ERIKA MIDORI KINJO

MODELAGEM E SIMULAÇÃO DE REDES BAYESIANAS PARA O CÁLCULO DE PROBABILIDADE DE FALHA EM SISTEMAS IoT NA SAÚDE

SÃO PAULO
2021

ERIKA MIDORI KINJO

MODELAGEM E SIMULAÇÃO DE REDES BAYESIANAS PARA O CÁLCULO DE PROBABILIDADE DE FALHA EM SISTEMAS IoT NA SAÚDE

Dissertação apresentada ao Programa de Pós-Graduação em Informática e Gestão do Conhecimento da Universidade Nove de Julho - UNINOVE, como requisito parcial para obtenção do título de Mestrado.

Professor Dr. André F. H. Librantz - Orientador

SÃO PAULO
2021

Kinjo, Erika Midori.
Modelagem e simulação de redes bayesianas para o cálculo de probabilidade de falha em sistemas IoT na saúde. / Erika Midori Kinjo. 2021.
87 f.
Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2021.
Orientador (a): Prof. Dr. Andre Felipe Henriques Librantz.
1. Modelagem. 2. Redes bayesianas. 3. Probabilidade de falha. 4. Internet das coisas.
I. Librantz, Andre Felipe Henriques. II. Título.
CDU 004

UNINOVE
Universidade Nove de Julho

PARECER – EXAME DE DEFESA

Parecer da Comissão Examinadora designada para o exame de defesa do Programa de PósGraduação em Informática e Gestão do Conhecimento, a qual se submeteu a aluna regularmente matriculada Erika Midori Kinjo.

Tendo examinado o trabalho apresentado para obtenção do título de "Mestre em Informática e Gestão do Conhecimento", com Dissertação intitulada "MODELAGEM E SIMULAÇÃO DE REDES BAYESIANAS PARA O CÁLCULO DE RISCO EM SISTEMAS IoT NA SAÚDE", a Comissão Examinadora considerou o trabalho:

(x) Aprovado **( ) Aprovado condicionalmente**

( ) Reprovado com direito a novo exame **( ) Reprovado**

Parecer:

_____
_____
_____.

EXAMINADORES

Prof. Dr. André Felipe Henriques Librantz (Orientador – UNINOVE)

_____

Prof. Dr. Rodrigo Franco Gonçalves (Membro Externo - UNIP)

_____

Prof. Dr. Fellipe Silva Martins (Membro Interno – UNINOVE)

_____

São Paulo, 25 de fevereiro de 2021.

AGRADECIMENTOS

Meus sinceros agradecimentos ao professor Dr. André Felipe Henriques Librantz, pela orientação, paciência e parceria. Muito obrigada por cada ensinamento durante essa trajetória. Ao professor Dr. Fellipe Silva Martins, meu primeiro contato com o PPGI, por ter acreditado em mim desde o início. Ao professor Dr. Fábio Cosme Rodrigues dos Santos pelas conversas e apoio na coleta de dados dos especialistas. Aos professores Edson Melo de Souza e Marcelo Galdino pelas contribuições importantíssimas neste trabalho. Aos meus colegas de turma, pela troca de experiência e apoio não somente do decorrer das disciplinas, mas em especial no módulo internacional.

Aos meus pais por toda a educação que me proporcionaram e, principalmente à minha mãe Suely Uema, pelo apoio e compreensão pela minha ausência. Aos líderes das empresas que passei durante essa trajetória, por me apoiarem nessa jornada.

E muito obrigada Universidade Nove de Julho pela bolsa recebida que viabilizou a realização desse curso.

RESUMO

A internet das coisas tem sido aplicada em diversos contextos: das cidades inteligentes, educação, cadeia de suprimentos e saúde. A implantação dessa tecnologia proporciona benefícios à vida, tais como: controle remoto de pragas na agricultura, monitoramento da cadeia de suprimentos, melhoria no ambiente físico e virtual na educação e acompanhamento de pacientes. Entretanto, apesar dos benefícios há desafios embarcados com a implantação dessa tecnologia, entre eles destacam-se manter a privacidade e segurança dos dados, zelar pela integridade e confiabilidade dos dados, assim como gerenciamento do custo de energia. Em especial, no que concerne à privacidade e segurança dos dados, por ser um dos maiores desafios da área é necessário avaliar a probabilidade de os componentes falharem e, consequentemente ocasionar esse problema. É neste contexto que este trabalho se propõe a identificar, modelar e calcular a probabilidade de falha, por meio de uma análise sistêmica, usando Redes Bayesianas. Os modelos construídos a partir dessa técnica permitem estimar diferentes cenários na utilização de uma rede de Internet das Coisas. A metodologia empregada foi a abordagem mista, conciliando características da abordagem qualitativa e quantitativa ao realizar a revisão sistemática da literatura, aplicação de formulários para coleta da percepção dos especialistas, além da utilização de outras técnicas para robustecer os resultados, entre elas destacam-se Delphi e Noisy-OR. Os resultados apontaram que por meio da utilização do modelo proposto é possível avaliar diferentes cenários para utilização de redes de Internet das Coisas, bem como simular o efeito de probabilidade de falha nos componentes críticos do sistema.

Palavras-Chaves: Modelagem, Redes Bayesianas, Probabilidade de falha, Internet das Coisas

ABSTRACT

The internet of things has been applied in several contexts: from smart cities, education, supply chain and health. The implantation of this technology provides benefits to life, such as: remote control of pests in agriculture, monitoring of the supply chain, improvement in the physical and virtual environment in education and monitoring of patients. However, despite the benefits, there are challenges embedded with the implementation of this technology, among which stand out maintaining data privacy and security, ensuring data integrity and reliability, as well as energy cost management. In particular, with regard to data privacy and security, as it is one of the biggest challenges in the area, it is necessary to evaluate the probability of the components failing and, consequently, causing this problem. It is in this context that this work proposes to identify, modelling and calculate probability of failure, using Bayesian Networks. The models built from this technique allow estimating different scenarios in the use of an Internet of Things network. The methodology used was the mixed approach, combining characteristics of the qualitative and quantitative approach when carrying out a systematic review of the literature, application of forms to collect the perception of specialists, in addition to the use of other techniques to strengthen the results, among which Delphi stands out. and Noisy-OR. And the results showed that through the use of the model it is possible to evaluate different scenarios for the use of Internet of Things networks, as well as simulating the effect of probability of failure on the critical components of the system.

Keywords: Modeling, Bayesian Networks, Failure Probability, Internet of Things

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

A Internet of Things (IoT) ou na tradução, Internet das coisas, é um conceito que reflete a interconexão de pessoa e objetos a qualquer hora e lugar, podendo impactar todo o negócio. É a interconexão de objetos e dispositivos inteligentes identificáveis dentro da infraestrutura de uma rede que estende os benefícios para além da relação entre máquinas (ISLAM *et al*, 2015).

A visão do mundo conectado possibilita economias mais inteligentes, sustentáveis e inclusivas, exigindo recursos relacionados à ubiquidade, confiabilidade, alto desempenho, eficiência e escalabilidade (BISWAS e GIAFFREFA, 2014).

