as leis de proteção de dados (Solomon, 2023).

A norma técnica ABNT NBR ISO/IEC 29100:2020 – Estrutura de Privacidade fornece uma estrutura de alto nível para a proteção de dados pessoais dentro de sistemas de tecnologia da informação e de comunicação (TIC). Ela é geral em sua natureza e coloca os aspectos organizacionais, técnicos e processuais em uma estrutura abrangente de privacidade.

Segundo a ABNT, esta Norma fornece uma estrutura de privacidade que:

a) especifica uma terminologia comum de privacidade;
b) especifica os atores e os seus papéis no tratamento de dados pessoais;
c) descreve considerações de salvaguarda de privacidade; e
d) fornece referências para princípios conhecidos de privacidade para tecnologia da informação (Associação Brasileira de Normas Técnicas, 2020a).

1.1.6 Inteligência Artificial: Lógica Fuzzy

De acordo com Charles Elkan, a Lógica Fuzzy representa uma extensão e aprimoramento da lógica clássica. Esta última baseia-se na atribuição de graus de verdade de 0 ou 1 a conceitos, resultando em um comportamento binário. Em outras palavras, a lógica clássica é aplicável somente a conceitos que podem ser categorizados como:

- Completamente verdadeiros: com grau de verdade igual a 1; ou
- Completamente falsos: com grau de verdade igual a 0.

Essa característica distintiva da lógica clássica, enquanto estrutura simplificada e limitante, contrasta com as propriedades mais flexíveis e graduais da Lógica Fuzzy, que permite a representação de conceitos com uma ampla gama de graus de verdade, fornecendo assim uma abordagem mais rica e aberta para a modelagem e resolução de problemas complexos. Neste contexto, a Lógica Fuzzy desempenha um papel fundamental na expansão do escopo da lógica e na capacidade de representar a incerteza e a imprecisão inerentes a muitos sistemas do mundo real. Portanto, a Lógica Fuzzy representa uma área de estudo de grande relevância e potencial para a pesquisa acadêmica, já que é aplicada em diversos campos, incluindo a tomada de decisões, a inteligência artificial e a teoria de sistemas.

A Lógica Fuzzy deve ser usada para adicionar incerteza no processo de inferência, permitindo processamento sobre conceitos inerentemente vagos. É importante destacar que as aplicações úteis, com emprego da Lógica Fuzzy, em geral, não estão na IA de alto nível, mas sim no controle de máquina de nível inferior, especialmente em produtos de consumo. Normalmente, controladores difusos são implementados como *software* rodando em microprocessadores padrões (Scientific American, 1999). A Lógica Fuzzy foi formulada por Lotfi Askar-Zadeh, com a proposta da teoria de conjuntos difusos, em 1965 (Zadeh, 1965).

Uma definição da Lógica Fuzzy é a fornecida por Shlomo Zilberstein, que define esta lógica como sendo uma técnica para representar e manipular informações incertas. Na lógica proposicional binária, mais tradicional, cada fato ou proposição, deve ser verdadeiro ou falso, ela também amplamente conhecida como booleana. Ainda assim, muitas das informações que as pessoas usam sobre o mundo envolve algum grau de incerteza. Como a teoria da probabilidade, a Lógica Fuzzy atribui valores numéricos entre 0 e 1, a cada proposição para representar

a incerteza. No entanto, enquanto a Teoria da Probabilidade mede a probabilidade de a proposição estar correta, a Lógica Fuzzy mede o grau de certeza sobre uma proposição (Scientific American, 1999).

No âmbito desta dissertação de mestrado, propomo-nos a investigar e esclarecer os conceitos fundamentais subjacentes à Lógica Fuzzy, bem como suas implicações e contribuições em diversas áreas do conhecimento. Numerosas interpretações equivocadas cercam a compreensão da Lógica Fuzzy. Como marco inicial, é imperativo elucidar que a Lógica Fuzzy não é envolta em ambiguidade ou obscuridade, ao contrário da percepção comumente difundida, ou seja, a Lógica Fuzzy não é nebulosa. Em contraste, a Lógica Fuzzy é precisa, embora ela trabalhe com a insegurança e a incerteza. Nesse sentido, pode-se considerar a Lógica Fuzzy como uma lógica precisa de imprecisão. Mais concretamente, a Lógica Fuzzy é um sistema de raciocínio e computação no qual os objetos de raciocínio e computação são classes com limites não precisos. Fundamentalmente, a imprecisão dos limites de classe pode ser equiparada à imprecisão (Zadeh, 2010).

A incorporação da Lógica Fuzzy na Gestão de Riscos de privacidade proporciona uma transição do modelo binário, caracterizado por extremos discretos, para um método que contempla um espectro contínuo de possibilidades. Divergindo da rigidez do binário, que se limita, por exemplo, a 'sim' ou 'não', a Lógica Fuzzy introduz uma gama de estados intermediários que refletem com maior fidelidade as complexidades e nuances do mundo real, frequentemente permeado por áreas cinzentas em vez de limites claramente definidos. Entre as vantagens mais notáveis da Lógica Fuzzy, destacam-se:

a) Modelagem de Incertezas: Capacita o tratamento de imprecisões e ambiguidades, as quais são aspectos comuns e desafiadores em numerosas questões práticas;
b) Flexibilidade: Mostra-se versátil, adaptando-se com eficácia a uma variedade de contextos e desafios distintos;
c) Tomada de Decisão: Aprimora o processo decisório em situações de incerteza, emulando a complexidade do raciocínio humano;
d) Ampla Aplicabilidade: Sua aplicabilidade estende-se por um vasto leque de áreas, abrangendo desde a gestão de processos até o desenvolvimento de sistemas de recomendação;
e) Intuitividade: A Lógica Fuzzy alinha-se de forma intuitiva com as estratégias cognitivas humanas, que descrevem e interpretam o mundo por meio de um prisma não binário.

Com a adoção da Lógica Fuzzy na Gestão de Riscos, é possível obter uma visão mais ampla e precisa dos riscos associados ao tratamento de dados pessoais e dados pessoais sensíveis de um determinado projeto, produto ou processo, permitindo que sejam tomadas decisões mais embasadas.

A complexidade do ambiente de dados, com destaque para os pessoais, contemporâneo, marcado por nuances e incertezas, requer uma abordagem sofisticada de Gestão de Riscos que vá além do binário e abarque a gama completa de possibilidades que a realidade apresenta. É neste contexto que a Lógica Fuzzy se apresenta como uma solução promissora, proporcionando uma ferramenta intuitiva e flexível para aprimorar o processo de tomada de decisão em relação à privacidade e proteção de dados.

Em outras palavras, a Lógica Fuzzy pode ser considerada como uma técnica matemática que lida com a incerteza e a imprecisão na tomada de decisão. E permite que sejam atribuídos graus de pertinência ou probabilidade a um determinado conceito ou ideia, em vez de simplesmente classificá-lo como verdadeiro ou falso. Na Gestão de Riscos, a Lógica Fuzzy pode ser utilizada para lidar com a incerteza e a imprecisão associadas a eventos de risco. Ela permite que sejam considerados diferentes graus de risco e incerteza, levando em conta não apenas a probabilidade de um evento ocorrer, mas também sua gravidade e impacto potencial. Por exemplo, em vez de simplesmente classificar um determinado risco como “alto” ou “baixo”, esta lógica pode ser utilizada para atribuir um grau de pertinência a esse risco, considerando, fatores como: a probabilidade de ocorrência, o impacto potencial, a experiência de especialistas e a capacidade de mitigação (Liao; Ma; Zhang, 2006).

A Lógica Fuzzy é uma maneira de modelar o raciocínio lógico em que a verdade de uma afirmação não é binária, como o que acontece com a lógica clássica, mas sim, multivalorada, indicando grau de verdade que varia de zero (0), que é absolutamente falso, a um (1), que é absolutamente verdadeiro. Este grau de verdade é apresentado a seguir, na Figura 3.

Figura 3 - Grau de Verdade na Lógica Fuzzy

Fonte: O autor, 2023.

A Lógica Fuzzy permite projetar um Sistema de Inferência Fuzzy, que é uma função que mapeia um conjunto de entradas, transformando-os em saída, usando regras interpretáveis, por humanos, ao invés do emprego de matemática mais abstrata. Esses tipos de funções são populares para aplicações de controle, onde uma referência e medições são alimentadas e, em seguida, usando um conjunto de regras baseadas, a luz da Lógica Fuzzy, uma saída é produzida. Mas, a Lógica Fuzzy é muito mais do que simplesmente uma técnica de controle, pois pode ser usada para qualquer processo de tomada de decisão (Zadeh, 1988).

Um Sistema de Inferência Fuzzy é uma forma de inteligência artificial que imita a maneira como os humanos abordam a resolução de problemas. Em outras palavras, a Lógica Fuzzy é o modo de codificar um conhecimento baseado na experiência de declarações vagas, de maneira que os computadores possam entender, ou seja, na forma de regras lógicas. Em um modelo simplificado, as regras desenvolvidas ao longo do tempo, são fundamentadas na experiência de um especialista, e às vezes, nos dados, são codificadas para alimentar o Sistema de Inferência Fuzzy. Desta forma, a codificação do conhecimento é o que dará suporte para a predição de um processo de tomada de decisão, que pode incluir processos de Identificação de Riscos, por exemplo (Zadeh, 1965b).

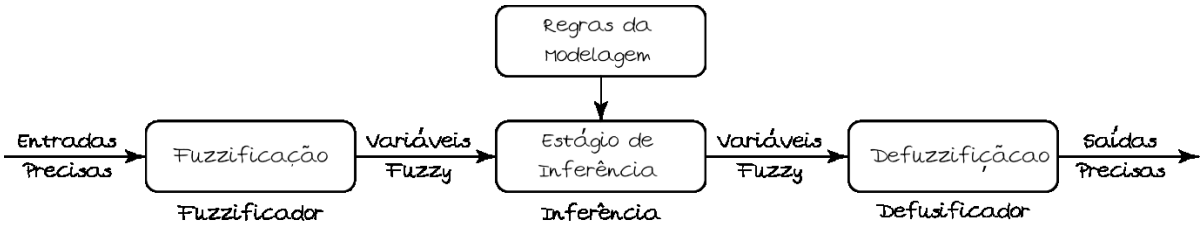
No Sistema de Inferência Fuzzy inicia-se tomando as Entradas Precisas (*Crisp inputs*), resultados de medições ou observações sobre as variáveis, ou características do problema, e inferindo esses valores nos Conjuntos Fuzzy de Entrada, processo realizado no estágio de Fuzzificação, que dá origem às Variáveis Fuzzy, correspondentes a estes conjuntos. No referido estágio, ocorre a ativação das Regras[37] fornecidas por um ou mais especialistas, ou extraídas de dados numéricos (Tanscheit, 2001).

[37] Regras: são fornecidas por especialistas ou extraídas de dados numéricos (Tanscheit, 2001).

No estágio seguinte, chamado de Estágio de Inferência[38], são obtidos os Conjuntos Fuzzy de Saída por meio da aplicação das funções de implicação (regras da modelagem). Assim, nesse estágio (Inferência) as operações com Conjuntos Fuzzy de Entrada, a partir da combinação dos antecedentes das regras, implicação e regra de inferência composicional, geram o Conjunto Fuzzy de Saída (Tanscheit, 2001b).

Em seguida, no último estágio, é realizada a interpretação do Conjunto Fuzzy de Saída, na etapa conhecida como Defuzzificação, dando origem às Saídas Precisas (*Crisp outputs*) (Tanscheit, 2001c), conforme diagrama de blocos da Figura 4 – Sistema de Inferência Fuzzy[39].

Figura 4 - Sistema de Inferência Fuzzy



Fonte: O autor, 2023.

A Lógica Fuzzy emerge como uma ferramenta de grande relevância na modelagem de sistemas de decisão complexos que frequentemente desafiam as abordagens tradicionais de modelagem. Essa técnica se destaca na capacidade de representar de forma eficaz sistemas cujas características são de difícil descrição por meio de outras metodologias de modelagem, mas que podem ser adequadamente traduzidas por meio de sistemas baseados em regras.

[38] Inferência: mapeia conjuntos Fuzzy e determina como as regras são ativadas e combinadas (Tanscheit, 2001).
[39] Sistema de Inferência Fuzzy: este termo, teve origem na língua inglesa, Fuzzy Inference System (FIS).

1.1.6.1 *Conjuntos Fuzzy*

O ponto de partida da Lógica Fuzzy é o conceito de um Conjunto Fuzzy. Um conjunto nebuloso A, em um espaço U, U={u}, é uma classe de elementos de U que possui limites não precisos. Uma classe com limites não precisos é definida por meio da associação com uma função de pertinência. A função de pertinência associa a cada elemento u, de U, seu grau de pertinência em A. Normalmente, os graus de pertinência são números no intervalo da unidade (Zadeh, 2010).

Segundo Tanscheit, 2001d), Zadeh propôs uma abordagem mais abrangente, ampliando a função característica de modo a permitir um número infinito de valores no intervalo entre 0 e 1. Dessa forma, um Conjunto Fuzzy A em um universo X é definido por uma função de pertinência $\mu_A(x)$: $X \rightarrow [0,1]$, e é representado por um conjunto de pares ordenados $A = \{\mu_A(x)/x\}$, no qual $x \in X$, onde:

a) *A*: Conjunto Fuzzy A;
b) *X*: é o universo de discurso;
c) $\mu_A(x)$: indica o quanto x é compatível com o conjunto A. Um determinado elemento pode pertencer a mais de um Conjunto Fuzzy, com diferentes graus de pertinência.

Os Conjuntos Fuzzy podem ser definidos, segundo (Tanscheit, 2001e), em:

a) Universo X discreto e finito: neste caso, o conjunto Fuzzy A é geralmente expresso por um vetor contendo graus de pertinência no conjunto A dos elementos correspondentes de X, através da seguinte notação: $\sum_{i=1}^{n} \mu A(xi)/xi$;
b) Universo X contínuo: emprega-se o símbolo de integral: $\int_x \mu A(x)/x$.

1.1.6.2 Regras da Modelagem

As regras, em geral, são fornecidas por um ou mais especialistas, através de sentenças linguísticas ou extraídas de dados numéricos. O bom desempenho de um Sistema Fuzzy está diretamente relacionado às regras que definem a estratégia de inferência. Caso estas não sejam consistentes, o Sistema Fuzzy terá um baixo desempenho (Tanscheit, 2001f).

1.1.6.3 Estágio de Inferência

O estágio de inferência é a etapa na qual, de fato, ocorrem as operações com conjuntos Fuzzy, com destaque para: combinação dos antecedentes das regras, implicação e *modus ponens*[40] generalizado. A definição dos Conjuntos Fuzzy que correspondem às variáveis de entrada e as de saída é um aspecto relevante, já que o desempenho do sistema de inferência dependerá do número de conjuntos e de suas formas (Tanscheit, 2001g).

1.1.6.4 Variáveis Linguísticas

Variável linguística é uma variável cujos valores são nomes de Conjuntos Fuzzy, por exemplo, uma variável linguística pode assumir valores como: *baixa, média e alta*. Segundo Klir e Yuan (1995), os valores de uma variável linguística também podem ser sentenças em uma linguagem especificada, a partir de:

a) Termos primários: *alto, baixo, pequeno, médio, grande, zero;*
b) Conectivos lógicos: *negação, não, conectivos e/ou;*
c) Modificadores: *muito, pouco, levemente, extremamente;*
d) Delimitadores: *como parênteses*.

Conforme Kosko (1996), as variáveis linguísticas têm como principal função oferecer uma maneira sistemática de caracterizar, de forma aproximada, fenômenos complexos ou mal definidos. Em outras palavras, utilizar descrições linguísticas em detrimento a variáveis quantificáveis permite tratar sistemas muito complexos, a fim de que sejam analisados por meio de termos matemáticos convencionais, utilizando a mesma abordagem que os seres humanos empregam.

[40] *Modus ponens*: é um termo em lógica que descreve uma forma válida de argumentação ou inferência. É uma regra de inferência que segue o seguinte padrão: se A, então B. A é verdadeira.

Uma variável linguística é definida formalmente por cinco elementos (N, T(N), X, G, M), a saber:

a) N: nome da variável;
b) T(N): conjunto de termos de N, ou seja, o conjunto de nomes dos valores linguísticos de N;
c) X: universo de discurso;
d) G: regra sintática[41] para gerar os valores de N como uma composição de termos de T(N), conectivos lógicos, modificadores e delimitadores;
e) M: regra semântica, para associar a cada valor gerado por G um Conjunto Fuzzy em X.

Uma variável linguística ou Fuzzy é definida por Marro *et al*. (2000) como entidade utilizada para representar de modo impreciso, ou seja, linguístico, um conceito ou uma varável de um determinado problema.

De acordo com Guillaume (2001), uma variável linguística, ao contrário de uma variável numérica, somente admite valores definidos na Linguagem Fuzzy que está utilizando-se dela.

1.1.6.5 Funções de Pertinência

Dubois e Prade (1980) apontam que as funções de pertinência podem ter diferentes formas, dependendo do conceito que se deseja representar e do contexto em que serão utilizadas. As funções de pertinência podem ser criadas a partir da experiência e perspectiva do usuário. É comum que a representação gráfica destas funções de pertinência, por padrão, seja de forma triangular, trapezoidal, gaussiana, sigmoide ou Pi. Em aplicações práticas, as formas escolhidas inicialmente podem ser ajustadas conforme os resultados observados.

[41] Regra sintática: especifica o conjunto de caracteres que constituem o alfabeto da linguagem e a maneira como os caracteres podem ser combinados para formar palavras válidas. Ou seja, especifica as sequências de símbolos que constituem estruturas sintáticas válidas, e são verificadas através de uma varredura (*parsing*) da representação interna do programa fonte. Estas regras permitem, por exemplo, o reconhecimento de expressões e comandos (Fernandes, [s.d.]).

Funções de pertinência descontínuas são compostas de segmentos contínuos lineares, resultando em formas triangulares ou trapezoidais. Funções de pertinência discretizadas consistem em conjuntos de valores discretos correspondendo a elementos discretos do universo (Cox, 1992).

1.1.6.6 Modelo de Inferência de Mamdani

O Modelo de Inferência de Mamdani é um tipo de Sistema de Inferência Fuzzy que usa regras linguísticas para transformar entradas imprecisas em saídas precisas. Ele foi proposto pelo pesquisador Lotfi Zadeh, em 1975.

Segundo Silva (2011) o Modelo de Inferência de Mamdani é composto por três componentes principais:

a) **a base de regras**: é uma coleção de regras linguísticas que relacionam as entradas às saídas. Cada regra é composta por duas partes: a antecedente, que especifica as condições para ativar a regra, e o consequente, que especifica a ação a ser tomada quando a regra é ativada. A base de regras é geralmente construída a partir do conhecimento de especialistas em um determinado domínio;
b) **o mecanismo de inferência**: usa as regras da base de regras para gerar uma saída a partir das entradas. Para fazer isso, ele usa uma técnica chamada Lógica Fuzzy, que permite que as entradas e as saídas sejam valores contínuos em um intervalo. A Lógica Fuzzy é baseada em funções de pertinência, que são curvas que associam um valor de entrada com um grau de pertinência a um Conjunto Fuzzy;
c) **a interface de saída**: é responsável por converter as saídas geradas pelo mecanismo de inferência em valores precisos que possam ser usados pelo sistema de controle. Isso é feito usando uma técnica chamada defuzzificação, que usa o princípio da centróide para calcular o valor final da saída.

Ainda de acordo com Silva (2011), a modelagem de Sistemas com Lógica Fuzzy, cumpre as seguintes etapas:

a) **Conjuntos Fuzzy**: permitem a manipulação de conceitos vagos e a modelagem de fenômenos não lineares. Estes conjuntos são definidos por funções de pertinência que atribuem a cada elemento um grau de verdade, possibilitando uma transição gradual entre a total pertinência e a total não pertinência;
b) **Variáveis Linguísticas**: servem como ponte entre termos linguísticos e números reais. Estes termos, como "baixo", "médio", e "alto", são utilizados para categorizar e quantificar as características do sistema em estudo, refletindo como humanos expressam e interpretam informações. As variáveis linguísticas podem ser divididas em:
    a. Variáveis de entrada (antecedentes);
    b. Variável de saída (consequente).
c) **Funções de Pertinência (*Membership*)**: quantificam o grau com que as entradas e as saídas pertencem a um Conjunto Fuzzy. A seleção da forma dessas funções (seja triangular, trapezoidal, gaussiana, sigmodal ou Pi) é fundamental e depende das características específicas do sistema modelado e do tipo de resposta esperada;
d) **Modelo de Mamdani**:
    a. Base de Regras: contém um conjunto de proposições condicionais do tipo "SE-ENTÃO" que mapeiam as relações entre as variáveis de entrada e saída;
    b. Mecanismo de Inferência: aplica às entradas Fuzzy as regras para gerar uma saída Fuzzy;
    c. Interface de Saída (defuzzificação): converte a saída Fuzzy em um número real, utilizando métodos como o da centróide, que calcula o centro de massa da área sob a curva da saída Fuzzy.

1.2 Trabalhos correlatos

Os trabalhos correlatos apresentados nesta subseção, reiteram que a Lógica Fuzzy é uma ferramenta matemática reconhecida por sua capacidade em modelar e gerar resultados sobre incerteza e imprecisão, e emerge como uma contribuição significativa no campo da Gestão de Riscos. A crescente complexidade dos ambientes organizacionais e as exigências de arcabouços

técnico-regulatório exigem abordagens inovadoras na avaliação e mitigação de riscos. Nesse contexto, a Lógica Fuzzy oferece uma perspectiva promissora, pois permite lidar com a ambiguidade e a imprecisão inerentes aos dados de risco.

As aplicações da Lógica Fuzzy na Avaliação de Riscos abrangem diversos domínios, incluindo a Avaliação de Riscos de privacidade e proteção de dados pessoais, liberação dinâmica de dados, cibersegurança, em diversas áreas, incluindo a Saúde e a Saúde Digital. Esses métodos fornecem uma estrutura flexível e adaptável para identificar, avaliar e priorizar riscos, permitindo tomadas de decisões fundamentadas em estratégias de mitigação de riscos.