A utilização da IoT vem percorrendo diversos setores da economia (RAY, 2017), como por exemplo no monitoramento da cadeia de suprimentos (BEN-DAYA *et al*, 2019), controle remoto de pragas no setor agrícola (LIN *et al*, 2019), acompanhamento preventivo de atletas (WILKERSON *et al*, 2018). Na educação não é diferente, também é uma tendência mundial, impactando o ambiente físico e virtual de aprendizagem (ELSAADANY e SOLIMAN, 2017).

Há aplicação em diversos contextos: dispositivos domésticos, devido à conveniência e eficiência energética (WANG, 2018). A IoT também foi usada no monitoramento da qualidade da água (SUN *et al*, 2017), bem como no gerenciamento de um zoológico (MALI, 2019). E dentre os diversos setores, os custos na área da saúde já representam 10% do Produto Interno Bruto (PIB) mundial (Organização das Nações Unidas, 2020), isso demonstra uma parcela do impacto que as soluções envolvendo IoT podem acarretar.

A IoT tem o potencial de melhorar as aplicações médicas, como o monitoramento remoto de saúde, programas de condicionamento físico, doenças crônicas e cuidados a idosos (ISLAM *et al*, 2015). Tudo isso acarreta em melhoria da qualidade de vida dos cidadãos, além de proporcionar mobilidade e autonomia nas atividades diárias (DOMINGUES *et at*, 2019).

Para melhorar os serviços médicos em hospitais, sistemas de tecnologia vestível (também chamados de wearable) são utilizados para detecção de casos de

emergência no momento da triagem (ALBAHRI *et al*, 2019). No contexto da mobilidade há trabalhos que utilizam sensores para captar a pressão na planta do pé e durante o caminhar pode-se identificar problemas de postura na coluna e lesões em pés diabéticos (DOMINGUES *et al*, 2019). Outra aplicação na área de saúde é na prevenção do desenvolvimento de doenças crônicas. Ali *et al* (2018) sugeriram a supervisão do paciente, através de sensores, após a recomendação de dietas com alimentos e medicamentos específicos.

Todos os exemplos de aplicabilidades de IoT possuem como objetivo final benefícios promissores. De modo geral, como consequência viabiliza a otimização de recursos, identifica desperdício, mal-uso, entre outros desafios.

Os benefícios somente são possíveis através do monitoramento de variáveis associadas a um determinado sistema IoT. Isto só acontece por meio da coleta e geração dos dados automaticamente, a partir de ações programadas, sem a intervenção humana (CERVANTES *et al.*, 2015). Entretanto, problemas decorrentes dessa automação podem ocorrer, são elas: manter a privacidade e segurança dos dados adversos da rede, permitindo sua análise ou não, sem comprometer os benefícios de sua aplicação (SHARMA *et al*, 2018; SAREEN, 2017; WANG *et al*, 2020; ZHANG e XU, 2020; SUN *et al*, 2017; VHADURI e POELLABAUER, 2019; manter a governança, permitindo o controle de acesso aos dados (EL BOUANANI *et al*, 2019; CHANG *et al*, 2020); manter a confiabilidade e integridade dos dados (MUHAMMED *et al*, 2018; AZIMI *et al*, 2019; GIA *et al*, 2018; SELVAN *et al*, 2019; WANG, 2018); rastreabilidade dos dados (LOMOTEY *et al*, 2017); gerenciar o custo da energia (GYAMFI *et al*, 2019; GIA *et al*., 2018; GUERRERO-RODRIGUEZ *et al*, 2020)

Para enfrentar esses desafios em sistemas IoT, MUHAMMED *et al*, (2018) propôs abordar componentes da rede relacionadas ao protocolo, dispositivo / sensor e ao gateway. Enquanto que SHARMA *et al* (2018), optou por abordar os algoritmos desses sistemas.

A implantação de um sistema de Internet das Coisas pode implicar em falhas. A utilização de técnicas para cálculo das probabilidades de falha foi abordada conforme descrito a seguir.

LOMOTEY *et al* (2017) aplicou a técnica de Petri nessa análise, no qual propôs uma arquitetura de streaming de dados do *wearable* que oferecesse a rastreabilidade

das rotas de dados em todo o fluxo do sistema. O intuito do trabalho era determinar os dados pertencentes a cada pessoa de maneira ágil.

O Teorema de Bayes foi implementado no estudo de ALBAHRI *et al*. (2019), a fim de obter um equilíbrio ideal entre minimizar o custo energético do pulso de transmissão e reduzir a incidência de perdas importantes durante a transmissão dos dados do paciente, como a frequência cardíaca. E propuseram um protocolo ideal para a transmissão desse tipo de dados.

As falhas em sistemas IoT foram abordados com tecnologias combinadas: *deep learning*, big data, computação de alto desempenho. No entanto, nos estudos mencionados, os autores propuseram soluções, geralmente, focadas em uma camada específica da rede, tais como: a camada de dispositivo, rede e aplicação. Na abordagem de somente uma camada específica da rede, as soluções podem não avaliar os reais impactos na rede toda e nem seus pontos críticos.

Com isso torna-se vital para a implementação bem-sucedida desses sistemas “modernos” se não somente concentrar-se um componente específico da rede, mas também distribuir a carga de trabalho entre seus participantes, a fim de remediar a probabilidade de falha envolvida (SHARMA *et al*, 2018).

Mittelstadt (2017a) e Mittelstadt (2017b) destacaram questões externas a rede, por exemplo, questões éticas. Entretanto, não há trabalhos que abordem questões externas à rede e como estas poderiam impactá-la.

É neste cenário que este trabalho procurou analisar, dentre um conjunto de variáveis e diferentes cenários característicos desses sistemas, as relações entre os componentes mais comuns e, com isso, apresentar um modelo através da técnica Delphi e Redes Bayesianas para mensurar o impacto desses fatores de forma conjunta.

1.1. PROBLEMA E A PERGUNTA DE PESQUISA

1.1.1. SITUAÇÃO PROBLEMA

O termo Internet das Coisas não é novo, foi apresentado primeiramente por Kevin Ashton, em 1999 (GREENGARD, 2015). No entanto, são recentes as publicações envolvendo IoT na área da saúde, como será abordado no decorrer desse trabalho. O termo IoT irrompeu com tanta frequência nas publicações como raramente aconteceu no passado, em especial na área da saúde, de modo a levantar a dúvida se é mais um nome “moderno”, especulativamente montado para aumentar a atenção em estudos e produtos em torno de tecnologias maduras, em vez de um elemento real da descontinuidade tecnológica (ATZORI *et al.*, 2017).

No cotidiano das pessoas as aplicações de IoT também estão cada mais presentes, por exemplo, no monitoramento em tempo real de dados do paciente para melhoria dos diagnósticos de doenças crônicas (TAN e HALIM, 2019), controle e propagação de surtos (SOOD e MAHAJAN, 2017). Entretanto, compreender o funcionamento dos componentes associados à redes e gerenciá-los foi identificado como sendo uma das atividades cruciais da administração (CAVINATO, 2004).

Com isso, os componentes causadores da falha uma vez identificados são variáveis importantes ligadas à gestão e controle, estes fatores podem fornecer informações essenciais para a melhoria das atividades realizadas pelas empresas (CALLADO, 2007).

Nos trabalhos selecionados na revisão da literatura foram utilizadas algumas técnicas na avaliação das falhas das redes IoT, tais como: Petri por LOMOTEY *et al.* (2017), Redes Bayesianas por GYAMFI *et al* (2019), ZHANG (2018), QINGPING *et al* (2018), ZHANG e XU (2020); SIRYANI *et al* (2017). O framework por MUHAMMED *et al* (2018), entre outros.