Uma das principais vantagens da Lógica Fuzzy reside na sua capacidade de lidar com dados imprecisos e incertos, preenchendo uma lacuna deixada por abordagens tradicionais que requerem dados precisos. Além disso, a Lógica Fuzzy possibilita a modelagem e análise de relacionamentos complexos entre variáveis, aspecto crucial em ambientes de alta incerteza e interconexão.

Ao fornecer uma estrutura para a tomada de decisões mais informadas sobre estratégias de mitigação de riscos, a Lógica Fuzzy pode contribuir para a redução da probabilidade de resultados adversos e para a promoção da resiliência organizacional diante de cenários desafiadores.

Assim, a aplicação da Lógica Fuzzy na Gestão de Riscos emerge como um campo promissor de investigação, oferecendo percepções valiosas para aprimorar a compreensão e a Gestão de Riscos em ambientes complexos e dinâmicos.

Pontos de concordância entre os autores dos trabalhos correlatos:

a) Métodos tradicionais de tomada de decisão são aprimorados quando convertidos para operações que utilizam Lógica Fuzzy;
b) Abordagem sistemática e integrada para a Avaliação de Riscos leva ao uso de métodos sistemáticos de tomada de decisão em grupo;
c) A Lógica Fuzzy é aceita como uma teoria governante sobre a estrutura sistemática.

Não foram observados pontos discordantes entre os autores.

1.2.1 Modelo de Avaliação de Riscos de Segurança e Privacidade (SGD)

Embora este Modelo de Avaliação de Riscos de Segurança e Privacidade não adote a Lógica Fuzzy, que constitui um dos fundamentos desta dissertação, já que adota a Probabilidade, ao contrário dos demais trabalhos correlatos, ele abrange três das cinco áreas-chave. Além disso, este modelo é amplamente difundido para auxiliar empresas públicas ou privadas e profissionais a realizarem Gestão de Riscos como parte das exigências relacionadas à LGPD.

Sendo assim, na presente dissertação, o modelo proposto é comparado com o Modelo de Avaliação de Riscos de Segurança e Privacidade estabelecido pela Secretaria de Governo Digital (SGD), vinculada à Secretaria Especial de Desburocratização, Gestão e Governo Digital, do Ministério da Economia. Essa abordagem é essencial para estabelecer uma base sólida de comparação, permitindo uma análise aprofundada das considerações e métodos adotados.

1.2.1.1 Dimensões do Modelo da SGD

De acordo com Ministério da Economia (2020), no que se refere ao modelo da SGD, foram agrupados controles, em três contextos distintos, denominados, dimensões, descritos a seguir:

a) **Dimensão Estrutura:** Composta por trinta e seis (36) controles, essa dimensão aborda aspectos estruturais do sistema, englobando processos e infraestrutura. As características ambientais analisadas nesta dimensão são essenciais para uma avaliação abrangente, sendo indispensáveis para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais;
b) **Dimensão Sistema:** Contando com trinta e nove (39) controles, esta dimensão está fundamentada no conceito de *Security-by-Design*[42]. Os controles propostos buscam incorporar a segurança da informação ao longo de todo o ciclo de vida do sistema, contribuindo assim para a redução da superfície de ataque a vulnerabilidades do

[42] *Security-by-Design*: é uma abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas. Isso inclui a incorporação de especificações de segurança no projeto, avaliação de segurança contínua em cada fase e adesão às melhores práticas (Secretaria do Governo Digital, 2020).

sistema. Esta dimensão engloba temas como desenvolvimento seguro, controles de acesso lógico, segurança web, entre outros; e

c) **Dimensão Privacidade:** Composta por trinta e oito (38) controles, esta dimensão está diretamente relacionada à conformidade legal no tratamento de dados pessoais. Os controles possibilitam que o controlador avalie o sistema responsável pelo tratamento de dados pessoais, verificando se os requisitos de adequação à privacidade estão sendo atendidos.

É importante destacar que a organização por dimensão não implica em vinculação exclusiva das medidas de segurança da informação e privacidade a uma dimensão específica. Essa abordagem permite uma análise mais holística, considerando múltiplos aspectos para garantir uma avaliação abrangente e eficaz do modelo proposto (Ministério da Economia, 2020).

Nesse contexto, é relevante salientar que o foco central desta dissertação repousa sobre a preservação da privacidade, embora haja algumas considerações pertinentes à infraestrutura. No entanto, é imperativo destacar que todas essas ponderações estão incontestavelmente vinculadas à observância rigorosa das normativas estabelecidas pela LGPD.

1.2.1.2 Medidas de Segurança e Privacidade

A presente seção apresenta as medidas de segurança e privacidade, bem como os objetivos dos controles nelas presentes. No total, são adotadas vinte e três (23) medidas, divididas em segurança da informação, com doze (12), e privacidade, com as demais. As medidas adotadas tiveram como base as normas ABNT NBR ISO/IEC 27002:2013, que estabelece o escopo para segurança da informação, e a ISO/IEC 29100:2011, que delimita o escopo para privacidade (Ministério da Economia, 2020).

Ao seguir tais normas, a SGD buscou assegurar que as medidas propostas estivessem alinhadas com padrões reconhecidos internacionalmente, reforçando a eficácia e a relevância do sistema em termos de segurança e privacidade. Essa abordagem normativa proporcionou uma base sólida e consagrada para a avaliação, garantindo a conformidade e a aderência a padrões reconhecidos pela comunidade global de segurança da informação e privacidade.

1.2.1.3 Riscos

Os riscos considerados no modelo da SGD foram fundamentados na norma técnica ISO/IEC 29134:2017. A SGD adotou quatorze riscos para avaliação.

1.2.1.4 Avaliação dos Riscos

A matriz de riscos, também conhecida como mapa de calor ou matriz de probabilidade/ consequência, foi a maneira pela qual a SGD exibiu os níveis de risco para o seu Modelo.

Para o suporte a esta matriz, o Modelo adotou parâmetros escalares com valor gradual para as classificações consideradas: Baixo, Moderado e Alto. Com base nestes parâmetros escalares, o Modelo apresentou a matriz de calor, que relacionou a probabilidade com o impacto. A magnitude de um risco, para este modelo, pode ser considerada como a multiplicação da probabilidade pelo impacto (Ministério da Economia, 2020).

Tradicionalmente, a Gestão de Riscos de segurança da informação e as avaliações correlatas têm se concentrado predominantemente no risco para a organização, utilizando frequentemente a fórmula amplamente aceita de risco = impacto x probabilidade.

A norma citada pela SGD para as definições dos termos probabilidade e impacto foi a norma ISO/IEC 31000:2009.

Segundo o Ministério da Economia (2020), diante da crescente importância da privacidade dos dados pessoais e dados pessoais sensíveis, torna-se imperativo considerar a necessidade de adaptar os modelos de Gestão de Riscos, incorporando aspectos específicos relacionados à proteção da privacidade. Essa adaptação é essencial para garantir uma abordagem abrangente e eficaz diante das novas demandas e desafios organizacionais. Nesse contexto, o impacto de privacidade seria resultado de um evento que afeta os objetivos, sendo interpretado como algo que tem efeito na privacidade de um titular de DP e/ou de um grupo de titulares de DP.

Destaca-se que o impacto de privacidade pode surgir tanto do tratamento de DP em conformidade com as exigências de salvaguardas de privacidade quanto em violação a tais requisitos. A última definição encontra respaldo na norma ABNT NBR ISO/IEC 27557:2023 - Segurança da Informação, segurança cibernética e proteção da privacidade - Aplicação da

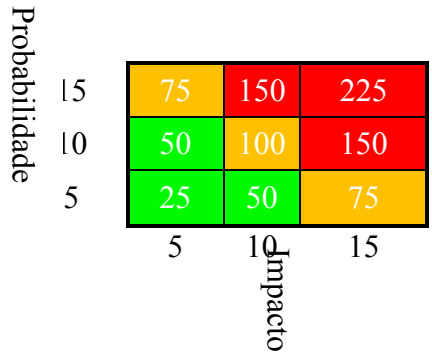
ABNT NBR ISO 31000:2018 para Gestão de Riscos de privacidade organizacional. Essa abordagem mais ampla e alinhada com normativas específicas proporciona um arcabouço mais robusto para a Gestão de Riscos, considerando integralmente as implicações na privacidade dos dados. As Tabelas 2 e 3, a seguir, ilustram os Parâmetros Escalares, Legendas de Cores e Matriz de Probabilidade x Impacto.

Tabela 2 - Parâmetros Escalares e Legenda de Cores

Classificação do Nível de Risco	Valor	Legenda
Baixo	5	Verde
Moderado	10	Amarelo
Alto	15	Vermelho

Fonte: O autor, 2023.

Tabela 3 – Matriz de Probabilidade x Impacto



Fonte: O autor, 2023.

1.2.1.5 Premissas do Método da SGD

De acordo com o Ministério da Economia (2020), o método delineado neste modelo parte de quatro premissas fundamentais para a compreensão da sua estruturação de avaliação. Essas premissas são descritas a seguir:

a) O sistema a ser avaliado é inicialmente categorizado com um nível de risco elevado (alta probabilidade e alto impacto), uma vez que os controles ainda não foram analisados para o sistema;
b) Os controles foram categorizados e agrupados em características comuns, totalizando 113 controles. Essa categorização é denominada medidas de segurança e privacidade;

c) Cada controle pode agir de maneira distinta em relação a um determinado risco, podendo contribuir para a prevenção, mitigação ou ambos simultaneamente. Controles de prevenção atuam na redução da probabilidade da ocorrência do risco, enquanto controles de mitigação atuam na redução do impacto do risco.
d) O método estabelece pesos para os controles, refletindo seu grau de importância em relação ao risco. A Tabela 4 apresenta os pesos utilizados nessa ponderação.

Essas premissas formam a base para a aplicação do modelo de avaliação proposto, fornecendo uma estrutura sólida para a análise e gestão dos riscos associados ao sistema em questão.

Tabela 4 – Descrição dos pesos utilizados

Peso	Descrição
0	Controle não se aplica ao risco
0,5	Controle se aplica
1	Controle se aplica e é prioritário

Fonte: Comitê Central de Governança de Dados (CCGD), 2020

Os controles desempenham um papel fundamental na Avaliação de Riscos, agindo tanto na mitigação quanto na prevenção de determinados riscos. A eficácia desses controles, quantificada por meio de seus pesos associados, influencia diretamente a redução da probabilidade (no caso de controles preventivos) e do impacto (quando se trata de controles de mitigação) dos riscos identificados. É relevante ressaltar que para os controles que não são aplicáveis ao sistema avaliado, não há impacto na probabilidade ou no impacto dos riscos, uma vez que sua implementação ou ausência não influencia diretamente nos cenários de risco específicos ao ambiente em questão.

O processo de cálculo do nível de risco, considerando a relação entre probabilidade e impacto, envolve as seguintes etapas:

a) Cálculo do total de controles que atuam na probabilidade e impacto: Realiza-se o somatório dos controles de prevenção (que influenciam a probabilidade) e dos controles de mitigação (que afetam o impacto);
b) Somatório dos controles de prevenção e mitigação nos grupos correspondentes: Realiza-se o somatório dos controles de prevenção no grupo de prevenção e dos controles de mitigação no grupo de mitigação;

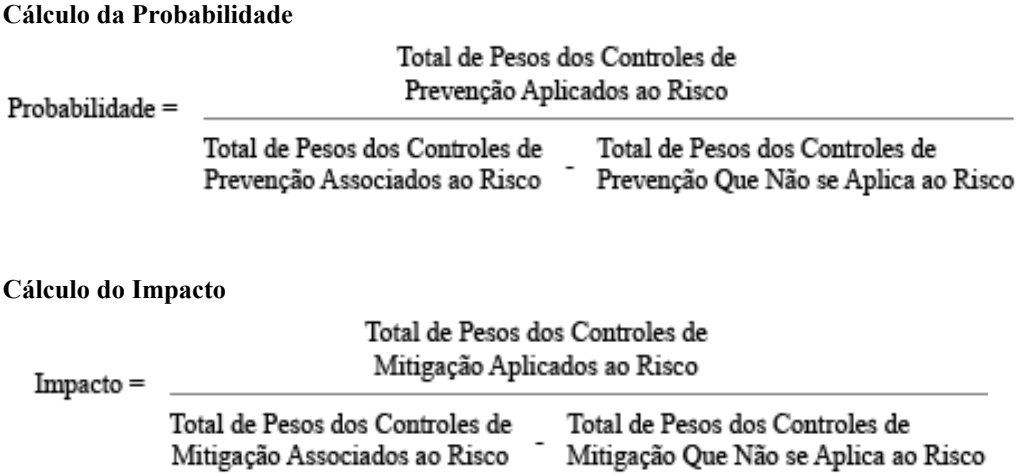
c) Contabilidade de todos os controles aplicados, não aplicados e os que não se aplicam para cada risco: esta contabilização é feita somando os pesos associados aos controles para um risco específico, levando em consideração se o controle foi aplicado, não aplicado ou se não se aplica ao risco em questão.

As fórmulas subsequentes visam medir o nível de risco a partir das respostas atribuídas aos controles (aplicado, não aplicado e não se aplica). Para calcular a probabilidade de determinado risco, realiza-se a seguinte sequência:

1. Soma de todos os pesos dos controles de prevenção aplicados ao risco, uma vez que alguns controles podem não ser aplicáveis;
2. Subtração da soma dos pesos dos controles de prevenção não aplicados da soma dos pesos dos controles de prevenção para o risco;
3. Divisão do resultado do primeiro passo pelo resultado do segundo.

Se todos os controles estão aplicados, a probabilidade é 1, e se nenhum controle está aplicado, a probabilidade é 0. Portanto, quanto mais próximo de 1, maior é a quantidade de controles aplicados, indicando uma redução significativa na probabilidade de ocorrência do risco. A fórmula de cálculo para o impacto segue um raciocínio semelhante, diferenciando-se apenas no tipo de controle avaliado (controles de mitigação), ambas apresentadas a seguir, através da Figura 5.

Figura 5 - Cálculo da Probabilidade e do Impacto



Fonte: O autor, 2023.

Conforme os controles são implementados, observa-se uma redução na classificação tanto da probabilidade quanto do impacto.

1.2.2 Modelo de Attaullah *et al*. (2022): Lógica Fuzzy, Riscos, Saúde Digital, Privacidade

Attaullah *et al.* (2022) propõe a aplicação, baseada em Lógica Fuzzy, para informações de saúde habilitadas para IoT. Esta técnica, além de anonimizar os dados, mantém sua utilidade e lida eficientemente com atualizações periódicas e dinâmicas sem comprometer a privacidade dos usuários. Introduz-se o conceito de Fuzzy-DP, que utiliza classificação Fuzzy para atribuir dados a compartimentos sem depender de consistência de assinatura. A eficácia dessa abordagem é formalmente verificada por meio do uso de Redes de Petri de Nível Superior, conhecidas como *Higher Level Petri Nets* (HLPNs) demonstrando sua capacidade de invalidar o Ataque de Assinatura Disjuntiva. Experimentos conduzidos mostram que o Fuzzy-DP supera as técnicas de anonimização existentes em termos de perda de informação, precisão de consulta e custo computacional.

Por outro lado, a modelagem formal refere-se a linguagens matemáticas empregadas para descrever sistemas e seus comportamentos. No contexto da Avaliação de Riscos, os modelos de Lógica Fuzzy emergem como uma ferramenta viável para avaliar a exposição de em-

presas a riscos que não estão completamente compreendidas. Ao contrário dos modelos tradicionais de probabilidade, a Lógica Fuzzy reconhece que a verdade pode ser uma questão de grau, permitindo uma representação mais realista da incerteza e imprecisão presentes nos cenários de risco. A modelagem formal e análise da abordagem proposta, incluindo a invalidação do Ataque de Assinatura Disjuntiva, são conduzidas utilizando HLPNs, garantindo uma análise precisa e detalhada do sistema proposto.

O Fuzzy-DP é um algoritmo proposto para proteger a privacidade de indivíduos com múltiplos atributos sensíveis (MSAs[43]) em um cenário de liberação dinâmica de dados. Ele é baseado em Lógica Fuzzy, que permite o uso de k variáveis e não fixo (número de indivíduos em cada compartimento/grupo) e um atributo sensível (em cada compartimento/grupo), e em cada liberação, ao contrário de outras abordagens que impõem consistência de assinatura.

O Fuzzy-DP tem três fases:

a) Classificação Fuzzy: Variáveis linguísticas presentes no conjunto de dados são identificadas, e valores únicos são atribuídos a cada variável. Pesos são determinados usando o centroide da ordem de classificação (ROC), e funções de pertinência (MFs) e Conjuntos Fuzzy (FSs) são definidos;
b) Atribuição de Compartimentos Fuzzy: identificadores quase-únicos e atributos sensíveis são classificados e atribuídos a compartimentos Fuzzy (FBs);
c) Anonimização: A tabela de identificadores quase-únicos anonimizados e os compartimentos de MSA são mesclados.

1.2.3 Modelo de Harth (2020): Lógica Fuzzy, GDPR, Privacidade e Especialistas

Os autores Harth, Ferrara e Paci, (2020) chamam atenção para as exigências do GDPR para que as organizações conduzam uma Avaliação de Impacto de Proteção de Dados, conhecida como *Data Protection Impact Assessment* (DPIA), quando os tratamentos de dados pessoais puderem acarretar altos riscos aos direitos e liberdades individuais dos cidadãos europeus.

[43] *Multiple Sensitive Attributes* (MSAs): referem-se à presença de vários atributos em um conjunto de dados que requerem proteção para garantir a privacidade dos indivíduos. Esses atributos podem incluir informações pessoalmente identificáveis (PII), como nome, endereço, histórico médico, informações financeiras e outros dados sensíveis. Os atributos são classificados como identificadores quase-únicos (QIs) ou atributos sensíveis (SAs), onde os QIs podem ser usados para potencialmente reidentificar indivíduos, enquanto os SAs representam as informações privadas que precisam ser protegidas (Harth, Ferrara e Paci, [s.d.]).

A DPIA permite que as organizações identifiquem, avaliem e priorizem os riscos relacionados ao tratamento de dados pessoais e selecionem mitigadores adequados para reduzir a gravidade destes riscos.

As metodologias existentes de DPIA medem a gravidade dos riscos de privacidade conforme asas opiniões dos analistas sobre a probabilidade e os fatores de impacto das ameaças. A avaliação é, portanto, subjetiva à experiência dos analistas. Para reduzir a subjetividade, os autores propõem um conjunto de critérios bem definidos que os analistas podem fazer uso para medir a probabilidade e o impacto de um risco de privacidade. Em seguida, Harth, Ferrara e Paci, (2020) adotam a Lógica Fuzzy de tomada de decisão multicritério para medirem sistematicamente a gravidade dos riscos de privacidade enquanto modelam a imprecisão e a vaguidade inerentes à avaliação linguística.

A abordagem proposta por Harth, Ferrara e Paci, (2020) consiste em três etapas:

a) a etapa de classificação: dados m ameaças e n critérios de avaliação, k tomadores de decisão expressam suas opiniões (ou pesos) sobre a importância de cada critério na avaliação da probabilidade e da intensidade do impacto das ameaças à privacidade, bem como suas avaliações sobre a gravidade de cada ameaça com relação a cada critério especificado. Nesta etapa, as opiniões dos tomadores de decisão, normalmente expressas em forma de Conjuntos Fuzzy, como termos linguísticos, são convertidas em números Fuzzy triangulares;
b) a etapa de agregação: pesos e avaliações são agregados e normalizados para calcular Matrizes Fuzzy ponderadas em relação tanto aos critérios de probabilidade quanto de impacto; e
c) a etapa de seleção: o nível de risco para ameaça é calculado usando valores Fuzzy para probabilidade e impacto. Finalmente, após a defuzzificação, as ameaças podem ser priorizadas de acordo com seu nível de risco.

Por fim, os autores entendem que, no entanto, as metodologias existentes de DPIA não fornecem uma solução eficaz para avaliar e priorizar os riscos de privacidade, pois dependem de analistas, ou seja, de especialistas, para avaliar o impacto e a probabilidade dos riscos.

1.2.4 Modelo de Garibaldi (2018): Lógica Fuzzy e Especialistas

Garibladi (2018) apresenta um *framework* conceitual de indistinguibilidade como o componente-chave da avaliação de sistemas computadorizados de suporte à decisão. Estudos de caso são apresentados nos quais demonstrou que o desempenho de especialistas humanos não é perfeito, juntamente com técnicas que podem permitir que Sistemas Fuzzy emulem o desempenho humano, incluindo a variabilidade.

O autor compartilha a necessidade da IA Fuzzy em dois sentidos:

a) a necessidade de Metodologias Fuzzy (no sentido técnico dos conjuntos e sistemas Fuzzy de Zadeh) como sistemas baseados em conhecimento para representar e raciocinar com incerteza; e
b) a necessidade de imprecisão (no sentido não técnico) com uma aceitação de desempenho imperfeito na avaliação de sistemas de IA.

Este trabalho artigo, ressalta a necessidade de Sistemas Especialistas Fuzzy como um componente útil de um conjunto de ferramentas necessário para sistemas de IA, e a necessidade de incorporar variação dentro desses sistemas. Enquanto os sistemas baseados em redes neurais de aprendizado profundo parecem atualmente oferecer talvez os mais altos níveis de desempenho disponíveis dos sistemas computadorizados (no contexto de problemas complexos que requerem técnicas de IA para serem resolvidos), eles são difíceis de explicar. Sistemas Especialistas Fuzzy fornecem algum nível aumentado de explicação, potencialmente suficiente para satisfazer os requisitos para tais sistemas serem capazes de explicar as decisões tomadas.

1.2.5 Softwares correlatos

Outros trabalhos, envolvendo outras tecnologias, são mencionados a seguir, e apesar de não detalharem seus modelos para inferência de risco, têm relevância no mercado brasileiro e estão relacionados com o modelo proposto, utilizando dados quantitativos e qualitativos para análise de risco. No entanto, é importante notar que ambos adotam uma abordagem que associa

o risco a uma lógica booleana de cumprimento ou não cumprimento, ao invés de empregar a Lógica Fuzzy. Abaixo, uma breve descrição das soluções:

- Trust Intelligence Platform, desenvolvida pela OneTrust[44];
- SoftExpert Excellence Suite, desenvolvida pela SoftExpert[45].

Embora esses softwares não adotem a Lógica Fuzzy, suas utilizações proporcionam às organizações meios eficazes para lidar com os desafios relacionados à gestão de riscos, segurança da informação, privacidade de dados e governança corporativa.

1.3 **Metodologia**

A justificativa para a realização deste trabalho assenta-se na lacuna existente entre as práticas atuais de privacidade e proteção de dados e a necessidade de adaptação às dinâmicas fluidas e complexas de tratamento da informação. A relevância de explorar a aplicabilidade da Lógica Fuzzy na Gestão de Riscos de privacidade está na sua capacidade de incorporar a incerteza e a ambiguidade nas estratégias de *compliance*, refletindo mais acuradamente o modo de operação do raciocínio humano. Além disso, diante das penalidades por não conformidade e o potencial prejuízo à reputação causado por incidentes de privacidade e proteção de dados pessoais, torna-se essencial a busca por metodologias que fortaleçam a confiança dos agentes de tratamento e assegurem o cumprimento das obrigações legais. Assim, investigar a Lógica Fuzzy como um meio de atingir esses objetivos, não é apenas oportuno, mas também é uma necessidade estratégica para as organizações que buscam excelência na governança de dados pessoais, que forem confiados a elas.

[44] Disponível em: https://www.onetrust.com/pt.
[45] Disponível em: https://www.softexpert.com/pt-br/solucao/lgpd.

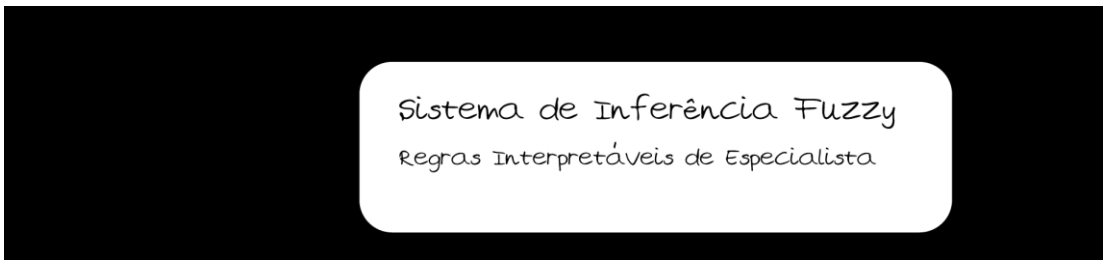
A metodologia empregada para alcançar os objetivos delineados na seção subsequente é fundamentada em uma abordagem qualitativa, a qual é escolhida por diversas razões estratégicas e metodológicas, incluindo:

a) Acesso Remoto a Participantes: A pesquisa qualitativa permite o estudo de indivíduos ou grupos aos quais não temos acesso físico, superando barreiras geográficas e possibilitando uma amostra mais diversificada;
b) Dados como Fonte Natural de Informação: Os dados tratados pelo sistema são considerados uma fonte de informação orgânica, refletindo as interações e comportamentos naturais dos sujeitos de estudo;
c) Identificação de Tendências Comportamentais: Este método é particularmente útil para identificar tendências e padrões no comportamento dos profissionais relacionados ao tratamento de dados pessoais e sensíveis;
d) Dados Pessoais: Os dados pessoais permanecerão os mesmos, num geral, após longos períodos;
e) Compreensão Aprofundada de Estruturas e Modelos: A abordagem qualitativa facilita a análise aprofundada das características, estruturas e modelos subjacentes associados aos dados pessoais e sensíveis.

Portanto, a escolha deste método qualitativo se alinha com a natureza dos objetivos de pesquisa e promete oferecer *insights* detalhados e contextualizados sobre a gestão e tratamento de dados pessoais e sensíveis.

A Figura 6 ilustra um modelo, baseado em Lógica Fuzzy para identificação de Risco, à luz da LGPD, na Saúde Digital. Neste caso, a Lógica Fuzzy pode ser usada para responder perguntas, o que pode ser extremante útil para aplicações na Saúde Digital relacionadas ao *compliance* com a LGPD. Este modelo é uma adaptação do que foi apresentado por Brian Douglas, que por sua vez, utilizou um exemplo de um sistema bancário que decide o risco de empréstimo de valores monetários para um cidadão, baseado em uma série de informações pessoais e financeiras (Zadeh, 1965b).

Figura 6 - Modelo hipotético



Fonte: Autor

1.3.1 Modelagem

No âmbito da presente dissertação, o foco recai sobre o desenvolvimento e a implementação de um Sistema de Inferência Fuzzy no qual o usuário é incumbido de fornecer valores específicos para as variáveis de entrada, também conhecidas como antecedentes, que neste caso estão diretamente relacionadas aos aspectos de privacidade e segurança da informação sob a perspectiva da LGPD. Após o recebimento e processamento dessas entradas, o sistema procede à execução de sua Lógica de Inferência Fuzzy para determinar a variável de saída, ou consequente. Neste contexto, a variável de saída é o 'Risco' associado, refletindo o percentual de risco decorrente das condições especificadas nas entradas.

Essa abordagem permite uma análise quantitativa e qualitativa das implicações da LGPD, oferecendo análises valiosas sobre os riscos potenciais em cenários variados de privacidade e segurança de dados. A clareza na definição destes processos é fundamental para compreender o funcionamento e a aplicabilidade do Sistema de Inferência Fuzzy no contexto da conformidade com a LGPD.

1.3.1.1 Problema que motivou o Projeto

O problema que catalisou o desenvolvimento deste projeto é a dificuldade intrínseca em avaliar e gerenciar o risco de violações de privacidade e segurança da informação no contexto da Saúde Digital, especialmente sob as regulamentações da LGPD. Com a digitalização acelerada dos serviços de saúde e o consequente aumento do volume e da sensibilidade dos dados processados, as organizações enfrentam desafios significativos para manter a conformidade re-

gulatória e proteger os dados pessoais e dados pessoais dos indivíduos. A incapacidade de sistemas tradicionais de lidar com a ambiguidade e complexidade dos dados de saúde e as exigências legais associadas, sublinha a necessidade de uma abordagem mais sofisticada e matizada para a Gestão de Riscos. A busca por uma solução que possa oferecer tanto flexibilidade quanto rigor na Avaliação de Riscos é o que impulsiona este projeto.

O problema exposto é amplificado pelas sanções impostas pela LGPD, e que poderão ser aplicadas pela ANPD aos agentes de tratamento que falham em cumprir suas exigências. Organizações e profissionais liberais que tratam dados pessoais e dados pessoais sensíveis, se não estabelecerem um mecanismo eficaz de Gestão de Riscos, estão sujeitos a uma série de penalidades. Além das sanções financeiras, os agentes de tratamento podem enfrentar danos reputacionais irreparáveis, perda de confiança por parte dos sujeitos de cuidado, e a possibilidade de suspensão parcial ou total do tratamento de tais dados. A exigência de um sistema capaz de identificar, avaliar e mitigar riscos de forma proativa torna-se, assim, uma questão crítica, não apenas para a conformidade legal, mas também para a sustentabilidade operacional e a integridade corporativa no setor da Saúde Digital.

1.3.1.2 Pergunta de Pesquisa

É possível mitigar riscos associados à adequação a arcabouços jurídico-regulatórios relacionados à privacidade e proteção de dados na área da Saúde; reduzir os riscos associados a incidentes de segurança da informação e da privacidade; e possibilitar melhores práticas para tratamento de dados pessoais e dados pessoais sensíveis?

Para abordar a presente questão de pesquisa, serão examinadas nas subseções seguintes a origem e as implicações dos resultados obtidos mediante a aplicação do método proposto.

Após a realização de cada teste nas diferentes variações, foram conduzidas análises sobre o comportamento do modelo. Essas análises basearam-se na métrica do erro das medidas de risco obtidas, calculado pela diferença entre o RO e o RE. As análises realizadas incluíram o Erro Médio (EM), Erro Médio Absoluto (EMA), Desvio Padrão do Erro Médio (DEM) e Desvio Padrão do Erro Médio Absoluto (DEMA).

Ao analisar o Erro Médio, observou-se um valor de -1,34 pontos, enquanto o Erro Médio Absoluto apresentou um valor de 2,34 pontos. Ambos os valores estão muito próximos de zero, o que indica um bom desempenho do modelo.

Sobre o Desvio Padrão do Erro Médio e o Desvio Padrão do Erro Médio Absoluto, foram obtidos os seguintes valores: 3,15 e 2,50, respectivamente. Esses resultados indicam que os erros estão aproximados da média e apresentam baixa dispersão. Isso evidencia a presença de poucos valores extremos ou anomalias, o que, por fim, sugere uma boa precisão do modelo.

1.3.1.3 Variáveis Linguísticas

A Modelagem Fuzzy desenvolvida para abordar o problema em voga foi realizada conforme o Modelo de Inferência de Mamdani, onde tanto as variáveis de entrada, quanto as de saída são variáveis linguísticas. Para as variáveis de entrada foram desenvolvidas nove variáveis linguísticas e para as variáveis de saída foi desenvolvida apenas uma (Tanscheit, 2001g).

A escolha das variáveis linguísticas de entrada foi fundamentada a partir de modelo de Inventário de Dados Pessoais (IDP), disponibilizado pelo Governo Digital (Governo Digital; Ministério da Gestão e da Inovação em Serviços Públicos, 2021). Já a escolha da variável linguística de saída, foi fundamentada no Guia de Avaliação de Riscos de Segurança e Privacidade (Roberto et al., 2020). Tais escolhas almejaram a realização de consultas ao banco de dados da ferramenta, por meio de *queries* SQL, além da adequação às diretrizes de risco previstas na Norma ABNT NBR ISO 31000: Gestão de Riscos – Diretrizes (Associação Brasileira de Normas Técnicas, 2018).

Desta forma, foram escolhidas as seguintes variáveis linguísticas de entrada:

a) Número de titulares;
b) Porcentagem de dados pessoais armazenados fora do território brasileiro;
c) Porcentagem de dados pessoais armazenados fora do ciclo de vida legal;
d) Porcentagem de dados pessoais sensíveis sem hipótese de tratamento;
e) Porcentagem de dados pessoais sensíveis com hipótese de tratamento indevida;
f) Número de pessoas com acesso a dados pessoais sensíveis;
g) Porcentagem de dados pessoais sem hipótese de tratamento;

h) Porcentagem de dados pessoais com hipótese de tratamento indevida;
i) Número de pessoas com acesso a dados pessoais.

A escolha da variável linguística de saída foi o percentual de Risco.

Cabe destacar que os valores das funções de pertinência (trapezionais e triangulares) apresentados nas páginas seguintes, para cada uma das variáveis linguísticas (entrada e saída), foram estabelecidos por especialista em Gestão de Riscos, privacidade e proteção de dados, com ênfase na LGPD. A seguir, são descritas as variáveis linguísticas de entrada, considerando os seus respectivos universos de discursos, rótulos e conjuntos nebulosos:

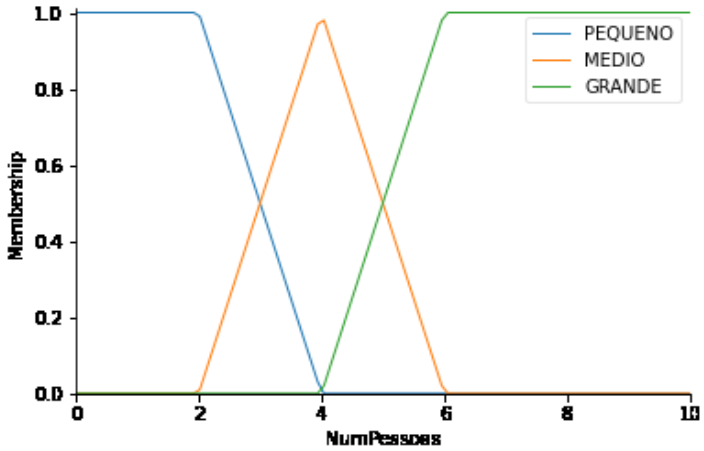
Número de titulares

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 10 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 2, e 4);
- MÉDIO: função de pertinência triangular com valores: (2, 4, e 6);
- GRANDE função de pertinência trapezoidal com valores: (4, 6, 10 e 10).

É importante ressaltar que o valor de entrada desta variável linguística é o número de titulares armazenados pelo sistema, na base logarítmica 10. O Gráfico 1 – *Variável Linguística de Entrada: Número de titulares* ilustra o gráfico do comportamento esperado para a referida variável.

Gráfico 1 - Variável Linguística de Entrada: Número de titulares



Fonte: O autor, 2023.

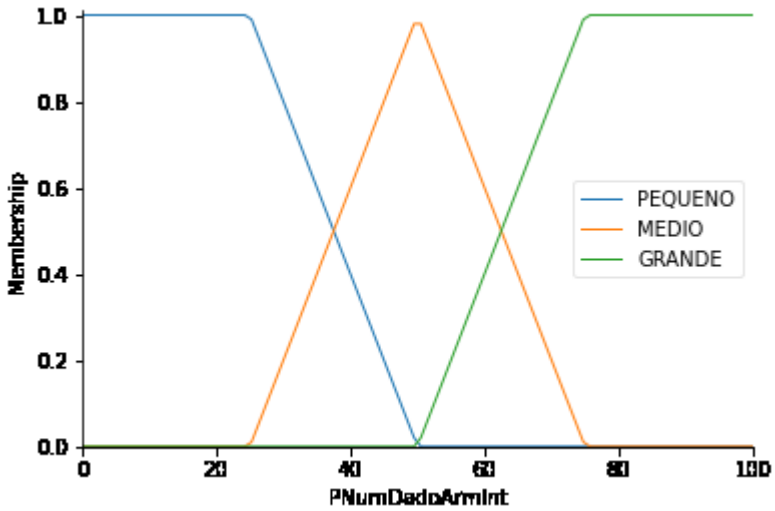
Porcentagem de dados armazenados internacionalmente

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 25 e 50);
- MÉDIO: função de pertinência triangular com valores: (25, 50 e 75);
- GRANDE sendo uma função de pertinência trapezoidal com valores: (50, 75, 100 e 100).

A entrada é a porcentagem de dados pessoais armazenados fora do território brasileiro. O Gráfico 2 – *Variável Linguística de Entrada: Porcentagem de dados armazenados fora do território brasileiro* ilustra o comportamento esperado para a referida variável.

Gráfico 2 - Variável Linguística de Entrada: Porcentagem de dados pessoais armazenados



Fonte: O autor, 2023.

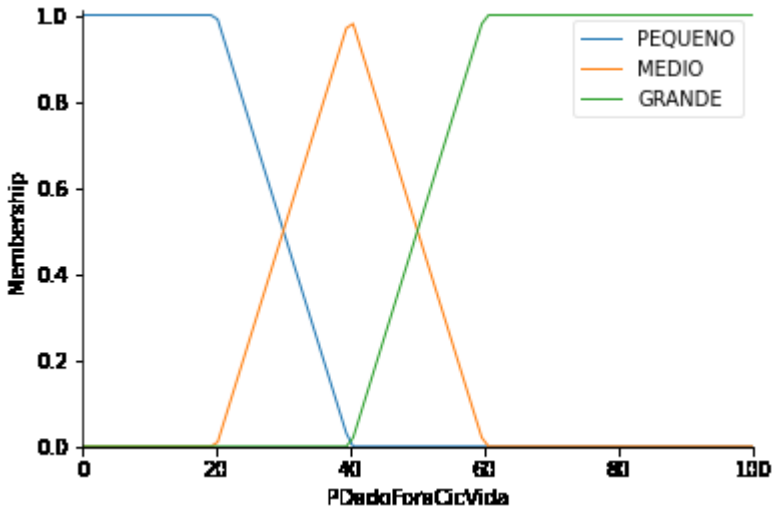
Porcentagem de dados armazenados fora do ciclo de vida

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 20 e 40)
- MÉDIO: função de pertinência triangular com valores: (20, 40 e 60)
- GRANDE: função de pertinência trapezoidal com valores: (40, 60, 100 e 100)

A entrada desta variável linguística é a porcentagem de dados pessoais armazenados pelo sistema e que seus armazenamentos e demais operações de tratamento extrapolaram os seus ciclos de vida previstos, e consequentemente a legalidade para os seus tratamentos. O Gráfico 3 – *Variável Linguística de Entrada: Porcentagem de dados pessoais armazenados fora do ciclo de vida legal previsto* ilustra o comportamento esperado para a referida variável.

Gráfico 3 - Variável Linguística de Entrada: Porcentagem de dados



Fonte: O autor, 2023.

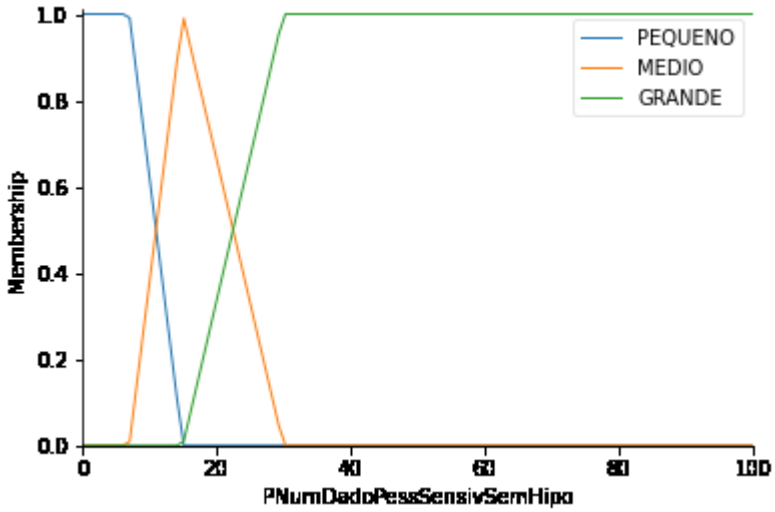
Porcentagem de dados pessoais sensíveis sem hipótese

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 7 e 15)
- MÉDIO: função de pertinência triangular com valores: (7, 15 e 30)
- GRANDE: função de pertinência trapezoidal com valores: (15, 30, 100 e 100).

A entrada desta variável linguística é a porcentagem de dados pessoais sensíveis, armazenados, sem hipótese de tratamento. O Gráfico 4 – *Variável Linguística de Entrada: Porcentagem de dados pessoais sensíveis sem hipótese* ilustra o comportamento esperado para a referida variável.

Gráfico 4 - Variável Linguística de Entrada: Porcentagem de dados pessoais sensíveis sem hipótese



Fonte: O autor, 2023.

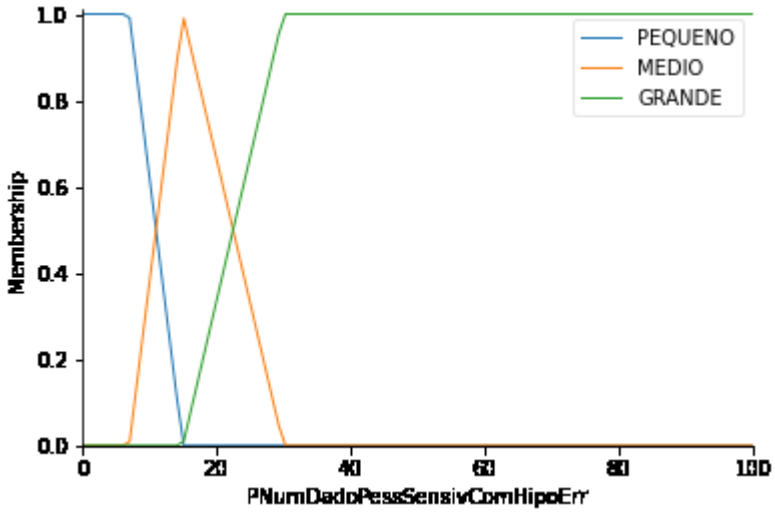
Porcentagem de dados pessoais sensíveis com hipótese equivocada

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 7 e 15);
- MÉDIO: função de pertinência triangular com valores: (7, 15 e 30);
- GRANDE: função de pertinência trapezoidal com valores: (15, 30, 100 e 100).

A entrada desta variável linguística é a porcentagem de dados pessoais sensíveis, armazenados, com hipóteses de tratamento equivocadas. O Gráfico 5 – *Variável Linguística de Entrada*: Porcentagem de dados pessoais sensíveis com hipótese equivocada ilustra o gráfico do comportamento esperado para a referida variável.

Gráfico 5 - Variável Linguística de Entrada: Porcentagem de dados pessoais sensíveis com hipótese equivocada



Fonte: O autor, 2023.

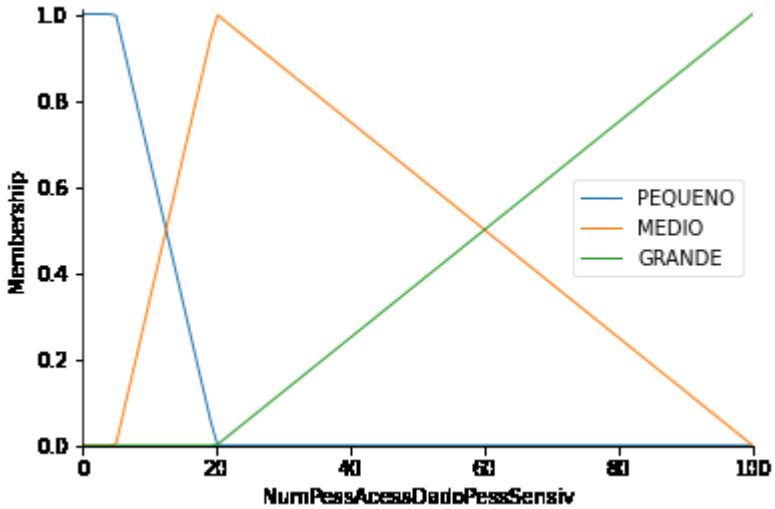
Número de pessoas com acesso a dados pessoais sensíveis

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 5 e 20);
- MÉDIO: função de pertinência triangular com valores: (5, 20 e 100);
- GRANDE: função de pertinência trapezoidal com valores: (20, 100, 100 e 100).