Entretanto, diante dos estudos apresentados, foi identificada a escassez de trabalhos que abordem uma avaliação conjunta da importância de cada componente, além do cálculo de probabilidade de falha decorrentes da utilização de redes IoT. Deste modo, verifica-se a lacuna de pesquisa a ser explorada.

Neste trabalho a modelagem e simulação foi utilizada para analisar o impacto quando um componente falhar dentro do sistema Internet das Coisas.

Consequentemente, a pergunta que este trabalho se propõe a responder, é: É possível calcular a probabilidade de falha a partir de uma análise dos componentes associados a redes da internet das coisas utilizando redes bayesianas?

1.1.2. OBJETIVOS

Neste item são apresentados os objetivos geral e específicos:

1.1.2.1. OBJETIVO GERAL

O objetivo deste trabalho é identificar, modelar e calcular de maneira conjunta a probabilidade de falha relacionados à utilização da internet das coisas (IoT).

1.1.2.2. OBJETIVOS ESPECÍFICOS

Como objetivos específicos, este trabalho se propõe:

i. Identificar na literatura, os principais fatores que podem ocasionar falhas durante a utilização de uma rede IoT, estabelecendo a relação de dependência entre fatores;
ii. Validar a interdependência o nível de relevância dos fatores e a probabilidade de falha com o auxílio de especialistas;
iii. Modelar relação de interdependência dos componentes falharem;
iv. Simular e validar a probabilidade de falha dos componentes da rede Internet das Coisas em diversas configurações de sistemas;
v. Coletar a percepção de especialistas sobre a utilidade do modelo proposto.

1.1.3. JUSTIFICATIVA E CONTRIBUIÇÕES DA PESQUISA

A Federação de Cientistas Americanos (FCA), listou internet das coisas como uma das seis tecnologias civis disruptivas. Segundo o órgão, em 2025 os pontos da Internet poderão residir em coisas do dia a dia - embalagens de alimentos, móveis, documentos em papel e muito mais. Os desenvolvimentos de hoje apontam para

oportunidades e problemas futuros, uma vez que a medida em que os objetos do dia-a-dia se se tornam uma ameaça à segurança das informações, a IoT pode distribuir esses riscos de forma muito mais ampla do que a Internet distribuiu até hoje (FEDERAÇÃO DE CIENTISTAS AMERICANOS, 2008).

Com isso esta pesquisa se faz necessária, devido à popularização do uso da internet das coisas e por se tratar de um assunto ainda emergente, conforme podemos perceber na evolução das publicações detalhada no capítulo 4 (Revisão da Literatura).

A utilização dessa tecnologia é acompanhada de desafios, entre eles estão a violação à privacidade e segurança dos dados. Conforme ANJUM *et al* (2018), a taxa de divulgação indevida dos dados de um indivíduo é de, 87%. Em contrapartida a esse uso indevido do uso de dados há o compartilhamento, análise e processamentos dos dados que são necessárias para agilizar os recursos de um sistema IoT.

No contexto da violação à privacidade e segurança dos dados, utilizar ferramentas e/ou técnicas que certamente contribuem para reduzir falhas e superar os desafios mencionados anteriormente que permeiam essas tecnologias, de maneira eficaz, se faz necessário. O assunto mostra-se relevante, apesar da quantidade de publicações referente à problemática ainda ser escassa. É neste cenário que este trabalho se propôs a contribuir.

Para atingir o objetivo proposto neste trabalho foram utilizadas Redes Bayesianas (RB), uma vez que possibilita gerar resultados satisfatórios para modelar e simular a probabilidade de falha dos componentes envolvidos. Esta técnica permite uma análise conjunta em situações de incertezas, estabelecendo a relação de dependência entre os fatores.

Para auxiliar o uso Redes Bayesianas foi utilizado a técnica Delphi, já consolidada na identificação as variáveis relevantes. Na implantação dessa técnica o auxílio de especialistas permitiu a identificação dos componentes de um sistema IoT passíveis de falha.

Ao considerar que o tema é emergente, contando com poucas publicações abordando os fatores de riscos de sistemas IoT com a combinação de técnicas

mencionadas anteriormente, este trabalho traz benefícios para a área de Internet das Coisas, uma vez que é possível simular diferentes cenários para diferentes, em diferentes contextos e que podem levar a falhas.

1.1.4. ESTRUTURA DO TRABALHO

Esta dissertação foi estruturada em 7 capítulos, no Capítulo 1 são apresentadas a introdução, problema e a pergunta de pesquisa, bem como os objetivos, justificativas e contribuições. O capítulo 2 expõe a fundamentação teórica, apresentando o alicerce teórico para o desenvolvimento deste trabalho, o Capítulo 3 contém a revisão da literatura e o Capítulo 4 com a metodologia de pesquisa. Seguido do capítulo 5 com os Resultados e Discussões, contendo a apuração dos valores finais e como foram alcançados, finalizando com o Capítulo 6, com as Conclusões.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados principais conceitos dos temas abordados neste trabalho.

2.1. INTERNET DAS COISAS

Uma rede global oferecendo vários tipos de serviços, como é proposto na Internet das Coisas, envolve complexidades de TI, de processos e pessoas. E é por isso que a sua implantação, de maneira geral, transformou os processos de negócio e também o modelo de inovação. Os benefícios agregados para a sociedade são inegáveis, porém o gerenciamento de falhas tornou-se uma questão importante na implantação dessas redes para superação desses desafios (CHANG *et al*, 2020).

2.2. GERENCIAMENTO DE FALHA

Falha são acontecimentos abruptos ou graduais devido à fadiga física ou humana que fazem com que o sistema tenha comportamentos indesejados (ROUSE, 2021).

O gerenciamento de falha envolve a garantia de continuidade das atividades propostas pela empresa, incluindo uma série de atividades relacionadas ao investimento, design e operação associada ao desenvolvimento do sistema.

Ao contrário da prevenção de acidentes, o gerenciamento de falhas refere-se à prováveis eventos de falhas.

Existem 4 atividades associadas ao gerenciamento de falhas que demonstram a importância de compreender o comportamento esperado do sistema. E com isso identificar pontos de falha para que medidas sejam tomadas com o objetivo de causar menos danos às pessoas impactadas (ROUSE, 2021):

(1) Detecção: determina como o sistema se comportará naturalmente, se nenhum evento indesejado ocorrer;
(2) Diagnóstico: identificação de eventos indesejados, definição de quais são esses eventos indesejados;
(3) Compensação: controle para que não ocorram eventos inesperados, e manutenção dos estados aceitáveis para o funcionamento sistema;

(4) Remediação: Correção ou reparo, quais ações devem ocorrer, em caso de falhas (eventos indesejados)