A entrada desta variável linguística é a porcentagem de dados pessoais sensíveis, armazenados, com hipóteses de tratamento equivocadas. O Gráfico 6 – *Variável Linguística de Entrada: Número de pessoas com acesso a dados pessoais sensíveis* ilustra o comportamento esperado para a referida variável.

Gráfico 6 - Variável Linguística de Entrada: Número de pessoas com acesso a dados pessoais sensíveis



Fonte: O autor, 2023.

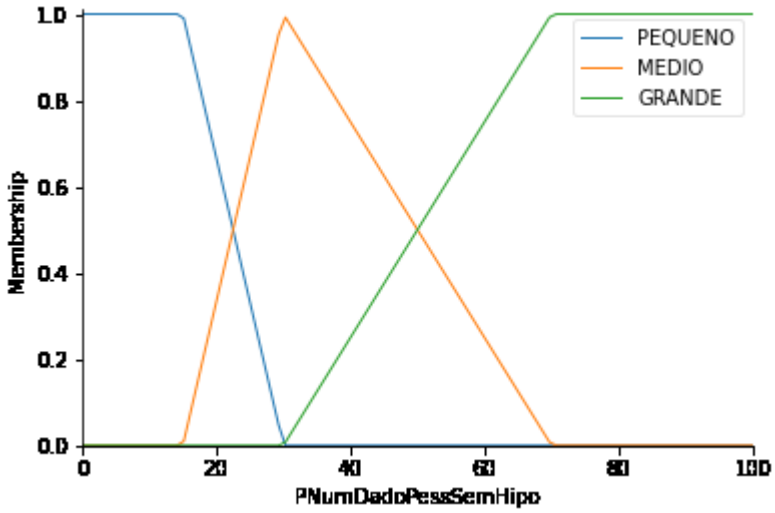
Porcentagem de dados pessoais sem hipótese

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 15 e 30)
- MÉDIO: função de pertinência triangular com valores: (15, 30 e 70)
- GRANDE: função de pertinência trapezoidal com valores: (30, 70, 100 e 100)

A entrada desta variável linguística é a porcentagem de dados pessoais sensíveis, armazenados, sem hipóteses de tratamento. O Gráfico 7 – *Variável Linguística de Entrada: Porcentagem de dados pessoais sem hipótese de tratamento* ilustra o comportamento esperado para a referida variável.

Gráfico 7 - Variável Linguística de Entrada: Porcentagem de dados pessoais sem hipótese de tratamento



Fonte: O autor, 2023.

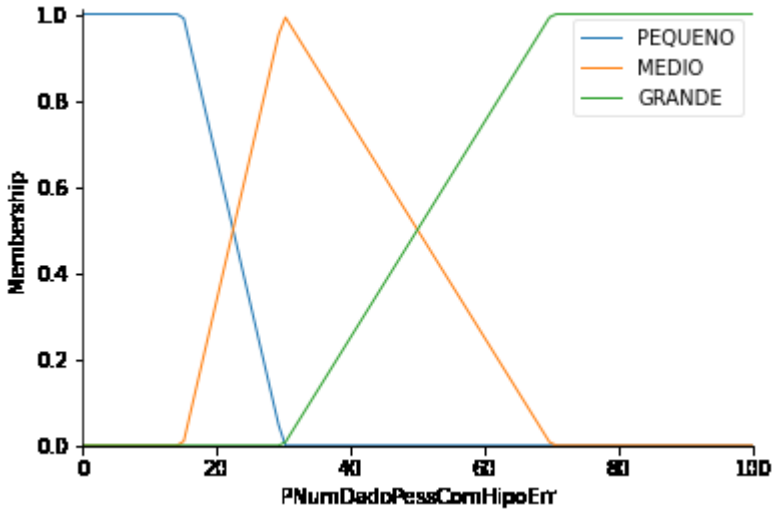
Porcentagem de dados pessoais com hipótese equivocada

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 15 e 30);
- MÉDIO: função de pertinência triangular com valores: (15, 30 e 70);
- GRANDE: função de pertinência trapezoidal com valores: (30, 70, 100 e 100).

A entrada desta variável linguística é a porcentagem de dados pessoais armazenados com hipóteses de tratamento equivocadas. O Gráfico 8 – *Variável Linguística de Entrada: Porcentagem de dados pessoais com hipótese equivocada* ilustra o comportamento esperado para a referida variável.

Gráfico 8 - Variável Linguística de Entrada: Porcentagem de dados pessoais com hipótese equivocada



Fonte: O autor, 2023.

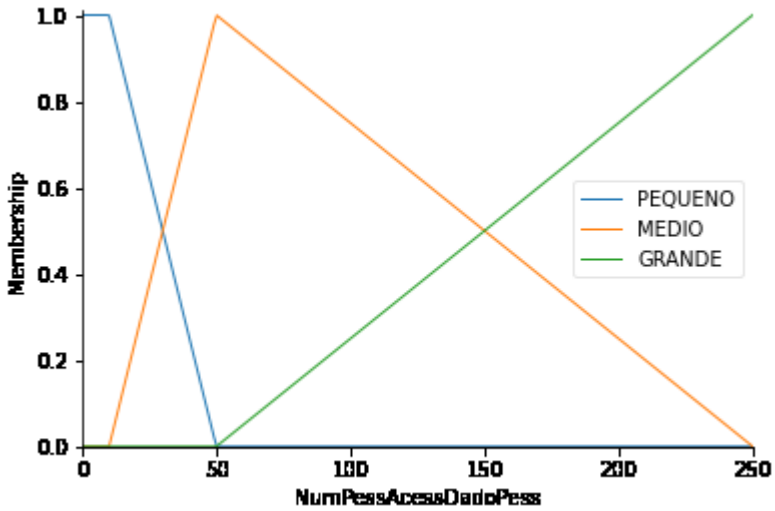
Número de pessoas com acesso a dados pessoais

A modelagem dessa variável linguística de entrada foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 10 e 50);
- MÉDIO: função de pertinência triangular com valores: (10, 50 e 250);
- GRANDE: função de pertinência trapezoidal com valores: (50, 250, 250 e 250).

A entrada desta variável linguística é o número de pessoas com acesso a dados pessoais. O Gráfico 9 – *Variável Linguística de Entrada: Número de pessoas com acesso a dados pessoais* ilustra o gráfico do comportamento esperado para a referida variável.

Gráfico 9 - Variável Linguística de Entrada: Número de pessoas com acesso a dados pessoais



Fonte: O autor, 2023.

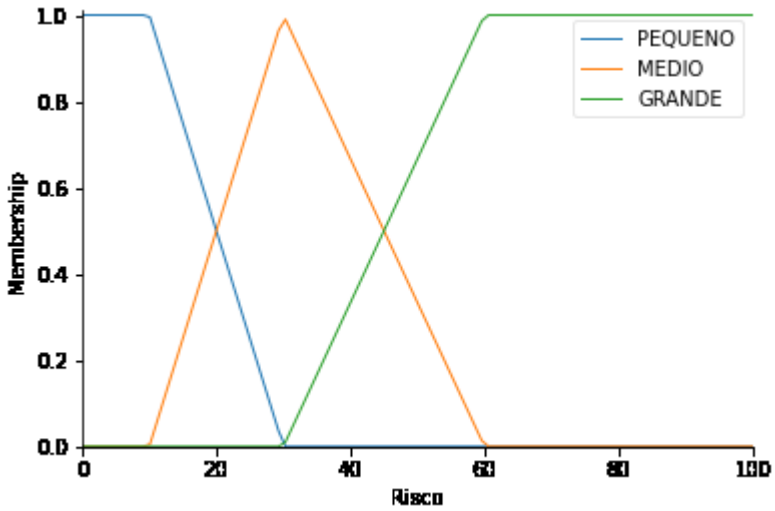
Risco

A modelagem dessa variável linguística de saída foi realizada a partir de um universo de discurso de 0 até 100 e de três rótulos, a saber: “PEQUENO”, “MÉDIO”, “GRANDE”. Onde cada um desses rótulos é descrito respectivamente pelos seguintes conjuntos nebulosos:

- PEQUENO: função de pertinência trapezoidal com valores: (0, 0, 10 e 25);
- MÉDIO: função de pertinência triangular com valores: (10, 25 e 50);
- GRANDE: função de pertinência trapezoidal com valores: (25, 50, 100 e 100).

A saída desta variável linguística é o resultado do cálculo do risco. O Gráfico 10 – Variável Linguística de Saída: Risco ilustra o comportamento esperado para a referida variável.

Gráfico 10 - Variável Linguística de Saída: Risco



Fonte: O autor, 2023.

1.3.1.4 Regras de Inferência

Para a modelagem das regras do método de inferência, foram empregadas apenas as operações clássicas AND (E) e OR (OU), conforme proposto por Zadeh (1965). No total, foram geradas 72 Regras de Inferência Fuzzy, detalhadas no Apêndice.

Ao utilizar essas Regras de Inferência Fuzzy com os dados de entrada, previamente fuzzificados pelos Conjuntos Fuzzy de cada Variável Linguística, é possível obter os graus de pertinência da variável de risco. Aplicando então o método de Defuzzificação do centro de área, calcula-se o valor para determinar o risco do sistema a ser avaliado.

A seguir, é apresentado um exemplo fictício do resultado da avaliação de um sistema cujas variáveis de entrada foram as seguintes:

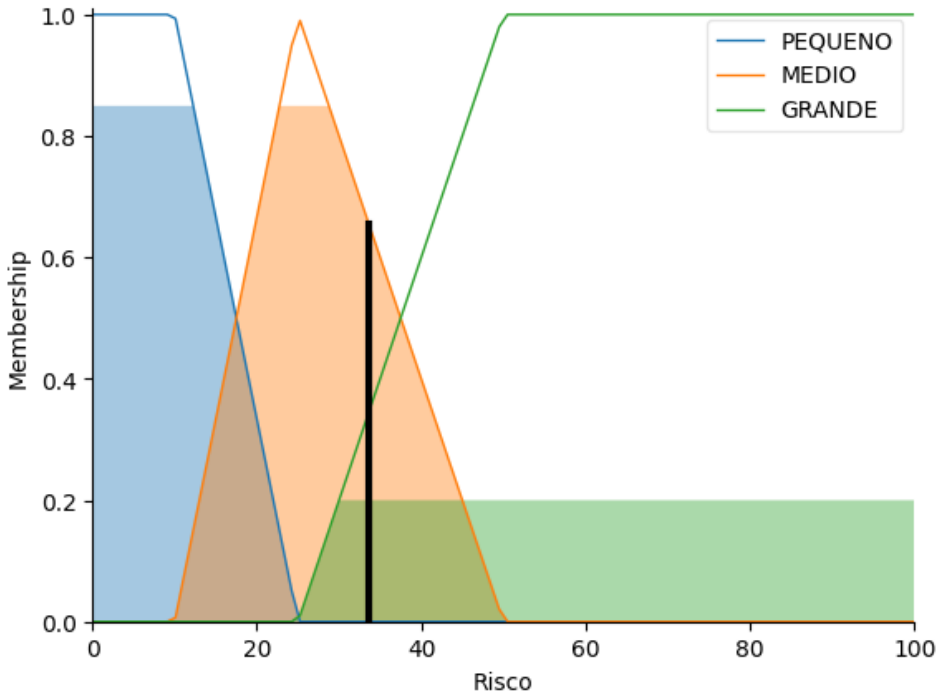
a) Número de pessoas = Número de pessoas = $\mathbf{log_{10}\ 100}$;
b) Porcentagem de dados armazenados internacionalmente = 5;
c) Porcentagem de dados armazenados fora do ciclo de vida = 5;
d) Porcentagem de dados pessoais sensíveis sem hipótese = 7;
e) Porcentagem de dados pessoais sensíveis com hipótese errada = 10;
f) Número de pessoas com acesso a dados pessoais sensíveis = 8;
g) Porcentagem de dados pessoais sem hipótese = 10;

h) Porcentagem de dados pessoais com hipótese errada = 15;

i) Número de pessoas com acesso a dados pessoais = 8.

O resultado obtido pelo exemplo pode ser observado na Figura 7.

Figura 7 - Conjuntos Fuzzy Variável Linguística de Saída: Risco



Fonte: O autor, 2023.

Neste exemplo, foi obtido o risco de 33,6%, frente às Variáveis Linguísticas adotadas para cumprimento de exigências da LGPD.

1.3.1.5 Produto Digital

A consolidação de boas práticas na entrega de produtos digitais torna-se imperativa, especialmente no contexto das organizações que prestam serviços na área da Saúde Digital. Este estudo propõe-se a abordar aspectos cruciais relacionados à integridade e conformidade no tratamento de dados pessoais e dados pessoais sensíveis, enfatizando a importância da gestão eficaz dessas informações, fundamentada na Gestão de Riscos. A essência desta pesquisa reside no desenvolvimento e aprimoramento de um produto digital destinado ao cadastro de pacientes,

considerando, elementos fundamentais como a transferência internacional de dados, a identificação de dados pessoais e/ou sensíveis sem uma hipótese legal de tratamento apropriada, e a Avaliação de Riscos associados.

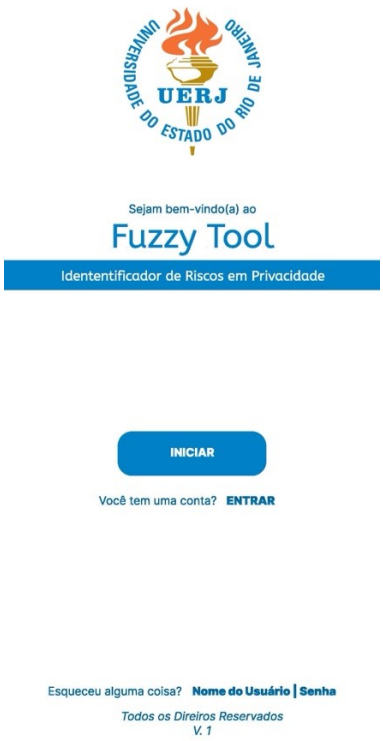
A fundamentação desta dissertação é solidificada por meio da investigação de patentes, consulta a artigos técnicos e científicos, revisão de livros e periódicos especializados, bem como a análise de normas técnicas pertinentes ao cenário da Saúde Digital. A abordagem holística adotada incorpora não apenas elementos técnicos, mas também estratégias para uma compreensão abrangente da temática.

A proposta de valor do produto digital consiste na implementação de mecanismos efetivos para o cadastro de pacientes, incluindo a devida consideração à transferência internacional de dados pessoais e/ou sensíveis. Destaca-se, igualmente, a identificação de dados pessoais sendo tratados sem uma hipótese legal de tratamento, ou em cenário mais comum, com uma hipótese legal indevida. A transparência na gestão dessas informações é promovida, respeitando a privacidade dos indivíduos e cumprindo as normativas vigentes, com destaque para a LGPD.

Além disso, o produto digital engloba proposição de uma avaliação abrangente de riscos associados aos tratamentos de dados pessoais e dados pessoais sensíveis, mesmo na ausência de uma hipótese legal de tratamento estabelecida. Esse enfoque proativo visa antecipar e mitigar potenciais ameaças à segurança e privacidade dos dados, contribuindo para uma abordagem mais resiliente e responsável na gestão de dados pessoais e dados pessoais sensíveis na Saúde Digital.

A tela inicial do produto digital denominado “Fuzzy Tool: Identificador de Riscos em Privacidade” é exposta na Figura 8 a seguir.

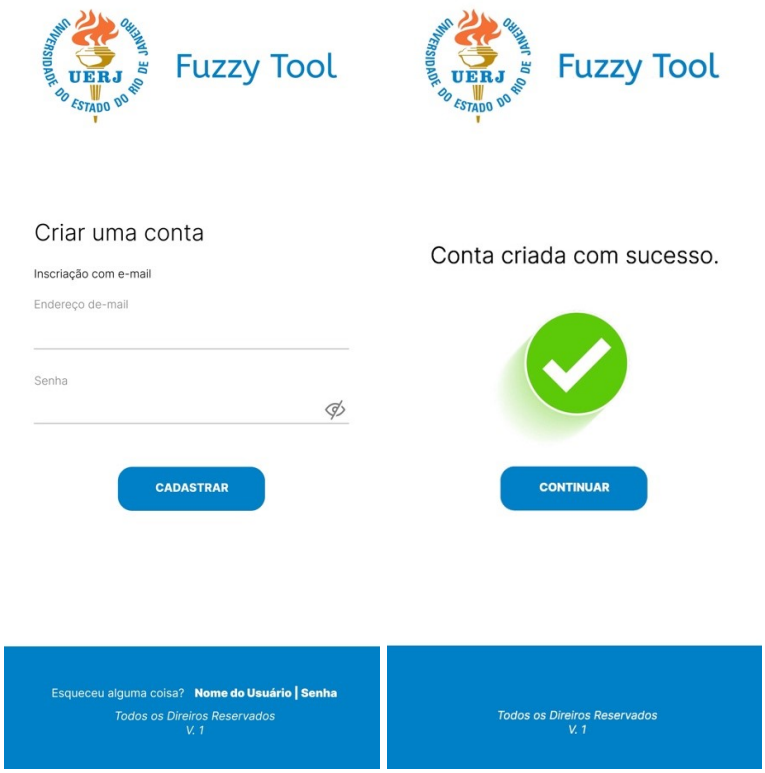
Figura 8 - Fuzzy Tool: tela inicial



Fonte: O autor, 2023.

A Figura 9, a seguir, exibe as interfaces de criação de cadastro de usuários no Fuzzy Tool: Identificador de Riscos em Privacidade.

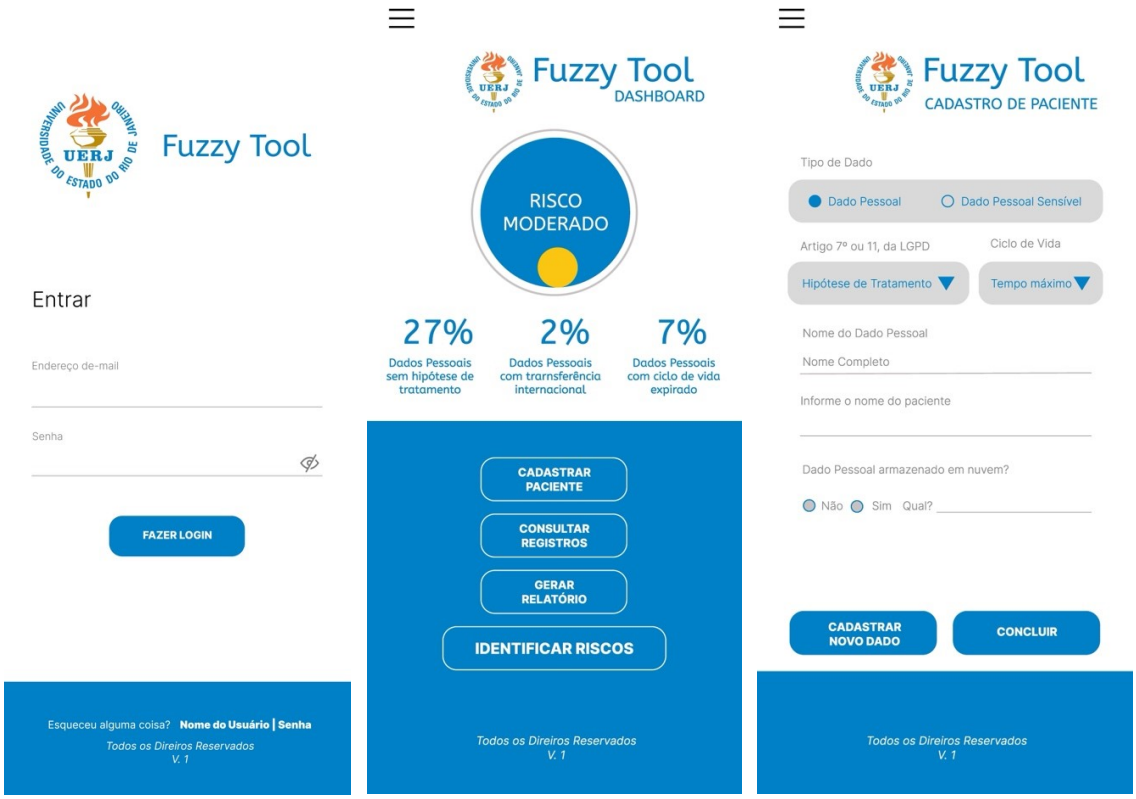
Figura 9 - Fuzzy Tool: criação de cadastro



Fonte: O autor, 2023.

A Figura 10, exibida adiante, ilustra a tela de login da ferramenta Fuzzy Tool, acompanhada das funcionalidades padrão para recuperação de login e senha disponíveis no rodapé.

Figura 10 - Fuzzy Tool: telas de login e cadastro



Fonte: O autor, 2023.

2 RESULTADOS

Nesta seção, são examinados três casos para avaliar o desempenho da metodologia e do modelo, fundamentados na Lógica Fuzzy, conforme descrito na subseção 2.3, para quantificação dos riscos associados ao tratamento de dados pessoais e dados pessoais sensíveis por agentes de tratamento da Saúde Digital.

2.1 Comparação do Modelo da SGD com o modelo proposto

A comparação entre o modelo proposto nesta dissertação e o Modelo de Avaliação de Riscos de Segurança e Privacidade, da SGD, revelou a inexistência de uma equivalência direta entre as variáveis linguísticas de entrada adotadas no modelo proposto e os critérios do Modelo da SGD. Enquanto este último se baseia em 113 controles estabelecidos por normas técnicas, associando o risco a uma lógica booleana de cumprimento ou não cumprimento, os parâmetros do modelo proposto nesta dissertação abrangem quantidades de registros (número de titulares), porcentagens derivadas desses registros e o número de controles. Esta diferença essencial indica que o Modelo da SGD não se concentra na análise de volumes de registros ou na quantidade de controles aplicados.