2.3. MODELAGEM E SIMULAÇÃO

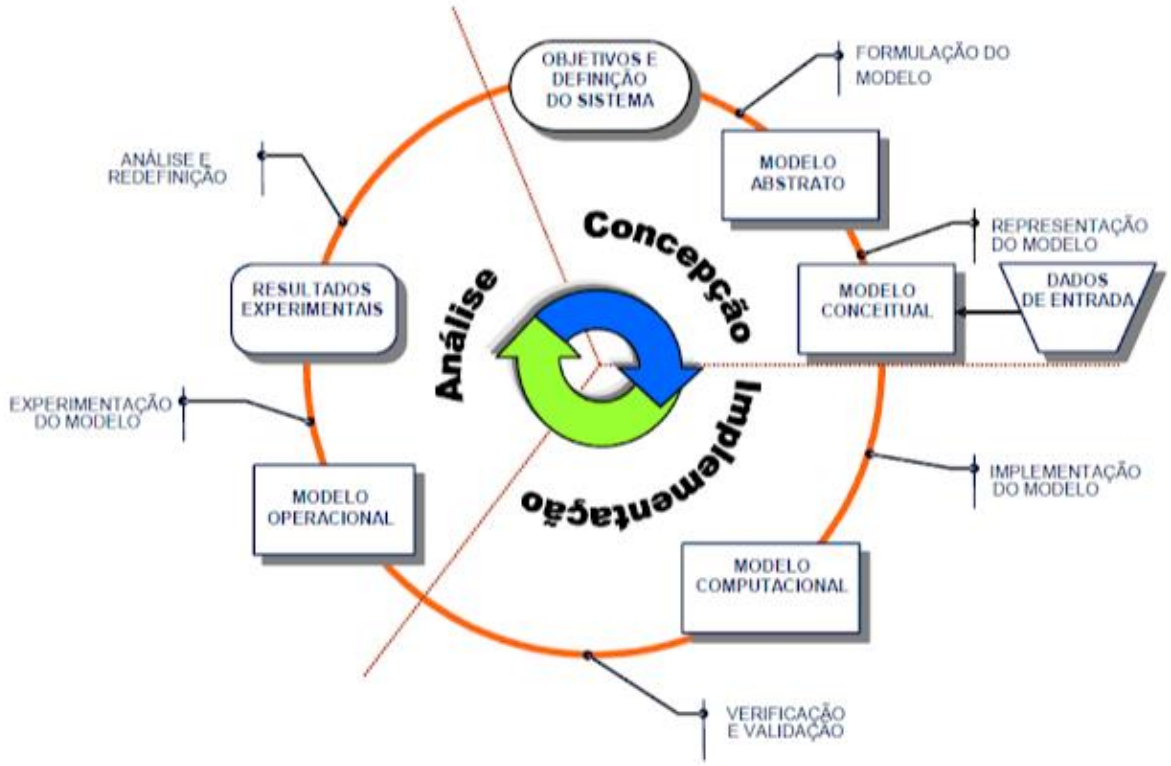
A simulação computacional pode ser entendida como a tentativa de replicação do comportamento de um sistema (VIEIRA e SOARES, 2004). A simulação computacional mostra-se uma poderosa ferramenta para análise de desempenho e otimização de sistemas com muitas particularidades no processo, uma vez que geralmente são complexos de serem analisados e envolvem custos altos para a simulação.

E ainda segundo VIEIRA e SOARES (2004), ao realizar a modelagem e simulação destacaram algumas vantagens, são elas:

- Desenvolvimento de modelos realísticos, mostrando como realmente o sistema opera;
- Desenvolvimento de cenários e avaliar o comportamento sob diversas condições;
- Análise do comportamento sistêmico em um curto período de tempo
- Simular um sistema que pode ainda não existir;
- Possibilidade de redução de custos, ao identificar variáveis controláveis.

A simulação computacional é dividida em três etapas importante e, são elas: concepção, implementação e análise (CIA). Conforme exibido na Figura 1.

Figura 1 - Metodologia de Simulação



Fonte: CHWIF (1999)

Segundo Robinson (2008) a modelagem conceitual, presente na etapa de concepção, impacta todos os aspectos do estudo. Um modelo bem concebido aumenta significativamente as possibilidades de sucesso da simulação.

Na etapa de implementação é apresentado o plano de ação. O Plano de ação corresponde ao que precisa ser feito para obtenção do resultado esperado (THIOLLENT, 2005).

E na etapa de avaliação, as ações elaboradas durante o planejamento das ações são avaliadas. Com isso podem ser identificadas também formas de melhoria (CHUNG-LEE e WEI, 2008).

Na etapa de concepção deste trabalho foram identificadas três técnicas/ métodos que melhor se adequam ao objetivo proposto, as quais são descritas a seguir:

2.4. TÉCNICAS E METODOS

2.4.1. TÉCNICA DELPHI

O uso de Delphi marcou a etapa inicial deste estudo, uma vez que permitiu a identificação e organização dos componentes que podem ocasionar falhas relevantes para objetivo proposto neste estudo.

A técnica Delphi foi desenvolvida, na década de 1950 pela RAND Corporation, com propósitos militares. O objetivo da técnica é obter julgamentos mais confiáveis de um grupo de especialistas, através de entrevistas contendo perguntas focadas no objetivo do problema (ROWE e WRIGHT, 2011).

Os especialistas são profissionais com habilidades e conhecimentos na área acadêmica e/ou comercial e que, segundo a literatura a quantidade mínima de especialistas participantes do processo de decisão depende da experiência e nível de conhecimento sobre o assunto (OLIVEIRA NETO *et al.* 2017).

Delphi é uma combinação de características da pesquisa qualitativa e quantitativas, uma vez que permite a coleta, de forma anônima, de opiniões e com isso extrair a estatística descritiva dos resultados (CHANG *et al.*, 2020).

2.4.1. REDES BAYESIANAS

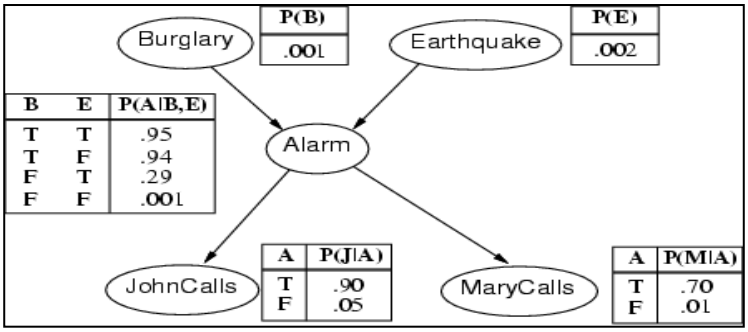
Redes Bayesianas são modelos gráficos que mostram um conjunto de variáveis possíveis e suas dependências condicionais. De modo geral, uma RB é composta por partes quantitativas e qualitativas. A parte qualitativa é um DAG e a parte quantitativa são as probabilidades atribuídas aos nós que representam as variáveis. Ao estabelecer a relação de causa e efeito fornecem resultados animadores no que se refere diagnóstico, previsão e classificação de falhas (LIBRANTZ *et al.*, 2020).

Esta abordagem permite que conhecimento de especialistas sejam incluídos na modelagem (LIBRANTZ *et al.*, 2020). Esta técnica representa uma boa estratégia para lidar com problemas que tratam incertezas.

A RB é caracterizada por grafos acíclicos, no qual os vértices representam os nós e as ligações representam a relação de dependência entre esses nós,

respectivamente são representados por elipse e setas. E os nós que não possuem dependência de outros nós, são denominados nós pais., conforme mostrado na Figura 2.

Figura 2 - Exemplo de rede bayesiana



Fonte: LIBRANTZ *et al*, 2020

Essas variáveis podem ser valores observáveis, variáveis ocultas ou parâmetros desconhecidos. As bordas do BN representam as dependências. Cada nó tem uma função de probabilidade que consiste na probabilidade inicial (para nós sem pais) ou probabilidades condicionais relacionadas a diferentes combinações de nós pais.

A cada valor possível é chamado de estado. Quando há números finitos de estados, as dependências são definidas por tabelas de probabilidade condicionais (TPC). Resumindo, a Tabela de Probabilidade Condicional consiste em um conjunto de distribuições de probabilidade indexadas pelas possíveis combinações de estados nós pais (ZAGORECKI e DRUZDZEL, 2013). O teorema de Bayes expressa a relação entre as variáveis dependentes, como segue:

$$P(H/E) = \frac{P(E/H).P(H)}{P(E)} \quad (1)$$

Na qual P (H / E) é uma probabilidade do evento H dado que o evento E ocorreu, P (E / H) é uma probabilidade do evento E dado que o evento H ocorreu, P (H) é uma probabilidade do evento H e P (E) é uma probabilidade do evento E. O teorema de Bayes usa um conhecimento probabilístico de uma hipótese antes de qualquer observação e, a seguir, apresenta um número estimado para a hipótese

após as observações. A primeira aplicação prática da BN foi o problema clássico do diagnóstico médico (PATTERSON *et al*, 1984). Empresas como a Microsoft usaram essas redes para diagnóstico de falhas, principalmente solução de problemas de impressora (HECKERMAN, MAMDANI e WELLMAN, 1995). As habilidades preditivas e diagnósticas de BN's o tornam uma ferramenta poderosa para a tomada de decisão sob incerteza.

2.4.1.1. INFERÊNCIA COM REDES BAYESIANAS

Formalmente, uma rede bayesiana é definida como um conjunto de variáveis $x = \{x1, \ldots, nx\}$ com: (1) uma estrutura de rede s que codifica um conjunto de dependências condicionais entre variáveis em x, e (2) um conjunto P de distribuições de probabilidade local associadas a cada variável. Juntos, esses componentes definem a distribuição de probabilidade conjunta de x. A estrutura de rede s é um grafo acíclico direcionado (DAG). Os nós em s correspondem às variáveis em Xi. Cada xi denota a variável e seu nó correspondente, e $Pa\ (Xi)$ os pais do nó Xi em s, bem como as variáveis correspondentes a esses pais. A falta de arcos possíveis em s codifica as independências condicionais. Em particular, dada a estrutura s, a distribuição de probabilidade conjunta para x é dada pelo produto de todas as probabilidades condicionais especificadas, como segue:

$$\left(X_{1,} \ldots X_{n,}\right) = \prod_{i=1}^{n} (P(X_i / P_a(X_i)) \qquad (2)$$

Para um determinado BN, as probabilidades dependerão apenas da estrutura do conjunto de parâmetros.

2.4.2. MÉTODO NOISY-OR

Conforme mencionado anteriormente a quantidade em demasia de distribuições de probabilidade é a grande dificuldade de uma rede bayesiana, a fim de reduzir essa complexidade é possível utilizar o método noisy-OR (PEARL, 1986).

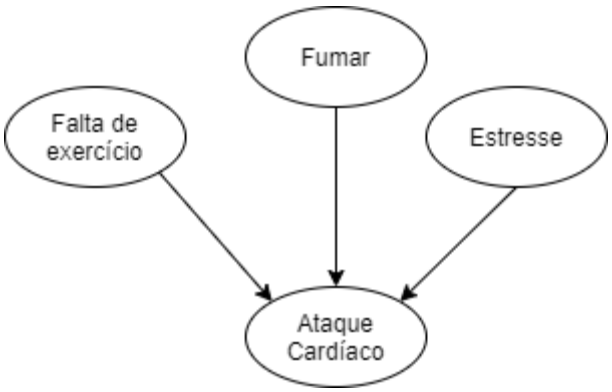
Este método é comum e permite retirar a complexidade das tabelas de probabilidade condicional utilizadas em redes bayesianas, utilizando valores

verdadeiros quando há a possibilidade de ocorrer a situação do mundo real ou caso contrário, falso (FENTON *et al*, 2019).

O método noisy -OR diminui o número de parâmetros necessários para um nó com n^2 pais para n, o que torna mais fácil modelar uma rede grande. A redução dos parâmetros também torna a metodologia mais atraente para aplicações: muitas vezes o conhecimento especializado deve ser utilizado na elicitação de probabilidade e, para fazer isso com sucesso, a quantidade de probabilidades a serem estimadas deve ser bastante limitada. Neste modelo, cada pai pode causar uma interrupção independente em um nó filho e, além disso, há uma "variável de vazamento" que pode causar uma interrupção neste nó, mesmo se os nós pais estiverem funcionais. Interações, ou seja, interrupções devido a mais de um fornecedor sendo interrompido simultaneamente, não são omitidas, mas seu impacto é calculado implicitamente. O tratamento implícito das interações reduz alguma precisão, mas as imprecisões causadas por essa simplificação são provavelmente pequenas.

Para demonstrar o método Noisy-OR, adaptou-se um exemplo proposto por RUSSEL e NORVING (1995): a probabilidade de sofrer ataque cardíaco, dadas algumas situações, como: fumar, falta de exercício e estresse, conforme Figura 3.

Figura 3 - Modelo Noisy-OR



Fonte: Autor

. As probabilidades (chamadas de probabilidades a priori) de não apresentar ataque cardíaco dado os sintomas, são representados da seguinte forma (onde encontramos ¬ lê-se “não apresenta”):

- P(¬ataque cardíaco | falta de exercício, ¬fumar, ¬estresse) = 0,6
- P(¬ataque cardíaco |¬ falta de exercício, fumar, ¬ estresse) = 0,2
- P(¬ataque cardíaco |¬ falta de exercício, ¬fumar, estresse) = 0,1

A Tabela 1 representa a distribuição de probabilidades condicionais utilizando o método Noisy-OR, no qual a letra V (verdadeiro) indica quando apresenta determinada característica e F (falso) quando não apresenta.

Tabela 1 - Tabela de probabilidade condicionais

Falta de exercício	Fumar	Estresse	P(Ataque cardíaco| falta de exercícios, fumar, estresse)	P(¬Ataque cardíaco)
F	F	F	0	1
F	F	V	0,9	0,1
V	F	F	0,8	0,2
V	F	V	0,98	0,02 = 0,2 * 0,1
F	V	F	0,4	0,6
F	V	V	0,94	0,06 = 0,6 * 0,1
V	V	F	0,88	0,12 = 0,6 * 0,2
V	V	V	0,988	0,012 = 0,6 * 0,1 * 0,2

Fonte: adaptado de RUSSEL e NORVING (1995)

Na tabela, a coluna P(¬Ataque cardíaco) são lançadas as probabilidades a priori e nas demais colunas onde encontramos mais letras V multiplicamos os valores correspondentes a cada situação. Portanto, a probabilidade de sofrer um ataque cardíaco (P(Ataque cardíaco| falta de exercícios, fumar, estresse)) é de 0,988 e assim é feito sucessivamente.