Não foram identificadas equivalências entre as variáveis linguísticas do modelo proposto nesta dissertação e os controles adotados pela SGD em seu modelo.

2.1.1 Teste Sintético através do modelo proposto

Uma série de testes foi conduzida para avaliar os resultados da modelagem em relação às expectativas dos especialistas do domínio. Esses testes foram realizados em ambientes preparados para simular o tratamento de dados pessoais e dados pessoais sensíveis. Em cada teste, uma única variável foi modificada, enquanto as demais foram mantidas constantes, visando validar a perturbação no modelo e a sensibilidade de cada variável em relação ao risco obtido.

Os valores de cada Variável Linguística foram fixados no limite mínimo da base de dados, a fim de explorar ao máximo a variação exclusiva de cada uma delas ao compará-las com as expectativas. Isso possibilitou uma análise individual precisa de cada variável. A linha de base para a fixação dos testes foi a seguinte:

a) Número de titulares = $\mathbf{log_{10}\ 100}$;
b) Porcentagem de dados armazenados internacionalmente = 25;
c) Porcentagem de dados armazenados fora do ciclo de vida = 20;
d) Porcentagem de dados pessoais sensíveis sem hipótese = 7;
e) Porcentagem de dados pessoais sensíveis com hipótese errada = 7;
f) Número de pessoas com acesso a dados pessoais sensíveis = 5;
g) Porcentagem de dados pessoais sem hipótese = 15;
h) Porcentagem de dados pessoais com hipótese errada = 15;
i) Número de pessoas com acesso a dados pessoais = 10.

A estruturação dos testes foi realizada por meio de tabelas individuais para cada variável. Os cabeçalhos das tabelas indicam a variável correspondente, identificada pelo número de sua respectiva variável linguística de entrada, seguindo a apresentação anterior, conforme a linha base de fixação, que está alinhada com a etapa da metodologia.

Além disso, foi implementada uma diferenciação no tratamento da variável linguística de saída. Nesse sentido, a variável foi representada pelo Risco Obtido (RO), para distingui-la da referência de Risco Esperado (RE), na qual será inserido o valor esperado durante a execução dos testes.

Os valores de RE foram determinados por meio da análise dos casos de teste sob a ótica de um especialista do domínio. Os especialistas possuem anos de experiência em estudo e trabalho na área da LGPD, com foco em privacidade, conformidade e proteção de dados. A principal finalidade desses valores foi proporcionar uma interpretação realista sobre as respostas esperadas do modelo.

A seguir, serão apresentadas as tabelas individuais de cada teste, juntamente com suas respectivas variações. Essas tabelas estão numeradas de 6 a 14.

A Tabela 5, apresentada a seguir, evidencia a variação do parâmetro em questão, Número de Titulares:

Tabela 5 – Parâmetro: Número de Titulares

1	2	3	4	5	6	7	8	9	RO	RE
10^1	25	20	7	7	5	15	15	10	9,6	17
10^2	25	20	7	7	5	15	15	10	10,2	20
10^3	25	20	7	7	5	15	15	10	22,4	30
10^4	25	20	7	7	5	15	15	10	29,6	35
10^5	25	20	7	7	5	15	15	10	56,8	50
10^6	25	20	7	7	5	15	15	10	60,3	65

Fonte: O autor, 2023.

A Tabela 6, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados armazenados internacionalmente:

Tabela 6 – Parâmetro: Porcentagem de dados armazenados internacionalmente

1	2	3	4	5	6	7	8	9	RO	RE
100	40	20	7	7	5	15	15	10	10,2	10
100	55	20	7	7	5	15	15	10	15,4	15
100	60	20	7	7	5	15	15	10	18,1	18
100	80	20	7	7	5	15	15	10	20	21

Fonte: O autor, 2023.

A Tabela 7, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados armazenados fora do ciclo de vida:

Tabela 7 – Parâmetro: Porcentagem de dados armazenados fora do ciclo de vida

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	7	5	15	15	10	10,2	10
100	25	40	7	7	5	15	15	10	10,4	12
100	25	50	7	7	5	15	15	10	18,8	18
100	25	60	7	7	5	15	15	10	20	25

Fonte: O autor, 2023.

A Tabela 8, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados pessoais sensíveis sem hipótese:

Tabela 8 – Parâmetro: Porcentagem de dados pessoais sensíveis sem hipótese

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	0	7	5	15	15	10	10,2	10
100	25	20	10	7	5	15	15	10	17,8	20
100	25	20	20	7	5	15	15	10	38,8	40
100	25	20	40	7	5	15	15	10	55,4	60

Fonte: O autor, 2023.

A Tabela 9, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados pessoais sensíveis com hipótese errada:

Tabela 9 – Parâmetro: Porcentagem de dados pessoais sensíveis com hipótese errada

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	0	5	15	15	10	10,2	10
100	25	20	7	10	5	15	15	10	17,8	20
100	25	20	7	20	5	15	15	10	38,8	40
100	25	20	7	40	5	15	15	10	55,4	60

Fonte: O autor, 2023.

A Tabela 10 apresentada a seguir, evidencia a variação do parâmetro em questão, Número de pessoas com acesso a dados pessoais sensíveis:

Tabela 10 – Parâmetro: Número de pessoas com acesso a dados pessoais sensíveis

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	7	5	15	15	10	10,2	10
100	25	20	7	7	15	15	15	10	20	20
100	25	20	7	7	30	15	15	10	28,5	30
100	25	20	7	7	60	15	15	10	44,9	40

Fonte: O autor, 2023.

A Tabela 11, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados pessoais sem hipótese:

Tabela 11 – Parâmetro: Porcentagem de dados pessoais sem hipótese

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	7	5	20	15	10	10,2	10
100	25	20	7	7	5	40	15	10	16,9	16
100	25	20	7	7	5	60	15	10	20,1	18
100	25	20	7	7	5	80	15	10	20,4	20

Fonte: O autor, 2023.

A Tabela 12, apresentada a seguir, evidencia a variação do parâmetro em questão, Porcentagem de dados pessoais com hipótese errada:

Tabela 12 – Parâmetro: Porcentagem de dados pessoais com hipótese errada

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	7	5	15	20	10	10,2	10
100	25	20	7	7	5	15	40	10	16,9	16
100	25	20	7	7	5	15	60	10	20,1	18
100	25	20	7	7	5	15	80	10	20,4	20

Fonte: O autor, 2023.

A Tabela 13, apresentada a seguir, evidencia a variação do parâmetro em questão, Variando Número de pessoas com acesso a dados pessoais:

Tabela 13 – Parâmetro: Número de pessoas com acesso a dados pessoais

1	2	3	4	5	6	7	8	9	RO	RE
100	25	20	7	7	5	15	15	0	10,2	10
100	25	20	7	7	5	15	15	60	12,5	12
100	25	20	7	7	5	15	15	80	15,1	15
100	25	20	7	7	5	15	15	100	16,9	18
100	25	20	7	7	5	15	15	120	18,1	21
100	25	20	7	7	5	15	15	140	19	24
100	25	20	7	7	5	15	15	200	20,1	27

Fonte: O autor, 2023.

2.1.2 Formulário *online* (casos reais)

A fim de investigar os tipos de risco aos quais estão expostas as clínicas, mesmo em um universo extremamente reduzido, foi desenvolvido um questionário *online* em 1º de março de 2024. Este questionário foi elaborado com base nas Variáveis Linguísticas adotadas para o presente estudo, à luz da Lógica Fuzzy, e foi submetido a duas clínicas: uma na área de Medicina/Telemedicina e outra na área de Nutrição/Telenutrição.

Apesar de as respostas a este formulário serem completamente anônimas, a ferramenta escolhida foi o LimeSurvey, instalado em um servidor brasileiro. Essa decisão foi tomada com

o intuito de evitar transferências internacionais de dados. Optou-se pelo LimeSurvey em detrimento de ferramentas como o Google Forms, que poderiam implicar em tais transferências de dados.

O formulário foi intitulado de Pesquisa para Mestrado em Telessaúde da UERJ. Em termos de considerações, destacam-se:

As respostas para este questionário são anônimas e foram tratadas como tal.

a) Cada grupo de perguntas foi mostrado separadamente durante o preenchimento do questionário;
b) As respostas incluíram a data de envio para registro;
c) A URL de referência foi registrada para fins de rastreamento;
d) Os participantes tiveram a opção de salvar questionários parcialmente respondidos para continuação posterior;
e) Uma notificação básica por e-mail foi enviada para informar sobre o recebimento do questionário;
f) Uma notificação detalhada, contendo códigos do resultado, foi enviada por e-mail para os participantes.

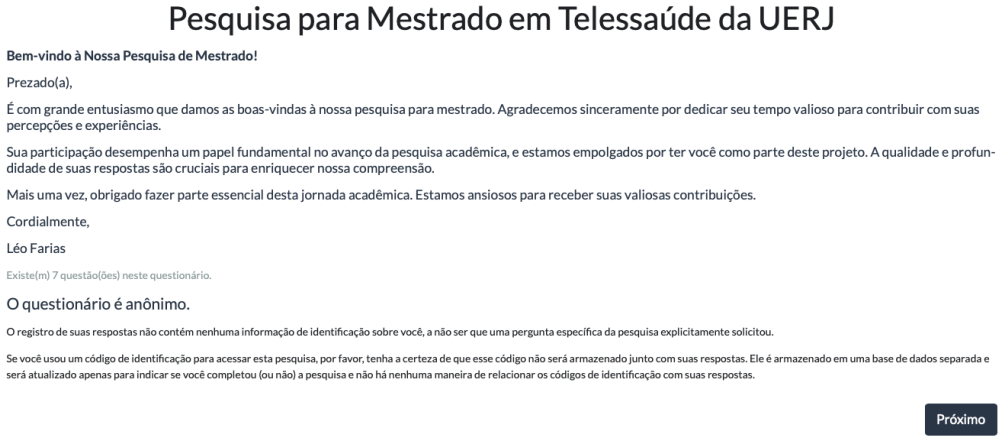
As perguntas adotadas para a pesquisa estão descritas, a seguir:

a) Esta pergunta visa compreender qual é o número de registros de pacientes considerados como Titulares que melhor representa a realidade da sua clínica, à luz da LGPD. Por favor, selecione a opção que mais se adequa à sua situação;
b) Esta pergunta está relacionada à infraestrutura de Tecnologia da Informação da clínica. Para o armazenamento dos dados tratados na clínica, incluindo, dados pessoais, dados pessoais sensíveis e dados comerciais, foi contratado algum serviço de armazenamento em nuvem?
c) Dados pessoais e dados pessoais sensíveis que estão armazenadas em nuvem, e os servidores desta nuvem está fisicamente instalado em outro país, é considerado, a luz da LGPD, como transferência internacional de dados pessoais e/ou dados pessoais sensíveis. Com base na infraestrutura desta clínica, qual é a faixa que melhor representa o percentual de dados pessoais e/ou dados pessoais sensíveis, em nuvem?

d) No contexto da LGPD, o tratamento de dados pessoais só poderá ser realizado caso seja adotada, formalmente, alguma das hipóteses legais de tratamento, previstas no Art. 7º e/ou Art. 11 desta Lei. Diferentes hipóteses podem ser adotadas para diferentes tratamentos de dados pessoais. Com base no exposto, qual ou quais das opções melhor reflete(m) a adoção de hipótese(s) por esta clínica?
e) Qual é o número aproximado de colaboradores e/ou terceiros que têm acesso às bases de dados da clínica?
f) Sobre a guarda dos dados pessoais e dados pessoais sensíveis nesta clínica, estes dados são armazenados por [...].

A Figura 11, a seguir, ilustra a tela inicial do formulário de pesquisa aplicado, para fins de investigação de riscos em clínicas da área da Saúde.

Figura 11 - Tela inicial do formulário *online* aplicado



Fonte: O autor, 2023.

As capturas de tela das telas do questionário e os resultados da pesquisa, através deste formulário *online*, estão disponíveis no Seção - Apêndice desta Dissertação.

2.1.3 Aplicação dos resultados dos casos reais ao modelo proposto

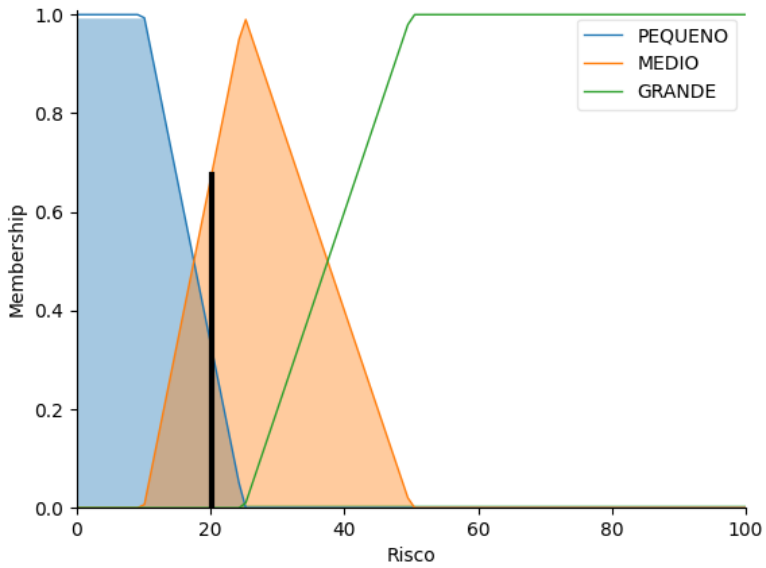
Tabela 14 - Comparação de resultados do formulário *online*

Parâmetros	Clínica de Nutrição	Clínica Médica
Número de titulares	100	100
Porcentagem de dados armazenados em nuvem	100%	100%
Porcentagem de dados armazenados internacionalmente	100%	100%
Porcentagem de dados armazenados fora do ciclo de vida	0%	60%
Porcentagem de dados pessoais sensíveis sem hipótese	0%	0%
Porcentagem de dados pessoais sem hipótese	0%	60%
Porcentagem de dados pessoais sensíveis com hipótese errada	0%	0%
Porcentagem de dados pessoais com hipótese errada	30%	20%
Número de pessoas com acesso a dados pessoais	2	1
Número de pessoas com acesso a dados pessoais sensíveis	1	1
Risco	20,1%	20,4%

Fonte: O autor, 2023.

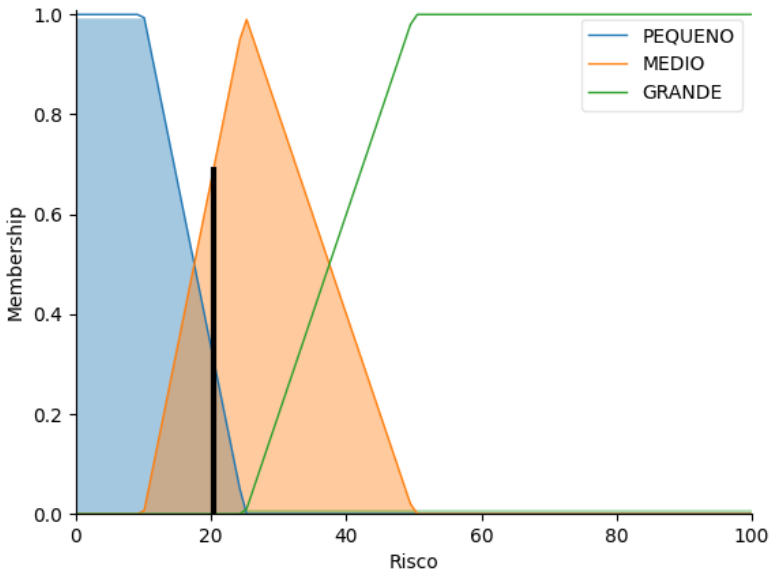
Os Gráficos 11 e 12 apresentados a seguir ilustram a Variável Linguística de Saída: Risco, como resultado da aplicação dos dados reais obtidos por meio do formulário ao modelo proposto nesta dissertação.

Gráfico 11 - Modelo da dissertação aplicado com caso real (Clínica de Nutrição)



Fonte: O autor, 2023.

Gráfico 12 - Modelo da dissertação aplicado com caso real (Clínica de Médica)



Fonte: O autor, 2023.

2.1.4 Aplicação dos resultados dos casos reais Modelo da SGD

Não foram identificadas equivalências diretas das perguntas do formulário para sua aplicação ao modelo da SGD.

3 DISCUSSÃO

Na literatura não há um modelo que englobe Lógica Fuzzy, Saúde Digital, Lei Geral de Proteção de Dados, Privacidade e Gestão de Riscos, o que acarreta que a proposta desta dissertação seja inovadora. O que há na literatura mais próximo desta proposta são os trabalhos correlatos apresentados na Seção 3.2 – Trabalhos Correlatos, comparados entre si, na Tabela 15, a seguir:

Tabela 15 - Comparação dos trabalhos correlatos e do modelo proposto

	Modelo Garibaldi	Fuzzy-DP (Attaullah)	Modelo SGD	Modelo Harth	Modelo Dissertação
GDPR	-	-	-	x	-
Lógica Fuzzy	x	x	-	x	x
Gestão de Riscos	x	x	x	x	x
Privacidade	-	x	x	x	x
LGPD	-	-	x	-	x
Saúde Digital	-	-	-	-	x

Fonte: O autor, 2023.

Sobre o Modelo da SGD, algumas normas adotadas para este modelo haviam sido canceladas e substituídas por versões mais recentes, com destaque para:

- ISO/IEC 31000:2009, de 13 de novembro de 2009;
- ABNT NBR ISO IEC 29100:2020, publicada em 27 de março de 2020.

Apesar de a norma ISO/IEC 31000:2009, citada pela SGD, para as definições dos termos probabilidade e impacto ter sido a norma ISO/IEC 31000:2009 e, não haver um limite no tempo de vida máximo de uma norma técnica, mesmo ao ser considerado a *ISO Systematic Review*, ao ser publicada uma nova revisão de uma norma, a anterior, é automaticamente revogada, ou seja, cancelada e substituída. No caso em pauta, a norma ISO/IEC 31000:2009 foi revogada em 14 de fevereiro de 2018, dando lugar à norma ISO/IEC 31000:2018 - *Risk management Principles and guidelines.* A versão desta norma foi adotada pelo Sistema de Conformidade Brasileiro em 28 de março de 2018 sob o título de ABNT NBR ISO 31000 - Gestão de Riscos - Diretrizes. A definição do termo probabilidade foi mantida. Contudo, o termo impacto, não. Para fins de registro, o tempo impacto:

- na norma ISO/IEC 31000:2009, foi definido como: "resultado de um evento que afeta os objetivos";
- na norma ABNT NBR ISO 31000:2018, o termo impacto foi substituído por consequência.

Os riscos considerados foram fundamentados na norma técnica ISO/IEC 29134:2017. A SGD adotou quatorze riscos para avaliação. Contudo, em 16 de novembro de 2020 foi publicada versão desta norma, em português, a norma ABNT NBR ISO/IEC 29134 - Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade - Diretrizes. Ainda sobre a norma técnica 29134, em 25 de março de 2023, foi publicada nova versão desta norma ISO/IEC 29134:2017 - *Information technology Security techniques Guidelines for privacy impact assessment*.

Após a publicação do Modelo de Avaliação de Riscos de Segurança e Privacidade até o momento atual, a ABNT NBR ISO/IEC 27002:2013 adotada foi substituída por versão mais recente, a ABNT NBR ISO/IEC 27002:2022, publicada em 05 de outubro de 2022.

Cumpre destacar que a ênfase atribuída às normas ISO/IEC e às ABNT NBR ISO/IEC nesta dissertação decorre da sua natureza como normas distintas, redigidas em idiomas diferentes, mas, crucialmente, apresentando conteúdo idêntico quando nos referimos à mesma revisão. Nas referências mencionadas neste trabalho, serão seguidas as diretrizes tanto da ISO quanto da ABNT. Nesse sentido, uma edição específica é identificada pela data de publicação, geralmente o ano. Quando apenas o título é mencionado, a referência é direcionada à versão mais recente da respectiva norma. Sendo assim, há diferenças nas citações, como exemplo, destaca-se que:

a) A ABNT NBR ISO/IEC 27002:2013 é diferente da ABNT NBR ISO/IEC 27002:2022;
b) A ISO/IEC 27002:2013 é diferente da ABNT NBR ISO/IEC 27002:2013;
c) A NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27002 e a ABNT NBR ISO/IEC 27002:2022 referem-se a mesma norma, já que a ABNT NBR ISO/IEC 27002:2022 é a mais atual.

A complexidade dos procedimentos de controle estabelecidos pelo modelo adotado pela SGD representa um desafio considerável para microempresas e profissionais liberais. Isso

ocorre devido à necessidade de conformidade com exigências normativas detalhadas, as quais requerem uma série de adaptações específicas. Além disso, o referido modelo não aborda aspectos mais específicos, como a contagem de registros de titulares, e consequentemente de dados pessoais, variáveis de grande relevância que deveriam ser objeto de avaliação minuciosa.

CONCLUSÃO

O objetivo deste trabalho foi avaliar a viabilidade do uso de um Sistema de Inferência Fuzzy para auxiliar na identificação do risco à privacidade dos dados pessoais de pacientes em um sistema dedicado à Saúde Digital. Os desvios-padrão e os erros médios da diferença entre os Riscos Obtidos e os Riscos Esperados demonstraram que o modelo conseguiu se comportar conforme o esperado, apresentando bom desempenho e precisão. Esses resultados sugerem a continuidade da exploração deste tópico sob a perspectiva da Lógica Fuzzy.

Mesmo diante da diversidade de ferramentas disponíveis para a conformidade com a LGPD, a conclusão deste estudo destaca a escassez de aplicações no mercado que se baseiam em sistemas de gestão ancorados em dados quantitativos e fundamentados na Lógica Fuzzy, a fim de substituir a lógica booleana. Atualmente, as aplicações são baseadas em controles de normas técnicas internacionais para garantir a confiabilidade de seus resultados. Nesse sentido, recomenda-se a incorporação de Modelos que adotam a Lógica Fuzzy e englobem sistemas de gestão padronizados, como o Sistema de Gestão da Qualidade, Sistema de Gestão de Riscos, Sistema de Gestão da Privacidade da Informação, Sistema de Gestão de Continuidade de Negócios e Sistema de Gestão de Segurança da Informação, dentre outros. Essa abordagem pode contribuir significativamente para a eficácia e a robustez das soluções desenvolvidas.

Urge que as organizações, tanto as desenvolvedoras de *softwares* quanto as em busca de conformidade com a LGPD, adotem as melhores práticas para o tratamento de dados pessoais e dados pessoais sensíveis e assegurem o respeito aos direitos dos titulares dos dados, incluindo crianças e adolescentes.

Cabe destacar como vantagem do modelo proposto nesta dissertação, o Modelo Fuzzy-LGPD para Gestão de Riscos na Saúde Digital, a questão da explicabilidade dos modelos baseados em Machine Learning está sendo cada vez mais exigida, ou seja, é um requisito mais do que desejável, já que as respostas precisam ser mais facilmente compreendidas pelas pessoas. E, neste caso, a Lógica Fuzzy atende a este requisito naturalmente, ou seja, de maneira intrínseca.

A implementação de um sistema abrangente que contempla as diversas fases de adequação à LGPD pode representar um investimento significativo. Soluções focadas unicamente no risco, e fundamentadas exclusivamente na probabilidade, como as oferecidas em iniciativas do Governo Digital, frequentemente demandam especialização em riscos e não são de manuseio intuitivo, em contraste com a solução proposta nesta dissertação. Com a evolução do sistema

aqui proposto, espera-se viabilizar a Gestão de Riscos para dados pessoais e sensíveis em sistemas digitais de saúde, dispensando a necessidade de o usuário possuir especialização em riscos ou na própria LGPD. A ferramenta desenvolvida promoverá uma interface autoexplicativa, permitindo ao usuário um entendimento claro das regras de IA empregadas na modelagem.

Em termos de conformidade com a LGPD, além da identificação e análise das hipóteses legais para o tratamento de dados, o sistema permitirá a incorporação de etapas adicionais, baseando-se nos requisitos e diretrizes estabelecidos por normativas reconhecidas, tais como:

a) ABNT NBR ISO/IEC 27557:2023 - Segurança da Informação, segurança cibernética e proteção da privacidade - Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional;
b) ABNT NBR ISO/ IEC 27001:2022 – Segurança da informação cibernética e proteção à privacidade – Sistemas de gestão de segurança da informação – Requisitos;
c) ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes;
d) ABNT NBR ISO 22301:2020 – Segurança e resiliência – Sistema de gestão de continuidade de negócios – Requisitos;
e) ISO 31700-1:2023(en) *Consumer protection – Privacy by design for consumer goods and services – Part 1: High-level requirements*;
f) ABNT NBR ISO/IEC 29100:2020 – Tecnologia da Informação - Técnicas de segurança - Estrutura de Privacidade;
g) ABNT NBR ISO 31022 – Gestão de Riscos - Diretrizes para a gestão de riscos legais;
h) ABNT NBR ISO 31000:2018 – Gestão de riscos – Diretrizes;
i) ISO/EC 27000:2018 – *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

Trabalhos Futuros

Nesta seção, delineiam-se possíveis direções e expansões do estudo atual que podem ser exploradas para aprofundar o entendimento e a aplicabilidade do sistema baseado em Lógica Fuzzy para a Gestão de Riscos à privacidade no contexto da Saúde Digital e da LGPD.

As pesquisas adicionais podem ser direcionadas para o refinamento e aprimoramento das funções de pertinência e das regras Fuzzy utilizadas no modelo. Isso pode incluir a integração de *feedbacks* de especialistas em proteção de dados e privacidade, bem como a inclusão de perspectivas de usuários finais dos sistemas de saúde digital. O objetivo seria melhorar a precisão e a eficiência do sistema em situações do mundo real, aumentando sua relevância prática e facilitando a adoção por parte das organizações.

Cumpre destacar que o desempenho do Sistema Fuzzy proposto pode ser otimizado considerando a consolidação das regras de modelagem com base em um número maior de especialistas, que definem a estratégia de inferência e que acarretarão a combinação dos antecedentes das regras, implicação e *modus ponens* mais assertivos.

A quantidade de controles deste modelo da SGD é um fator limitante para microempresas e profissionais liberais, já que ele leva em consideração normas técnicas que têm como requisitos uma série de adequações. Além disso, este modelo não faz avaliações de cunho mais específico como número de registros de titulares, que é uma característica importante de ser avaliadas. Contudo, é importante destacar que o modelo proposto nesta dissertação e o modelo da SGD pode ser considerados como modelos complementares, de modo a combinar as Lógicas Fuzzy e Booleana, e consequentemente, as variáveis linguísticas com os controles oriundos de normas técnicas.

Outro caminho promissor é a avaliação longitudinal do sistema implementado em diferentes contextos organizacionais. Isso permitiria observar a eficácia do sistema ao longo do tempo, avaliando sua capacidade de se adaptar a mudanças regulatórias, tecnológicas e de mercado. Estudos de caso detalhados poderiam ser realizados para entender melhor os impactos do sistema na redução de riscos de privacidade e na promoção da conformidade com a LGPD em variados ambientes de Saúde Digital.

Almeja-se a inclusão de outras variáveis linguísticas, a fim de aprimorar a eficácia do modelo proposto, desta vez, a partir de controles booleanos, como os adotados pela SGD para o seu modelo.

Além disso, o desenvolvimento de uma interface de usuário mais intuitiva e a integração com outras ferramentas de TI, como sistemas de gestão de saúde eletrônicos, poderiam ser explorados para aumentar a usabilidade e a integração do Sistema de Gestão de Riscos. Isso ajudaria a garantir que a solução possa ser facilmente implementada e utilizada por profissionais não especializados em riscos ou em legislação de proteção de dados.

Por fim, é vital explorar a intersecção entre a Lógica Fuzzy e as demais práticas emergentes de IA, como a aprendizagem profunda e o processamento de linguagem natural, para desenvolver sistemas ainda mais avançados de avaliação de risco. A inclusão dessas tecnologias pode proporcionar um Sistema de Gestão de Riscos mais dinâmico e adaptável, capaz de identificar e responder a novas ameaças à privacidade em tempo real.

Ao seguir essas direções, espera-se contribuir para a evolução contínua do campo da Gestão de Riscos de privacidade e para a adaptação das organizações às exigências da LGPD, promovendo um ecossistema de Saúde Digital mais seguro e confiável.

REFERÊNCIAS

ASSISTANT SECRETARY FOR PLANNING AND EVALUATION. ***Health Insurance Portability and Accountability Act of 1996***. Disponível em: https://aspe.hhs.gov/ reports/health-insurance-portability-accountability-act-1996. Acesso em: 25 mar. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000: Gestão de riscos - Diretrizes**. 28 mar. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 29100 - Tecnologia da Informação — Técnicas de segurança — Estrutura de Privacidade**. 27 mar. 2020a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31022 - Gestão de Riscos - Diretrizes para a gestão de riscos legais**. 18 dez. 2020b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001: Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos**. 23 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005 — Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação**. [s.l: s.n.].

ATTAULLAH, H. *et al*. ***Fuzzy-Logic-Based Privacy-Aware Dynamic Release of IoT-Enabled Healthcare Data***. IEEE Internet of Things Journal, v. 9, n. 6, p. 4411–4420, 15 mar. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD publica regulamento de aplicação de sanções administrativas**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria. Acesso em: 30 mar. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Resolução CD/ANDP n.º 4**. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 30 mar. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; ORTUNHO JUNIOR, W. G. **Enunciado CD/ANPD n.º 1, de 22 de maio de 2023**. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934. Acesso em: 15 jan. 2024.

BRASIL. **Decreto-Lei n.º 2.848**. Disponível em: https://www.planalto.gov.br/ccivil_03/ decreto-lei/del2848compilado.htm. Acesso em: 30 mar. 2023.

BRASIL. **Decreto-Lei n.º 3.688**. Disponível em: http://www.planalto.gov.br/ccivil_03/ decreto-lei/del3688.htm. Acesso em: 30 mar. 2023.

BRASIL. **Decreto-Lei n.º 4.657**. Disponível em: https://www.planalto.gov.br/ccivil_03/ decreto-lei/del4657.htm. Acesso em: 30 mar. 2023.
BRASIL. **Lei n.º 10.406**. Disponível em: https://www.planalto.gov.br/ccivil_03/ leis/2002/l10406compilada.htm. Acesso em: 30 mar. 2023.

BRASIL. **Decreto n.º 9.203**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 28 mar. 2023.

BRASIL. **Lei n.º 13.709**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 28 mar. 2023.

BRASIL. **Lei n.º 14.510**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm. Acesso em: 24 mar. 2023.

CAVOUKIAN, A. ***The 7 Foundational Principles***. Disponível em: www.privacybydesign.ca. Acesso em: 29 mar. 2023.

CAVOUKIAN, A. ***Understanding How to Implement Privacy by Design, One Step at a Time***. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8977606. Acesso em: 29 mar. 2023.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM n.º 1.931/09 - Código de Ética Médica**. Disponível em: https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf. Acesso em: 30 mar. 2023.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 2.314, de 20 de abril de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852. Acesso em: 25 mar. 2023a.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM n.º 2.314**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852. Acesso em: 30 mar. 2023b.

CONTROLADORIA-GERAL DA UNIÃO. **Metodologia de Gestão de Riscos**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/cgu_metodologia_gestao_riscos.pdf. Acesso em: 28 mar. 2023.
COX, E. Fuzzy fundamentals. 1992.

DEETJEN, U. et al. ***Digital Health @ Worldwebforum***. Disponível em: https://www.mckinsey.com/~/media/mckinsey/locations/europe%20and%20middle%20east/switzerland/our%20insights/worldwebforum/digital-health-at-worldwebforum.pdf. Acesso em: 25 mar. 2023.

DIAS, A. **Projeto de Lei n.º 1.164**. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8080168&ts=1630408547768&disposition=inline. Acesso em: 30 mar. 2023.
DINIZ, C. E. I. **A boa-fé objetiva no Direito Brasileiro e a Proibição de Comportamentos Contraditórios**. Disponível em: https://www.emerj.tjrj.jus.br/serieaperfeicoamentode magistrados/paginas/series/13/volumeI/10anosdocodigocivil_61.pdf. Acesso em: 30 mar. 2023.

DINIZ, D.; CORRÊA, M. Declaração de Helsinki: relativismo e vulnerabilidade. **Cadernos de Saúde Pública**, v. 17, n. 3, p. 679–688, 2001.

DOUGLAS, B. ***What Is Fuzzy Logic?*** Disponível em: https://www.youtube.com/watch?v=__0nZuG4sTw. Acesso em: 31 mar. 2023.

DUBOIS, D.; PRADE, H. M. ***Fuzzy Sets and Systems: Theory and Applications (Mathematics in science and engineering)***. [s.l.] Academic Press, 1980. v. 144.

FAKHRAVAR, H. **Quantifying Uncertainty In Risk Assessment Using Fuzzy Theory**. [s.l: s.n.].

FERNANDES, L. G. **Elementos Sintáticos e Semânticos**. [s.d.].

FRIEDE, R. **Teoria da Norma Jurídica**. Disponível em: https://www.mprj. mp.br/documents/20184/2490901/Reis%20Friede.pdf. Acesso em: 30 mar. 2023.

GARIBALDI, J. M. **The Need for Fuzzy AI**. [s.l: s.n.]. Disponível em: https://en.wikipedia.org/wiki/Turn.

GHOOL, R. B. **The Nuremberg Code - A critique**. Disponível em: www.picronline.org. Acesso em: 30 mar. 2023.

GOVERNO DIGITAL. **Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 30 mar. 2023.

GOVERNO DIGITAL; MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. **Guias e modelos**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao -de-dados-pessoais-lgpd. Acesso em: 2 abr. 2023.

GUILLAUME, S. Designing Fuzzy Inference Systems from Data: An Interpretability - Oriented Review. **IEEE Transactions on Fuzzy Systems**, v. 9, n. 3, 2001.

HARTH, S.; FERRARA, A. L.; PACI, F. ***Fuzzy-based Approach to Assess and Prioritize Privacy Risks***. 2020.

HELTON, T. **A importância do princípio da boa-fé na prática da advocacia**. Disponível em: https://www.aurum.com.br/blog/principio-da-boa-fe/. Acesso em: 30 mar. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ***ISO IEC 27005 2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks***. 25 out. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ***ISO 31700-1:2023(en) Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements***. 31 jan. 2023.

JANDOO, T. ***WHO guidance for digital health: What it means for researchers***. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6952850/pdf/10.1177_2055207619898984.pdf. Acesso em: 25 mar. 2023.

KLEE, A. E. L.; PEREIRA NETO, A. N. **Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica**. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 30 mar. 2023.

KLIR, G. J.; YUAN, B. O. ***Fuzzy sets and Fuzzy logic: Theory and Applications***. 1995.

KOSKO, B. **Fuzzy Engineering**. [s.l.] Prentice Hall, 1996.

LIAO, Y.; MA, C.; ZHANG, C. ***A New Fuzzy Risk Assessment Method for the Network Security Based on Fuzzy Similarity Measure***; 2006 6th World Congress on Intelligent Control and Automation, v. 2, 2006.

LUZ, J. C. J. **A Abordagem baseada no risco para a conformidade com a LGPD**. Disponível em: https://www.conjur.com.br/2022-jan-05/jean-luz-abordagem-baseada-risco-conformidade -lgpd. Acesso em: 28 mar. 2023.

MALDOFF, G. **The Risk-Based Approach in the GDPR: Interpretation and Implications**. Disponível em: https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/. Acesso em: 25 mar. 2023.

MARRO, A. A. et al. Lógica Fuzzy: Conceitos e aplicações. [s.d.].

MATPLOTLIB. **mplot3d Tutorial — Matplotlib 2.0.2 documentation**. Disponível em: https://matplotlib.org/2.0.2/mpl_toolkits/mplot3d/tutorial.html#. Acesso em: 30 mar. 2024.

MINISTÉRIO DA ECONOMIA. Secretaria de Governo Digital. Guia de Avaliação de Riscos de Segurança e Privacidade. nov. 2020.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS; GOVERNO DIGITAL. **Gestão de riscos**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/gestao-riscos. Acesso em: 28 mar. 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **MJ apresenta nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais**. Disponível em: https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais. Acesso em: 30 mar. 2023.

MINISTÉRIO DA SAÚDE. **Saúde Digital**. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-digital. Acesso em: 25 mar. 2023.

NAÇÕES UNIDAS. **Declaração dos Direitos Humanos das Nações Unidas**. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em: 29 mar. 2023.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. ***A Health Telematics Policy in support of WHO's Health-for-All Strategy for Global Health Development (WHO/DGO/98.1)***. Geneva: [s.n.]. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/63857/WHO_DGO_98.1. pdf?sequence=1&isAllowed=y. Acesso em: 24 mar. 2023.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **WHA58.28 - eHealth**. [s.l: s.n.]. Disponível em: https://apps.who.int/gb/ebwha/pdf_files/WHA58/WHA58_28-en.pdf. Acesso em: 25 mar. 2023.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Classification of Digital Health Interventions v 1.0**. [s.l: s.n.]. Disponível em: http://who.int/reproductivehealth/topics/mhealth/en/.. Acesso em: 25 mar. 2023.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Global strategy on digital health 2020-2025**. [s.l: s.n.]. Disponível em: http://apps.who.int/bookorders.. Acesso em: 25 mar. 2023a.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **Recommendations on digital interventions for health system strengthening**. [s.l: s.n.]. Disponível em: https://www.who.int/publications/i/item/9789241550505. Acesso em: 25 mar. 2023b.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. **The protection of personal data in health information systems-principles and processes for public health**. [s.l: s.n.]. Disponível em: https://apps.who.int/iris/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf?sequence=1&isAllowed=y. Acesso em: 28 mar. 2023.

ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE. **A Telemedicina e a Telessaúde embarcadas no ecossistema de Saúde Digital**. Disponível em: https://www.paho.org/pt/information-systems-health-is4h-blog/telemedicina-e-telessaude-embarcadas-no-ecossistema-saude. Acesso em: 25 mar. 2023.

PARLAMENTO EUROPEU; CONSELHO. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=EN. Acesso em: 25 mar. 2023.

PARLAMENTO EUROPEU; CONSELHO. **General Data Protection Regulation**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 25 mar. 2023.

PLAZZOTTA, F.; SOMMER, J. **Telemedicina: Diseño y ejecución en sistemas de información en salud**. 1ª Edição ed. Buenos Aires: Hospital Italiano de Buenos Aires, 2020.

PRIVACY INTERNATIONAL. **What Is Privacy?** Disponível em: https://privacyinternational.org/explainer/56/what-privacy. Acesso em: 1 abr. 2023.

PUBMED. **Telemedicine**. Disponível em: https://pubmed.ncbi.nlm.nih.gov/?term= telemedicine&sort=. Acesso em: 22 mar. 2024.

RAZAVISOUSAN, R.; JOSHI, K. P. ***Analyzing GDPR compliance in Cloud Services' privacy policies using Textual Fuzzy Interpretive Structural Modeling (TFISM)***. [s.l: s.n.].

SAMANI, B. A.; SHAHBODAGHLOU, F. **A Fuzzy Systematic Approach to Construction Risk Analysis**. [s.l: s.n.].

SANTOS, L. **Governo quer mais proteção de dados na internet**. Disponível em: https://www.conjur.com.br/2011-jan-25/consulta-publica-traca-diretrizes-lei-protecao-dados-pessoais. Acesso em: 26 mar. 2023.

SCIENTIFIC AMERICAN. ***What is "Fuzzy Logic"? Are there computers that are inherently Fuzzy and do not apply the usual binary logic?*** Disponível em: https://www.scientificamerican.com/article/what-is-fuzzy-logic-are-t/. Acesso em: 30 mar. 2023.

SEBRAE. **POC (Proof of Concept): o que é e por que é importante para softwares**. Disponível em: https://inovacaosebraeminas.com.br/artigo/poc-proof-of-concept. Acesso em: 31 mar. 2024.

SECRETARIA DE ESTADO DA SAÚDE; GOVERNO DO ESTADO DE SÃO PAULO. **Perguntas e respostas: tire suas dúvidas sobre o novo coronavírus**. Disponível em: http://www.saude.sp.gov.br/ses/perfil/cidadao/homepage/destaques/perguntas-e-respostas-tire-suas-duvidas-sobre-o-novo-coronavirus. Acesso em: 24 mar. 2023.

SEDLMAIER, C. E.; HERNANDEZ, D. P. **Origens do Consentimento Informado na prática clínica do Médico e sua importância na Bioética**. Disponível em: https://www.unifeso.edu.br/revista/index.php/medicinafamiliasaudemental/article/view/1576. Acesso em: 30 mar. 2023.

SHANG, K.; HOSSEN, Z. ***Applying Fuzzy Logic to Risk Assessment and Decision-Making Sponsored by CAS/CIA/SOA Joint Risk Management Section***. [s.l: s.n.].

SHAW, T. et al. ***What is eHealth? Development of a Conceptual Model for eHealth: Qualitative Study with Key Informants***. Disponível em: http://www.jmir.org/2017/10/e324/. Acesso em: 25 mar. 2023.

SILVA, F. Desvendando a Lógica Fuzzy. 2011.

SOLOMON, H. ***Privacy by Design to become an ISO standard next month***. Disponível em: https://www.itworldcanada.com/article/privacy-by-design-to-become-an-iso-standard-next-month/521415. Acesso em: 29 mar. 2023.

SOMBRA, T. L. **GDPR e proteção de dados pessoais: uma agenda também brasileira**. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/gdpr-agenda-brasileira-25052018. Acesso em: 30 mar. 2023.

SOUZA, M. K. et al. Termo de consentimento livre e esclarecido (TCLE): fatores que interferem na adesão. **ABCD. Arquivos Brasileiros de Cirurgia Digestiva (São Paulo)**, v. 26, n. 3, p. 200–205, set. 2013.

TANSCHEIT, R. **Fundamentos da Lógica Fuzzy e Controle Fuzzy**. 2001.

TANSCHEIT, R. **Sistemas Fuzzy**. Acesso em: 1 abr. 2023.

VADE MECUM BRASIL. ***Dura Lex Sed Lex***. Disponível em: https://vademecumbrasil.com.br/palavra/dura-lex-sed-lex. Acesso em: 30 mar. 2023.

WARREN, S. D.; BRANDEIS, L. D. **The Right to Privacy**. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em: 28 mar. 2023.

ZADEH, L. A. Fuzzy sets. **Information and Control**, v. 8, n. 3, p. 338–353, 1965.