Modelar uma rede bayesiana e utilizar o método Noisy-OR, à princípio, pode parecer complexo, no entanto, há vários sistemas computacionais que podem auxiliar na modelagem e raciocínio da modelagem. Dentre eles destacam-se citar o Microsoftw MSBNx6, Agena e o GeNIe entre outros.

3. REVISÃO DA LITERATURA

Este capítulo tem como objetivo apresentar uma Revisão Sistemática da Literatura (RSL) sobre questões de pesquisa. O objetivo de um RSL é propor uma estrutura completa da base teórica, identificando, analisando e interpretando todas as evidências disponíveis, destacando as lacunas da pesquisa em (KITCHENHAM e CHARTERS, 2007).

A revisão sistemática da literatura é baseada em uma estratégia de pesquisa bem definida, o objetivo é extrair o máximo de literatura relevante possível referente ao tema de pesquisado, reduzindo assim o viés de entendimento (KITCHENHAM e CHARTERS, 2007).

Para iniciar uma revisão sistemática da literatura, deve-se definir um conjunto de palavras-chave relacionadas ao tema de pesquisa.

Conforme mencionado anteriormente, o termo "Internet of Things" pode ser referido por sua abreviatura Internet of Things (IoT). Portanto, uma combinação de palavras-chave que tenta combinar essas duas situações produz 8 conjuntos de palavras-chave. São eles:

I. “IoT” and “Failure Probability” and “Health”
II. “Internet of things” and “Failure Probability” and “Health”
III. "IoT" and "failure" and “Health”
IV. "internet of things" and " failure" and “Health”
V. "IoT" and "evaluation " and “health
VI. "internet of things" and "evaluation " and “Health”
VII. "IoT" and "assessment” and “health"
VIII. "internet of things" and "assessment” and “health"

Esses conjuntos de palavras-chave foram usados na RSL. Os dados foram coletados em 4 bases diferentes, incluindo SCOPUS, Web of Science, EBSCO e IEEE Explore.

Primeiramente, a partir dos 8 conjuntos de palavras chaves, foram pesquisadas nas 4 bases de pesquisa sem o uso de filtros de data para entender a evolução, do tema pesquisado. As buscas foram utilizadas o operador lógico “ou” entre os

conjuntos de palavras chaves, uma vez que o operador lógico “e” limita ainda mais o resultado da pesquisa.

O operador lógico “ou” foi aplicado nas combinações das palavras chaves, sendo representado na Tabela 2. As buscas foram realizadas pelo título, resumo, palavras chaves nas bases de pesquisa.

Tabela 2 - Relação dos resultados bases de pesquisa

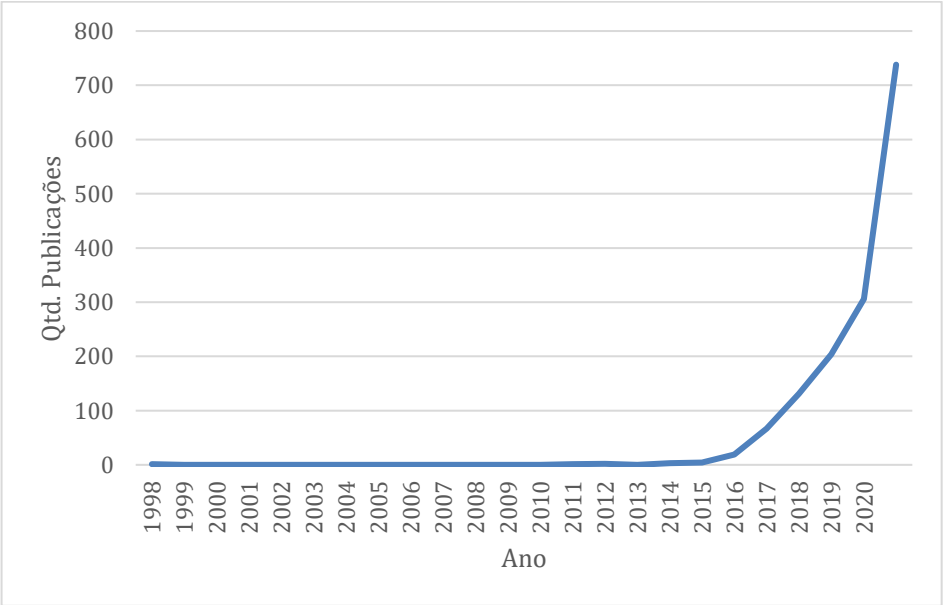
	Sem restrição de data	**Últimos 5 anos**
Scopus	390	336
WoS	377	327
IEE Explorer	159	199
EBSCO	242	140
Total	**1168**	**1002**

Fonte: Autor

Portanto, foi obtido um total de 1002 artigos após desconsiderar os 364 artigos duplicados, no qual a Web of Science apresentou maior contribuição em artigos novos. E com o objetivo de assegurar a qualidade do estudo os critérios de exclusão e inclusão foram aplicados aos resultados preliminares.

As buscas nas bases de pesquisa confirmaram o interesse pelo tema deste trabalho, uma vez que a quantidade de publicações ainda está em ascensão. A Figura 4, apresenta a evolução das publicações.

Figura 4 - Evolução das Publicações



Fonte: Autor

A definição de critérios de inclusão (CI) e exclusão (CE) explícitos são exigências de uma RSL. Para isso, neste trabalho foram utilizados os critérios de inclusão e exclusão propostos por LIAO (2017), conforme a Tabela 3.

Tabela 3 - Critério de Inclusão e Exclusão

Critério	Subcritério	Descrição do subcritério
Exclusão	Sem texto completo	Um artigo sem texto completo para ser avaliado
	Não relacionado	Não aborda o tema pesquisado
	Levemente relacionado	Um artigo não se concentra na revisão, pesquisa, discussão ou solução de problemas
Inclusão	Parcialmente relacionado	1 - Uma pesquisa sobre o tema sem abordar um tópico importante/2 - O termo é apenas mencionado para apoiar algum desafio, problema ou tendência
	Totalmente relacionado	Os esforços de pesquisa de um artigo são explícita e especificamente dedicados ao tema pesquisado

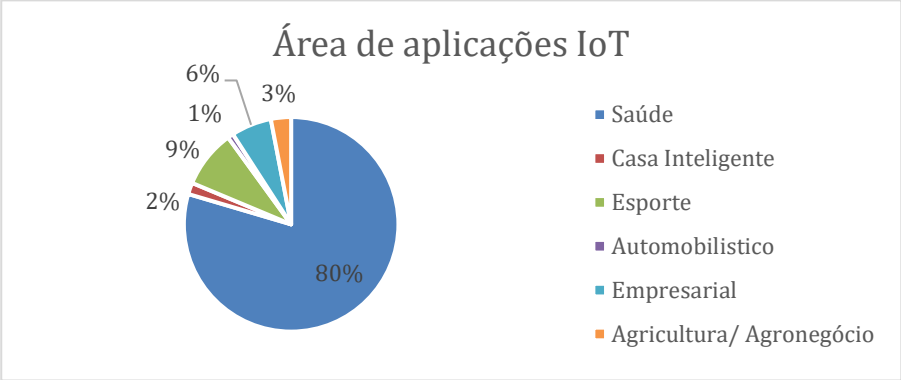
Fonte: adaptado pela autora de LIAO *et al*, 2017

Após a aplicação dos critérios mencionados resultou em 75 artigos, que foram utilizados para a extração dos dados requeridos. E esses 75 artigos reforçaram a lacuna de pesquisa a que esse trabalho se propõe a preencher.