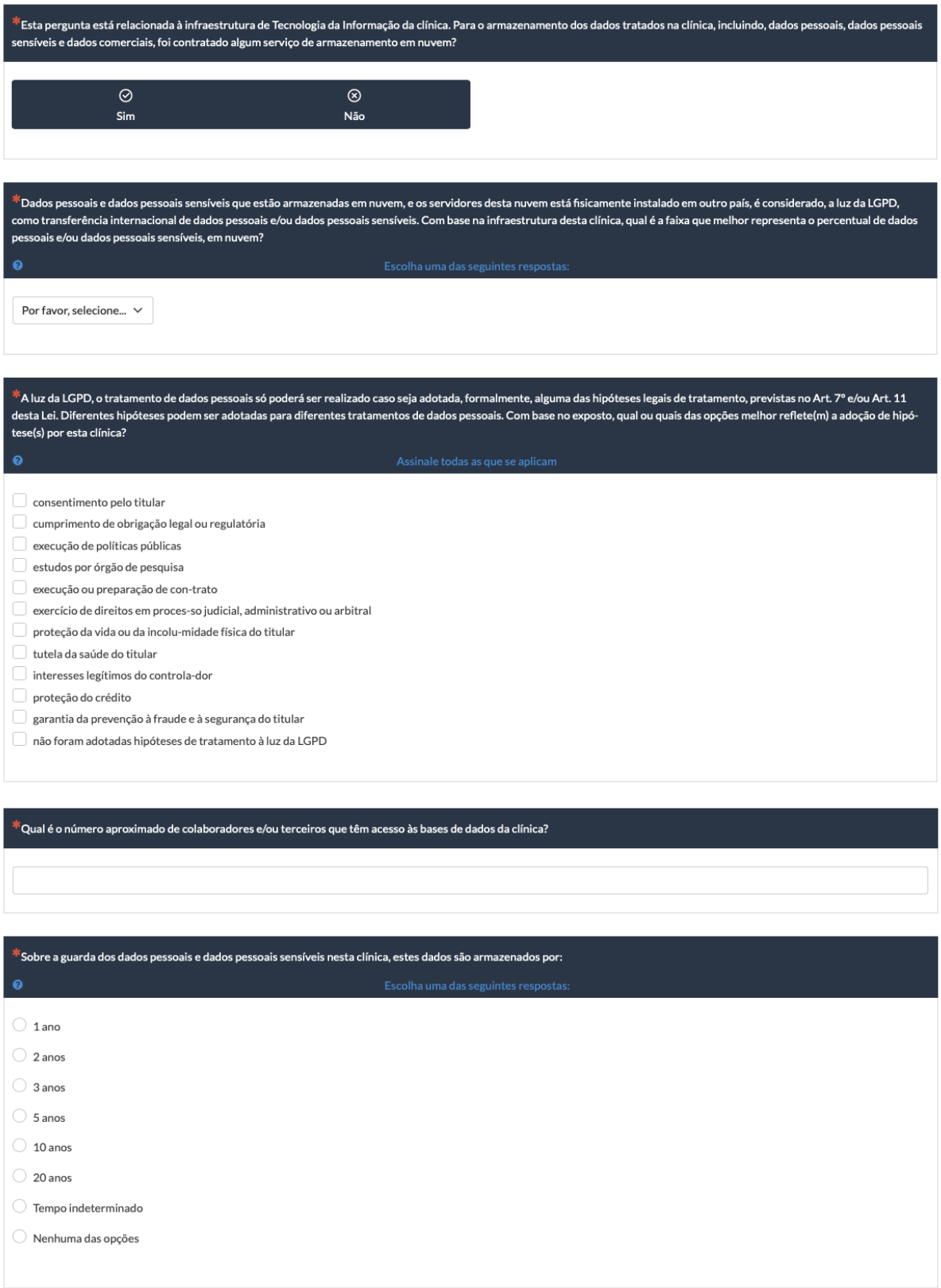
ZADEH, L. A. ***A Summary and Update of "Fuzzy Logic".*** *2010 IEEE International Conference on Granular Computing*, 2010.

APÊNDICE - Figuras do Formulário de Pesquisa *online*

Figura 12 - Inicio do questionário: parte I

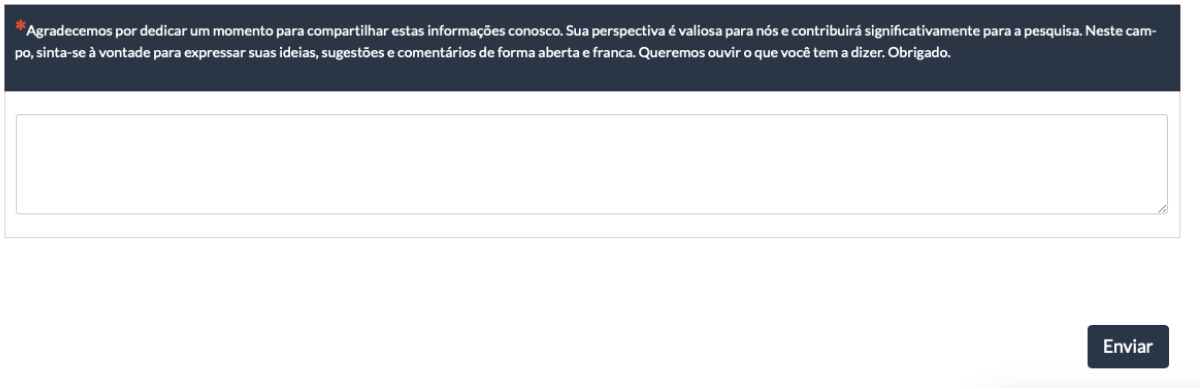
Fonte: O autor, 2023.

Figura 13 - Início do questionário: parte II



Fonte: O autor, 2023.

Figura 14 - Início do questionário: parte III



Fonte: O autor, 2023.

Regras de Inferência Fuzzy

Para a modelagem das regras do método de inferência, foram utilizadas apenas as operações clássicas AND e OR, E e OU respectivamente, de Zadeh. Onde no total foram produzidas 72 (setenta e duas) regras de inferência Fuzzy, apresentadas a seguir:

1. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "PEQUENO" THEN Risco IS "PEQUENO"

2. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "MÉDIO" THEN Risco IS "MÉDIO"

3. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "GRANDE" THEN Risco IS "GRANDE"

4. IF Número de pessoas IS "MÉDIO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "PEQUENO" THEN Risco IS "MÉDIO"

5. IF Número de pessoas IS "MÉDIO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "MÉDIO" THEN Risco IS "MÉDIO"

6. IF Número de pessoas IS "MÉDIO" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "GRANDE" THEN Risco IS "GRANDE"

7. IF Número de pessoas IS "GRANDE" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "PEQUENO" THEN Risco IS "GRANDE"

8. IF Número de pessoas IS "GRANDE" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "MÉDIO" THEN Risco IS "GRANDE"

9. IF Número de pessoas IS "GRANDE" AND Porcentagem de dados pessoais sensíveis com hipótese errada IS "GRANDE" THEN Risco IS "GRANDE"

10. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis sem hipótese IS "PEQUENO" THEN Risco IS "PEQUENO"

11. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis sem hipótese IS "MÉDIO" THEN Risco IS "MÉDIO"

12. IF Número de pessoas IS "PEQUENO" AND Porcentagem de dados pessoais sensíveis sem hipótese IS "GRANDE" THEN Risco IS "GRANDE"

13. IF Número de pessoas IS "MÉDIO" AND Porcentagem de dados pessoais sensíveis sem hipótese IS "PEQUENO" THEN Risco IS "MÉDIO"

14. IF Número de pessoas IS "MÉDIO" AND Porcentagem de dados pessoais sensíveis sem hipótese IS "MÉDIO" THEN Risco IS "MÉDIO"

15. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais sensíveis sem hipótese IS “GRANDE” THEN Risco IS “GRANDE”

16. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sensíveis sem hipótese IS “PEQUENO” THEN Risco IS “GRANDE”

17. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sensíveis sem hipótese IS “MÉDIO” THEN Risco IS “GRANDE”

18. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sensíveis sem hipótese IS “GRANDE” THEN Risco IS “GRANDE”

19. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais sem hipótese IS “PEQUENO” THEN Risco IS “PEQUENO”

20. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais sem hipótese IS “MÉDIO” THEN Risco IS “PEQUENO”

21. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais sem hipótese IS “GRANDE” THEN Risco IS “MÉDIO”

22. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais sem hipótese IS “PEQUENO” THEN Risco IS “PEQUENO”

23. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais sem hipótese IS “MÉDIO” THEN Risco IS “MÉDIO”

24. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais sem hipótese IS “GRANDE” THEN Risco IS “GRANDE”

25. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sem hipótese IS “PEQUENO” THEN Risco IS “MÉDIO”

26. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sem hipótese IS “MÉDIO” THEN Risco IS “GRANDE”

27. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais sem hipótese IS “GRANDE” THEN Risco IS “GRANDE”

28. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais com hipótese errada IS “PEQUENO” THEN Risco IS “PEQUENO”

29. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais com hipótese errada IS “MÉDIO” THEN Risco IS “PEQUENO”

30. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados pessoais com hipótese errada IS “GRANDE” THEN Risco IS “MÉDIO”

31. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais com hipótese errada IS “PEQUENO” THEN Risco IS “PEQUENO”

32. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais com hipótese errada IS “MÉDIO” THEN Risco IS “MÉDIO”

33. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados pessoais com hipótese errada IS “GRANDE” THEN Risco IS “GRANDE”

34. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais com hipótese errada IS “PEQUENO” THEN Risco IS “MÉDIO”

35. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais com hipótese errada IS “MÉDIO” THEN Risco IS “GRANDE”

36. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados pessoais com hipótese errada IS “GRANDE” THEN Risco IS “GRANDE”

37. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados internacionalmente IS “PEQUENO” THEN Risco IS “PEQUENO”

38. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados internacionalmente IS “MÉDIO” THEN Risco IS “PEQUENO”

39. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados internacionalmente IS “GRANDE” THEN Risco IS “MÉDIO”

40. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados internacionalmente IS “PEQUENO” THEN Risco IS “PEQUENO”

41. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados internacionalmente IS “MÉDIO” THEN Risco IS “MÉDIO”

42. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados internacionalmente IS “GRANDE” THEN Risco IS “MÉDIO”

43. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados internacionalmente IS “PEQUENO” THEN Risco IS “MÉDIO”

44. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados internacionalmente IS “MÉDIO” THEN Risco IS “MÉDIO”

45. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados internacionalmente IS “GRANDE” THEN Risco IS “GRANDE”

46. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “PEQUENO” THEN Risco IS “PEQUENO”

47. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “MÉDIO” THEN Risco IS “MÉDIO”

48. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “GRANDE” THEN Risco IS “GRANDE”

49. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “PEQUENO” THEN Risco IS “MÉDIO”

50. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “MÉDIO” THEN Risco IS “GRANDE”

51. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “GRANDE” THEN Risco IS “GRANDE”

52. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “PEQUENO” THEN Risco IS “MÉDIO”

53. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “MÉDIO” THEN Risco IS “GRANDE”

54. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais sensíveis IS “GRANDE” THEN Risco IS “GRANDE”

55. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais IS “PEQUENO” THEN Risco IS “PEQUENO”

56. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais IS “MÉDIO” THEN Risco IS “PEQUENO”

57. IF Número de pessoas IS “PEQUENO” AND Número de pessoas IS com acesso a dados pessoais IS “GRANDE” THEN Risco IS “MÉDIO”

58. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais IS “PEQUENO” THEN Risco IS “MÉDIO”

59. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais IS “MÉDIO” THEN Risco IS “MÉDIO”

60. IF Número de pessoas IS “MÉDIO” AND Número de pessoas IS com acesso a dados pessoais IS “GRANDE” THEN Risco IS “GRANDE”

61. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais IS “PEQUENO” THEN Risco IS “MÉDIO”

62. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais IS “MÉDIO” THEN Risco IS “GRANDE”

63. IF Número de pessoas IS “GRANDE” AND Número de pessoas IS com acesso a dados pessoais IS “GRANDE” THEN Risco IS “GRANDE”

64. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “PEQUENO” THEN Risco IS “PEQUENO”

65. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “MÉDIO” THEN Risco IS “PEQUENO”

66. IF Número de pessoas IS “PEQUENO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “GRANDE” THEN Risco IS “MÉDIO”

67. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “PEQUENO” THEN Risco IS “PEQUENO”

68. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “MÉDIO” THEN Risco IS “MÉDIO”

69. IF Número de pessoas IS “MÉDIO” AND Porcentagem de dados armazenados fora do ciclo de vida IS “GRANDE” THEN Risco IS “MÉDIO”

70. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados fora do ciclo de vida IS “PEQUENO” THEN Risco IS “MÉDIO”

71. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados fora do ciclo de vida IS “MÉDIO” THEN Risco IS “GRANDE”

72. IF Número de pessoas IS “GRANDE” AND Porcentagem de dados armazenados fora do ciclo de vida IS “GRANDE” THEN Risco IS “GRANDE”

Exemplo de aplicação

Na elaboração desta dissertação, um exemplo prático foi empregado para ilustrar a aplicação de um Sistema de Inferência Fuzzy. Este exemplo focaliza a determinação do percentual adequado de gorjeta a ser pago, levando em conta dois fatores críticos: a qualidade da comida e a qualidade do serviço.

A análise detalhada e o entendimento deste exemplo são fundamentais, pois fornecem uma base sólida para a compreensão das metodologias e abordagens discutidas na Subseção 3.3 - Metodologia. A exploração deste exemplo prático não só facilita a compreensão dos conceitos teóricos subjacentes aos Sistemas de Inferência Fuzzy, mas também demonstra a aplicabilidade prática destes sistemas na resolução de problemas do mundo real, particularmente na otimização da tomada de decisão em situações que envolvem variáveis qualitativas e quantitativas.

Neste exemplo, foram consideradas três etapas: Fuzzificação, Inferência e Defuzzificação.

Fuzzificação: duas variáveis linguísticas de entrada - Entradas Precisas (*Crisp inputs*) a partir de um universo de discurso de 0 até 10 e de respectivos rótulos, a saber:

- Variável Linguística: Qualidade da Comida: "*ruim*", "*boa*", "*saborosa*";
- Variável Linguística: Qualidade do Serviço: "*ruim*", "*aceitável*", "*ótimo*".

A Figura 15 apresenta uma ilustração das variáveis linguísticas mencionadas, ou seja, a Qualidade da Comida e a Qualidade do Serviço. Os valores 7 e 8 ilustrados, serão abordados nos texto subsequente.

Figura 15 - Variáveis Linguísticas do Exemplo: Qualidade da Comida e do Serviço

Fonte: O autor, 2023.

Na abordagem de Fuzzificação aplicada ao presente estudo, foram consideradas as duas variáveis linguísticas supracitadas, ambas representando entradas precisas (*Crisp inputs*) em um universo de discurso que varia de 0 a 10.

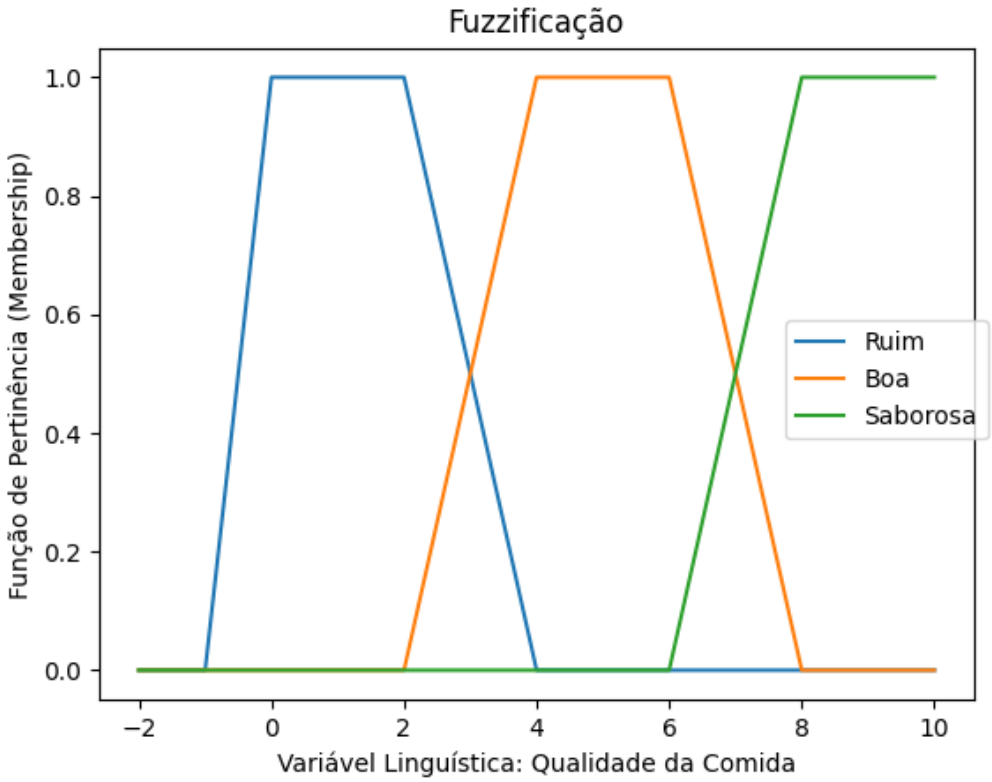
As representações gráficas subsequentes demonstram o comportamento destas variáveis linguísticas e os seus respectivos graus de pertinência.

O Gráfico 11, a seguir, apresenta a função de pertinência trapezoidal, que é utilizada para traduzir o valor numérico da variável de entrada Qualidade da Comida, sete (7). Através da aplicação dessa função, obtemos os seguintes graus de associação:

- para o rótulo "*ruim"*, o grau de pertinência é 0, indicando que um valor de entrada de sete não está associado à qualidade "*ruim"* da comida;
- para o rótulo "*boa"*, o grau de pertinência é de 0,55, demonstrando uma associação moderada a alta com o conceito de "boa";
- para o rótulo "*saborosa"*, o grau de pertinência é de 0,45, sugerindo uma associação também significativa com esse conceito, embora ligeiramente inferior à associação com "*boa"*.

Esses valores refletem a interpretação Fuzzy dos dados numéricos e permitem uma análise do que seria possível com uma avaliação binária ou categórica estrita.

Gráfico 13 - Exemplo: Variável linguística: Qualidade da Comida



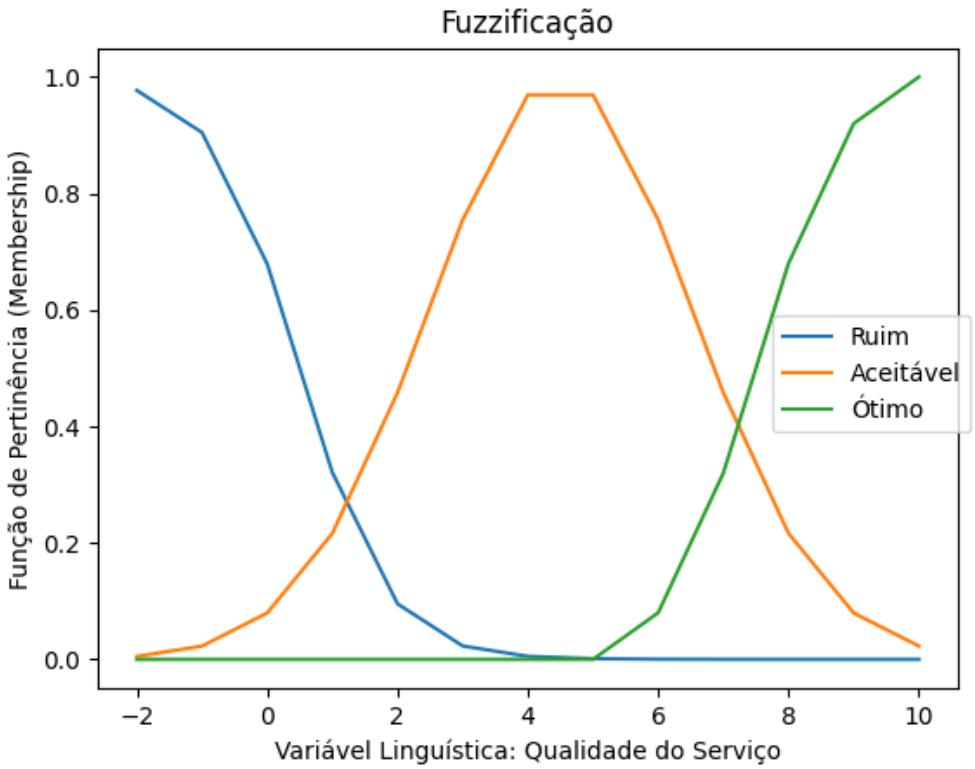
Fonte: O autor, 2023.

Já o Gráfico 12 ilustra a interpretação dos dados que é feita por meio de outra função de pertinência, no caso, a Sigmoide. Contudo, poderiam ser utilizadas outras funções de pertinência, como, por exemplo, as funções Gaussiana e Pi, para modelar a variável de entrada Qualidade do Serviço com um valor numérico de oito (8). Com base nessa modelagem, a função Sigmoide pode ser utilizada para representar transições suaves entre os graus de pertinência, enquanto a Gaussiana modela a pertinência em torno de um ponto central, e a Função Pi, no contexto de Conjuntos Fuzzy, é uma função de pertinência caracterizada por uma combinação de duas funções sigmoides, uma ascendente e outra descendente.

Para o rótulo "*ruim"*, o grau de pertinência é zero (0), refletindo a inexistência de associação entre um serviço classificado com o valor oito e a qualificação de "*ruim"*. Para o rótulo "*aceitável*", a função atribui um grau de pertinência de 0,2, indicando uma baixa associação

com este nível de serviço, considerado acima do mediano. Por fim, o rótulo “ótimo” recebe um grau de pertinência de 0,7, o que indica uma forte associação com o valor de entrada, sugerindo que um serviço avaliado com o valor oito é predominantemente percebido como “*ótimo”*. Este Modelo Fuzzy permite uma compreensão mais detalhada e diferenciada das percepções dos clientes sobre o serviço prestado.

Gráfico 14 - Exemplo: Variável linguística: Qualidade do Serviço



Fonte: O autor, 2023.

Para a elaboração dos gráficos correspondentes às Figuras foram utilizados dois ambientes de desenvolvimento: o Microsoft Visual Studio Code, conhecido com VS Code e o Google Colab Research, conhecido popularmente como Colab. Este último é um ambiente virtual baseado em nuvem para a execução de códigos escritos em Python, linguagem de programação adotada para o presente estudo, acessível por meio de um navegador web (*browser*). Esta plataforma é uma ferramenta de pesquisa desenvolvida pela empresa Google, que permite a escrita, execução e compartilhamento de códigos Python de forma colaborativa, além de fornecer acesso gratuito a recursos computacionais avançados.