3.1. TRABALHOS CORRELATOS

A revisão da literatura demonstrou que os trabalhos referentes ao tema abordam o contexto de cidades inteligentes, agricultura, recursos humanos, cadeia de suprimentos, esportes, sendo que, em sua grande maioria aborda a temática da saúde. Nota-se na Figura 5, que a área da saúde teve maior impacto das publicações com essa tecnologia.

Figura 5 - Área de aplicação de redes IoT



Fonte: elaborada pela autora

Entretanto, nos trabalhos estudados, os desafios enfrentados são semelhantes, bem como as técnicas aplicadas para superação desses desafios. A Tabela 4, relaciona as técnicas aplicadas e os desafios abordados.

Tabela 4 - Técnicas utilizadas nos trabalhos pesquisados

Autor	Desafio	Técnica
LOMOTEY *et al* (2017)	Rastreabilidade das rotas dos dados	Rede Petri
GYAMFI *et al* (2019)	Custo de energia	Redes Bayesianas
CHANG *et al*(2020)	Governança da Rede/Controle Interno	Delphi
SHARMA *et al*(2018), SAREEN(2017)	Privacidade dos dados	Framework kHealth (desenvolvido pela Wright State University)
AZIMI *et al* (2019)	Integridade dos dados	Método de Imputação Múltipla
WANG *et al* (2020)	Privacidade e Segurança dos dados, Performance, Intenção	Questionário/ Análise dos dados
ZHANG e XU (2020)	Segurança dos dados	Redes Bayesianas
SUN *et al* (2017)	Identificação de intrusão	Redes Bayesianas
VHADURI e POELLABAUER (2019)	Privacidade e Segurança dos dados	Análise dos dados
MUHAMMED *et al* (2018)	Roteamento dos dados, Confiabilidade dos dados	Framework UbeHealth (baseado em deep learning, big data, high performance computing)
SELVAN *et al* (2019)	Confiabilidade dos dados	Lógica Fuzzy
HOU *et al* (2020)	Processamento de dados	Machine Learning
GUERRERO-RODRIGUEZ *et al* (2020)	Gerenciamento de energia	Análise dos dados
GIA *et al* (2018)	Custo de energia/ Integridade dos dados	Análise dos dados
ZHANG *et al*(2018)	Segurança dos dados	Redes Bayesianas
QINGPING *et al* (2018)	Segurança dos dados	Redes Bayesianas

Fonte: elaborada pela autora

Nos trabalhos destacados na Tabela 3, há autores que optaram por utilizar apenas Framework, como o UbeHealth para abordar, em alguns casos, desafios semelhantes aos trabalhos que utilizaram técnicas mais conhecidas.

Identifica-se também a aplicação de outras técnicas, em menor representatividade, por exemplo, rede Petri na rastreabilidade de rota dos dados.

Gyamfi *et al* (2019), utilizou redes bayesianas ao otimizar a rede proporcionando redução do custo de energia em uma rede que recebe dados de batimento cardíaco, cuja perda do dado pode ocasionar em dados irreversíveis para quem o utiliza.

Enquanto que Zhang e Xu (2020) propôs a utilização de redes bayesianas combinados com protocolos avaliar a segurança dos dados trafegados na rede.

Em adição, de modo geral, os trabalhos publicados propuseram soluções envolvendo um ou outro fator da rede, atribuindo-se o nível de importância de forma isolada.

Tal avaliação dificulta avaliar o impacto de qualquer alteração na rede. A proposta deste trabalho é a avaliação conjunta dos fatores de, utilizando como premissa a probabilidade de falha.

Falhas em sistemas IoT são inevitáveis e podem ocorrer devido à problema em hardware, erros nos softwares ou até mesmo fatores sociais (WOO *et al*, 2017; Mittelstadt[1][2], 2017). Porém, estas falhas podem ocasionar desde um simples consumo desnecessário de energia até inconsistência dos dados médicos.

Uma vez que as falhas acontecem, a compreensão da rede permite reduzir esse clima de incerteza. Uma das etapas iniciais nesse processo de entendimento da rede é a identificação de componentes críticos que a compõe (PURI *et al*, 2021).

3.2. COMPONENTES x FALHA

No processo de revisão da literatura notou-se que alguns componentes se tornaram recorrentes às atividades de uma rede IoT e que muitas vezes podem resultar em violação à privacidade e segurança dos dados, perda de confiabilidade nos dados ou mau gerenciamento de energia. Na Revisão Sistemática da Literatura

foram levantados 8 componentes críticos de uma rede Internet das Coisas, conforme a Tabela 5.

Tabela 5 - Principais componentes que podem ocasionar falhas extraídos da literatura

Componente	Conceito	Exemplo	Estudos que corroboram
Dispositivo/ Sensor	Responsável por coletar dados sobre sintomas relacionados à saúde e vários eventos dentro e ao redor do ambiente relacionados ao usuário. Os dados são coletados a partir dos dispositivos de hardware sem fio incorporados ao corpo do usuário, dentro e nos arredores do usuário.	Wearable, Dispositivo de saúde pessoal (PHD) vestível	SOOD e MAHAJAN (2017), WANG (2018), MUHAMMED *et al* (2018), WOO *et al* (2017)
Gateway	Plataforma de gerenciamento de interconexão e serviços; portanto, o gateway é necessário para funcionar como tradutores de protocolo, dispositivos de correspondência de impedância e conversores de taxa entre eles.	Access point, Wireless Transmission (SIM7000C (NB-IoT))	WANG (2018), HU et al (2019), AZIMI *et al*, (2019)
Algoritmo	Atua como uma ponte entre os sensores da IoT e os Serviços de Provedor. É usado para processamento e análise em tempo real de dados acumulados de sensores baseados em IoT.	Algoritmo incorporado, criptografia, algoritmo genético	SOOD e MAHAJAN (2017) ,WANG (2018), ALBAHRI *et al* (2019)
Protocolo	Permite a interoperabilidade nas redes heterogêneas e permita a troca de dados sem interrupções em todo o sistema da Internet das Coisas	Compartilhamento secreto Shamir, LEACH protocol (cluster), IKEv2, IPv6, oneM2M	MITTELSTADT[1][2] (2017), SHARMA *et al* (2018), WANG (2018), MUHAMMED *et al* (2018)
Provedor de Serviços	Armazenamento dos dados (criptografados, perturbados ou anonimizados e sem nenhuma informação de identificação pessoal (PIIs)).Podendo optar por terceirizar dados e computação para um provedor de nuvem que fornece infraestrutura para armazenamento e análise.	Nuvem pública e privada	SOOD e MAHAJAN(2017), SHARMA *et al*2018)
Processamento	Distribuição da carga de trabalho total de estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis. Uma estrutura prática deve garantir que as partes com recursos limitados realizem tarefas de menor complexidade, enquanto as tarefas caras são paralelas à parte com recursos abundantes, como uma nuvem.	Paralelo, distribuído	SHARMA *et al*(2018)
Social	Interação social através da distância geográfica, participação em grupos e localização. Está conectado à privacidade física.	Ética	MITTELSTADT (2017a), MITTELSTADT (2017b)
Aplicação	Responsável pelo controle e gerenciamento dos dados transferidos para o servidor a partir dos elementos de processamento. [...] Para resolver a falta de comunicação entre pacientes e médicos no atual sistema de monitoramento de saúde	Website, Chat	TAN e HALIM (2019), HU *et al* (2019), AZIMI *et al*, (2019)

Fonte: Autor

Conforme a tabela de levantamento dos componentes, WOO *et al* (2017), destacou o dispositivo como fator essencial quando o monitoramento remoto no contexto da saúde foi considerado.