Os gráficos foram gerados utilizando-se bibliotecas de visualização de dados da linguagem Python, que são amplamente reconhecidas por suas funções robustas e flexibilidade. Entre elas, destacam-se Matplotlib, Scikit-Fuzzy e Seaborn, que proporcionam uma gama de funcionalidades para a criação de representações gráficas estatísticas complexas. Essas ferramentas são particularmente adequadas para a modelagem de funções de pertinência empregadas em Sistemas Fuzzy, possibilitando uma interpretação visual precisa das relações e dos graus de pertinência definidos para as variáveis linguísticas em questão.

A Figura 16, apresentada a seguir, contém o código-fonte, escrito na linguagem de programação Python utilizando as bibliotecas NumPy, Scikit-Fuzzy e Matplotlib para realização das análises do Sistema Fuzzy e para a geração dos gráficos mencionados, exemplificando a aplicação prática de conceitos teóricos de Lógica Fuzzy.

Figura 16 - Código-fonte escrito em Python para geração de gráficos

Fuzzy Too.py 1

```python
import numpy as np
import skfuzzy as fuzz
import matplotlib.pyplot as plt

# Criando as variáveis do problema
food_quality = np.arange(-2, 11, 1)
service_quality = np.arange(-2, 11, 1)

# Criando as funções de pertinência para Food Quality
food_ruim = fuzz.trapmf(food_quality, [0, 0, 2, 4])
food_boa = fuzz.trapmf(food_quality, [2, 4, 6, 8])
food_saborosa = fuzz.trapmf(food_quality, [6, 8, 10, 10])

# Criando as funções de pertinência para Service Quality
service_ruim = fuzz.sigmf(service_quality, 0.5, -1.5)
service_aceitavel = fuzz.gaussmf(service_quality, 4.5, 2)
service_otimo = fuzz.pimf(service_quality, 5, 10, 11, 11)

# Visualizando as funções de pertinência para cada variável
plt.figure()

plt.plot(food_quality, food_ruim, 'b', linewidth=1.5, label='Ruim')
plt.plot(food_quality, food_boa, 'g', linewidth=1.5, label='Boa')
plt.plot(food_quality, food_saborosa, 'r', linewidth=1.5, label='Saborosa')
plt.title('Qualidade da Comida')
plt.legend()

plt.figure()

plt.plot(service_quality, service_ruim, 'b', linewidth=1.5, label='Ruim')
plt.plot(service_quality, service_aceitavel, 'g', linewidth=1.5, label='Aceitável')
plt.plot(service_quality, service_otimo, 'r', linewidth=1.5, label='Ótimo')
plt.title('Qualidade do Serviço')
plt.legend()

plt.show()
```

Fonte: O autor, 2023.

Na construção do Modelo de Inferência Fuzzy para o presente estudo, optou-se pela aplicação exclusiva das operações clássicas propostas por Zadeh. A estruturação das regras de

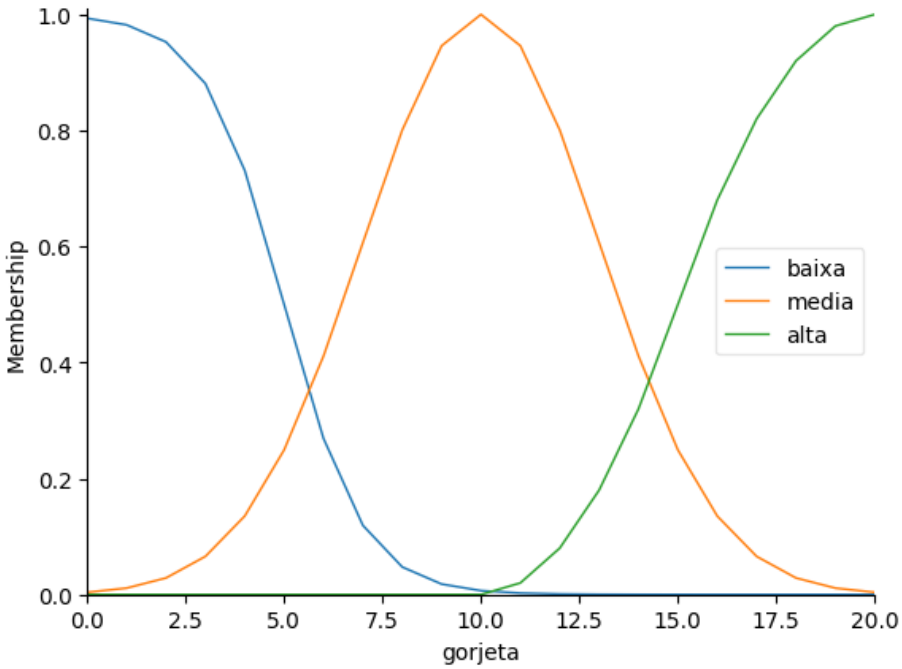
inferência é uma etapa crítica na definição do comportamento do Sistema Fuzzy e, neste caso, foram estabelecidas três regras fundamentais para a dedução da quantidade de gorjeta a ser oferecida, com base na qualidade do serviço e da comida. As Regras de Inferência Fuzzy adotadas são detalhadas a seguir:

1. A primeira regra estabelece que, se o serviço for classificado como *'ruim'* OU a comida for classificada como *'ruim'*, então a gorjeta atribuída deve ser *'baixa'*. Esta é representada pela equação de inferência que toma o valor máximo entre os graus de pertinência para *'serviço ruim'* e *'comida ruim'*. Matematicamente, é expressa por: *baixa* = max(*serviço ruim, comida ruim*). Com os graus de pertinência atribuídos sendo ambos zero, o resultado calculado é: *baixa* = max(*0, 0*) = *0*;
2. A segunda regra determina que se o serviço for considerado *'aceitável'*, então a gorjeta correspondente deve ser *'média'*. A operação de inferência é direta e reflete o grau de pertinência para *'serviço aceitável'*, resultando em:
   média = aceitável
   média = 0,20;
3. A terceira e última regra propõe que se o serviço for *'ótimo'* OU a comida for *'saborosa'*, então a gorjeta deve ser *'alta'*. A inferência é feita pelo valor máximo entre os graus de pertinência para *'serviço ótimo'* e *'comida saborosa'*, como segue: *alta* = max(*serviço ótimo, comida saborosa*). Com base nos valores de pertinência dados, tem-se: *alta* = max(*0,20, 0,70*) = *0,70*.

Essas regras são implementadas dentro do Sistema Fuzzy para automatizar o processo de decisão relativo à gorjeta, oferecendo uma solução que considera a qualidade percebida tanto do serviço quanto da comida de maneira integrada.

O Gráfico 13, a seguir, representa as funções de pertinência obtidas para a gorjeta.

Gráfico 15 - Exemplo: Funções de pertinência

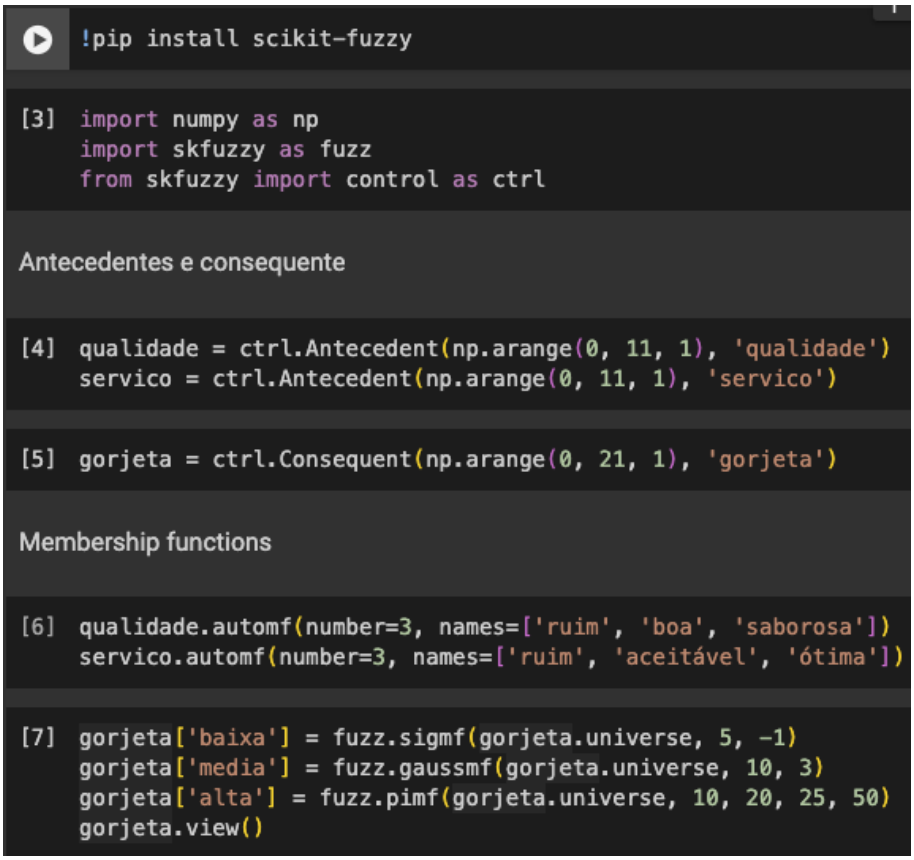


Fonte: O autor, 2023.

Inserida na metodologia deste estudo, a Fase de Modelagem Fuzzy englobou a definição das antecedentes (ou premissas), do consequente (ou conclusão) e das respectivas funções de pertinência. Esta etapa culminou na elaboração do Gráfico 3, que sintetiza a relação entre as variáveis de entrada e de saída dentro do Sistema de Inferência Fuzzy proposto. A construção desse gráfico foi viabilizada pela execução de um código, cujos detalhes são ilustrados na Figura 17.

A utilização da linguagem Python para este propósito fundamenta-se na sua robustez e na diversidade de bibliotecas científicas disponíveis, como NumPy, para manipulação de *arrays* numéricos, e Matplotlib, para a geração de gráficos. Essas ferramentas, associadas à sintaxe clara e concisa de Python, permitem a modelagem eficiente dos Sistemas Fuzzy e a correspondente visualização dos processos de inferência, essenciais para a validação e interpretação dos resultados obtidos através do modelo.

Figura 17 - Funções de Pertinência



```
!pip install scikit-fuzzy
```

```
[3] import numpy as np
    import skfuzzy as fuzz
    from skfuzzy import control as ctrl
```

Antecedentes e consequente

```
[4] qualidade = ctrl.Antecedent(np.arange(0, 11, 1), 'qualidade')
    servico = ctrl.Antecedent(np.arange(0, 11, 1), 'servico')
```

```
[5] gorjeta = ctrl.Consequent(np.arange(0, 21, 1), 'gorjeta')
```

Membership functions

```
[6] qualidade.automf(number=3, names=['ruim', 'boa', 'saborosa'])
    servico.automf(number=3, names=['ruim', 'aceitável', 'ótima'])
```

```
[7] gorjeta['baixa'] = fuzz.sigmf(gorjeta.universe, 5, -1)
    gorjeta['media'] = fuzz.gaussmf(gorjeta.universe, 10, 3)
    gorjeta['alta'] = fuzz.pimf(gorjeta.universe, 10, 20, 25, 50)
    gorjeta.view()
```

Fonte: O autor, 2023.

Para dar início à etapa de defuzzificação dentro do sistema de Lógica Fuzzy, tornou-se imperativo concretizar os resultados provenientes das Regras de Inferência Fuzzy. Neste contexto específico, os graus de pertinência obtidos para cada um dos rótulos linguísticos foram definidos como: *'ruim'* com um grau de pertinência de 0, refletindo a ausência de associação com a qualidade *'ruim'*; *'aceitável'* com um grau de pertinência de 0,20, indicando uma associação moderada; e *'ótimo'* com um grau de pertinência de 0,70, denotando uma forte associação. Esses valores são cruciais para o procedimento de defuzzificação, uma vez que estabelecem a base quantitativa necessária para a transformação dos valores Fuzzy em uma saída numérica única e acionável.

A técnica de defuzzificação através da centróide desempenha um papel fundamental na teoria dos conjuntos difusos. Essa abordagem busca determinar o "centro de gravidade" de um conjunto difuso em relação ao eixo x, considerando-o como uma área com espessura e densidade uniformes. A centróide pode ser concebida como o ponto ao longo do eixo x onde o conjunto difuso se equilibra, analogamente ao centro de massa de um objeto físico.

A fórmula utilizada para calcular a centróide é expressa segundo a fórmula, a seguir, em que $\mu(x_i)$ representa o valor de pertinência para o ponto x no universo do discurso:

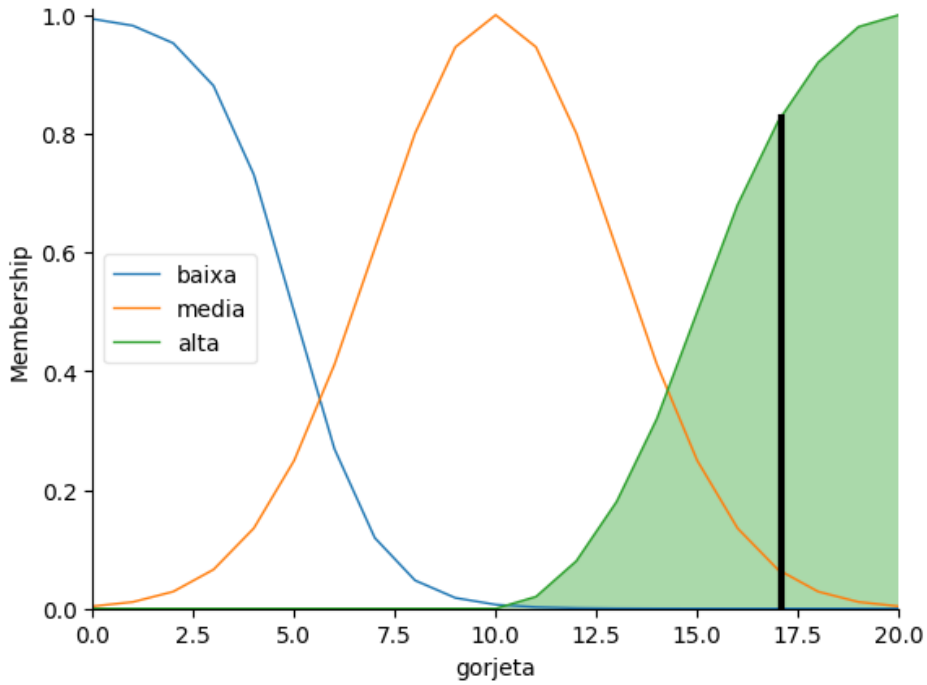
$$\text{Centróide} = \frac{\sum_i \mu(x_i) x_i}{\sum_i \mu(x_i)}$$

Essa expressão matemática é responsável por determinar o ponto médio ponderado ao longo do eixo x, levando em consideração os valores de pertinência associados a um conjunto difuso. A defuzzificação da centróide é uma ferramenta crucial na Lógica Fuzzy, permitindo a transformação de conjuntos difusos em valores numéricos que representam a sua localização central ou média. Esta técnica possui ampla aplicabilidade em áreas diversas, desempenhando um papel significativo em problemas que envolvem incerteza e imprecisão.

O Gráfico 14 ilustra a forma combinada dos valores de inferência e a marcação do traço vertical indica a centróide. O valor da gorjeta neste exemplo é de 17,07%, considerando os valores de Qualidade de Comida = 7 e de Qualidade de Serviço = 8. A fim de aprofundar novos testes, outros valores podem ser explorados.

Ao explorar diferentes valores para as variáveis de qualidade da comida e do serviço, pode-se induzir variações no percentual de gorjeta calculado pelo sistema. Esta abordagem permite não apenas testar a resiliência e adaptabilidade do sistema a diferentes cenários, mas também possibilita a geração de novos gráficos. Estes gráficos servirão como ferramentas visuais para ilustrar as respostas do sistema a essas perturbações, oferecendo uma compreensão mais profunda de como variações nas entradas afetam os resultados. Este procedimento é fundamental para garantir uma compreensão abrangente do comportamento do Sistema de inferência Fuzzy, contribuindo significativamente para o corpo de conhecimento sobre a aplicabilidade prática e a eficácia de tais sistemas em situações do mundo real.

Gráfico 16 - Exemplo: Valor percentual da gorjeta



Fonte: O autor, 2023.

Para o gráfico da Figura 18, foi utilizado o seguinte código, em Python:

Figura 18 - Valor percentual da gorjeta

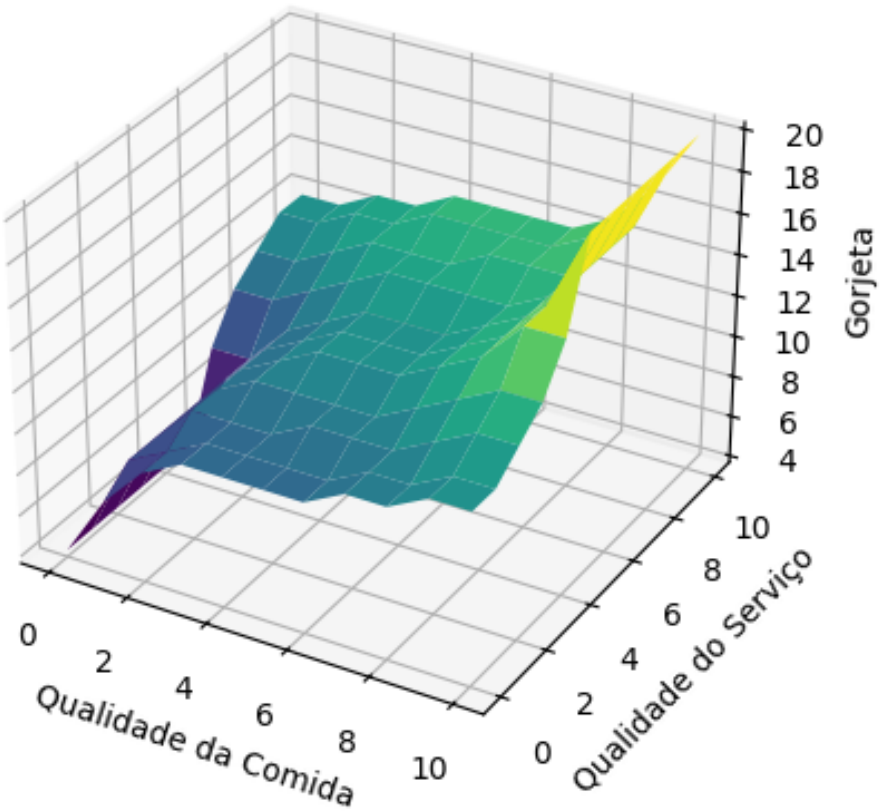
```
[20] regra1 = ctrl.Rule(qualidade['ruim'] | servico['ruim'], gorjeta['baixa'])
     regra2 = ctrl. Rule(servico['aceitável'], gorjeta['media'])
     regra3 = ctrl.Rule(servico['ótimo'] | qualidade['saborosa'], gorjeta['alta'])

Sistema de controle

[22]  sistema_controle = ctrl.ControlSystem([regra1, regra2, regra3])

[23] sistema = ctrl.ControlSystemSimulation(sistema_controle)

[35] sistema.input['qualidade'] = 7
     sistema.input['servico'] = 8
     sistema.compute()

     print(sistema.output['gorjeta'])
     gorjeta.view(sim=sistema)

     17.06666666666667
```

Fonte: O autor, 2023.

Na análise dos gráficos, empregou-se uma *Lookup Table* visando reduzir o esforço computacional. Para tal propósito, recorreu-se à função plot_surface do módulo mpl_toolkits.mplot3d da biblioteca Matplotlib. Embora outras alternativas, como a função gensurf do MATLAB, pudessem ser empregadas para visualizar superfícies análogas, optou-se pelo uso do Python para a obtenção dos resultados.

A função **plot_surface** do módulo **mpl_toolkits.mplot3d** desempenha um papel fundamental na visualização de superfícies tridimensionais. Ao receber dados organizados em uma grade 2D, em que cada ponto da grade possui coordenadas x, y e z, esta função é capaz de gerar uma representação tridimensional que ilustra de forma clara e intuitiva como os valores de z variam em relação às coordenadas x e y. Dessa forma, torna-se possível explorar e comunicar visualmente as relações entre três variáveis de maneira precisa e eficaz. O Gráfico 15 ilustra o resultado alcançado por meio dessa abordagem (Matplotlib, 2024).

Gráfico 17 - Geração de superfície tridimensional



Fonte: O autor, 2023.

A Figura 19, apresentada a seguir, ilustra o código-fonte utilizado para a visualização de superfícies tridimensionais por meio da função **plot_surface** do módulo **mpl_toolkits.mplot3d**. Este trecho de código desempenha um papel crucial na análise e interpretação de dados complexos em um contexto tridimensional. Por meio da organização e processamento adequados dos dados, a função **plot_surface** é capaz de gerar representações visuais detalhadas que permitem uma compreensão mais profunda das relações entre as variáveis envolvidas.

Figura 19 – Código-fonte do Gráfico tridimensional.

```
# Visualização das funções de pertinência para Gorjeta
gorjeta.view(sim=sistema)

# Criação dos valores para a superfície
qualidade_values = np.arange(0, 11, 1)
servico_values = np.arange(0, 11, 1)
qualidade_grid, servico_grid = np.meshgrid(qualidade_values, servico_values)

# Preparação dos valores para a superfície
Z = np.zeros_like(qualidade_grid)
for i in range(len(qualidade_values)):
    for j in range(len(servico_values)):
        sistema.input['Qualidade'] = qualidade_values[i]
        sistema.input['Serviço'] = servico_values[j]
        sistema.compute()
        Z[i, j] = sistema.output['Gorjeta']

# Visualização da superfície
fig = plt.figure()
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(qualidade_grid, servico_grid, Z, cmap='viridis')
ax.set_xlabel('Qualidade')
ax.set_ylabel('Serviço')
ax.set_zlabel('Gorjeta')
plt.show()
```

Fonte: O autor, 2023.