O Gateway foi elencado por Azimi (2019) como outro fator da rede, este fator atua como uma ponte entre o dispositivo e o provedor de serviços. Oferecendo toda a infraestrutura para o armazenamento dos dados e ampla quantidade de técnicas analíticas são responsabilidades do Provedor de Serviços. A contratação de uma infraestrutura de terceiros para este serviço está diretamente relacionada à forma como ser processado os dados, sendo este outro fator que pode influenciar a rede segundo SHARMA *et al* (2018)

O Protocolo foi abordado na solução proposta por MUHAMMED *et al* (2018) para enfrentar os desafios enfrentados por essa tecnologia, tais como latência da rede, largura da banda e confiabilidade dos dados.

O Algoritmo utilizado na rede foi destacado no trabalho de SOOD e MAHAJAN (2017) como outro fator a ser abordado, uma vez que a combinação de algoritmos trouxe resultados interessantes para o controle e propagação do vírus da Chikungunya.

Segundo Tan *et al* (2018), a rede apresenta a Aplicação, no formato de Web sites, Chats, como o fator relevante para a rede. É por meio da aplicação que os usuários (médico e pacientes) visualizar os dados e informações obtidas.

Para finalizar questões sociais também foram abordadas no trabalho de apresentado por Mittelstadt (2017a) e Mittelstadt (2017b). Vale ressaltar que o fator social não considerado em nenhum outro trabalho como fator relevante para reduzir incertezas e falhas na rede, sendo considerado uma lacuna nos trabalhos já apresentados.

Além disso não foi encontrado na literatura nenhum trabalho que aborde diretamente um componente específico da rede, de maneira geral os autores dividiam o sistema IoT em camadas e analisavam apenas uma dessas camadas. Entre essas camadas destacaram a camada física, comunicação e apresentação. Com isso componentes externos a rede, por exemplo, questões éticas não eram avaliadas.

Com o objetivo de detalhar os componentes mencionados anteriormente foram elencados 14 subcomponentes. A associação desses componentes e subcomponentes foi representada na Tabela 6.

Tabela 6 - Componente e Subcomponente

Fator	Subcomponente	Conceito	Exemplo(s)
Dispositivo/ Sensor	Quantidade	Número de dispositivos que coletam informações dos pacientes, que podem ser valores extrínsecos e intrínsecos. As características extrínsecas são a temperatura, localização e assim por diante. As características intrínsecas são a pressão arterial, nível de glicose no sangue, batimento cardíaco e assim por diante que são coletados	1 sensor, 2 sensores
	Parâmetro	Refere-se à seleção do conjunto de dados e o que ele representa para o modelo	Dados de localização, saúde, ambiente, meteorológicos
	Tipo	Classificação do sensor em relação a forma como é captado os dados	Smartphone, Weareable
	Modelo	Atributos do dispositivo	Modelo, precisão/acurácia (alta, média, baixa)
Gateway	Tipo	Desempenhar os papéis das infraestruturas físicas e também poderia desempenhar os papéis das infraestruturas de transmissão	SIM7000C
Algoritmo	Quantidade	Número de combinações de algoritmos para atingir o objetivo	
	Objetivo	Os algoritmos devem ser capazes de ajudar a identificar um problema específico e escolher a melhor técnica para isso	Criptografia
	Linguagem	Refere-se à linguagem de programação escolhida para o desenvolvimento da solução para atingir o objetivo	C, JAVA
Protocolo	Configuração	Refere-se ao padrão internacional para comunicação, especifica quando e como os dados são carregados para o servidor ou o comando é baixado pelos dispositivos de detecção e pode influenciar o consumo de energia	I2C de 7 bits.
Provedor de Serviços	Recursos	Refere-se aos recursos usados na arquitetura de rede IoT, como tipo, escalabilidade e investimento	Cloud, On Premisses
Processamento	Recursos	Refere-se à distribuição da carga de trabalho total de estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis para eles. Uma estrutura prática deve garantir que as partes com recursos limitados desempenhem de acordo com a complexidade	Paralelo, Distribuído
Social	Ético	Refere-se a problemas éticos decorrentes dos falhas inerentes à rede IoT, a sensibilidade dos dados relacionados à saúde e seu impacto na prestação de cuidados de saúde. Garantir tecnologia robusta e cientificamente confiável, ao mesmo tempo em que permanece eticamente responsável, confiável e respeitador dos direitos e interesses do usuário.	Direito de possuir e proteger o espaço pessoal, Sentimento de intimidade/ controle, autonomia
Aplicação	Formato(tipo)	Refere-se a forma os usuários podem adquirir suas informações de interesse	API, Website, Chat
	Público Alvo	Refere-se a quem foi projetado para usar a interface, podendo ser um usuário comum ou o gerente do sistema	Médicos, Hospitais, Pacientes

Fonte: Autor

A relação do fator e seus respectivos subcomponente foram utilizados como base para a construção do modelo de redes bayesianas.

Por fim, a revisão sistemática da literatura referente às falhas envolvendo IoT na área da saúde, demonstrou que se trata de uma oportunidade de pesquisa, uma vez que o assunto não foi explorado da mesma forma que é apresentada neste estudo e o tema encontra-se em ascensão.

4. METODOLOGIA

Este capítulo apresenta a metodologia adotada para a realização desta pesquisa. São apresentadas a natureza do estudo e o processo metodológico. O processo metodológico inclui o esquema de desenvolvimento para coleta de dados e técnicas utilizadas para construção do modelo e análise dos dados.

4.1. MÉTODO DE PESQUISA

Trata-se de uma pesquisa aplicada, pois todo o processo de coleta de dados, aplicação de técnicas e análise dos dados teve como propósito gerar conhecimento para uma aplicação prática (KUMAR, 2011).

A método escolhido foi a abordagem mista, conciliando características da abordagem qualitativa e quantitativa. A vantagem de utilizar a abordagem mista é obter resultados mais assertivos para o objetivo do estudo (CRESWELL e CLARK, 2013).

A abordagem qualitativa foi escolhida para atribuição de nível de relevância e também para probabilidade de falha dos componentes do sistema Internet das Coisas e foi realizada com o auxílio de especialistas. Os especialistas auxiliaram na identificação do nível de relevância foram fornecidos aos especialistas as opções “Pouco relevante”, “Médio” e “Muito Relevante” e para atribuição da probabilidade de falhar as opções eram: “Muito baixa”, “Baixa”, “Mediana”, “Alta”, “Muito alta”.

Existem outros métodos para obtenção de tais informações, por exemplo a atribuição direta de valores numéricos, na escala de 1 a 10 para o nível de relevância e 0 a 100% para a probabilidade de falha. Apesar de simples este método pode acarretar em efeitos adversos, tais como o preenchimento de números inteiros (10%, 20%, 30%, ...).

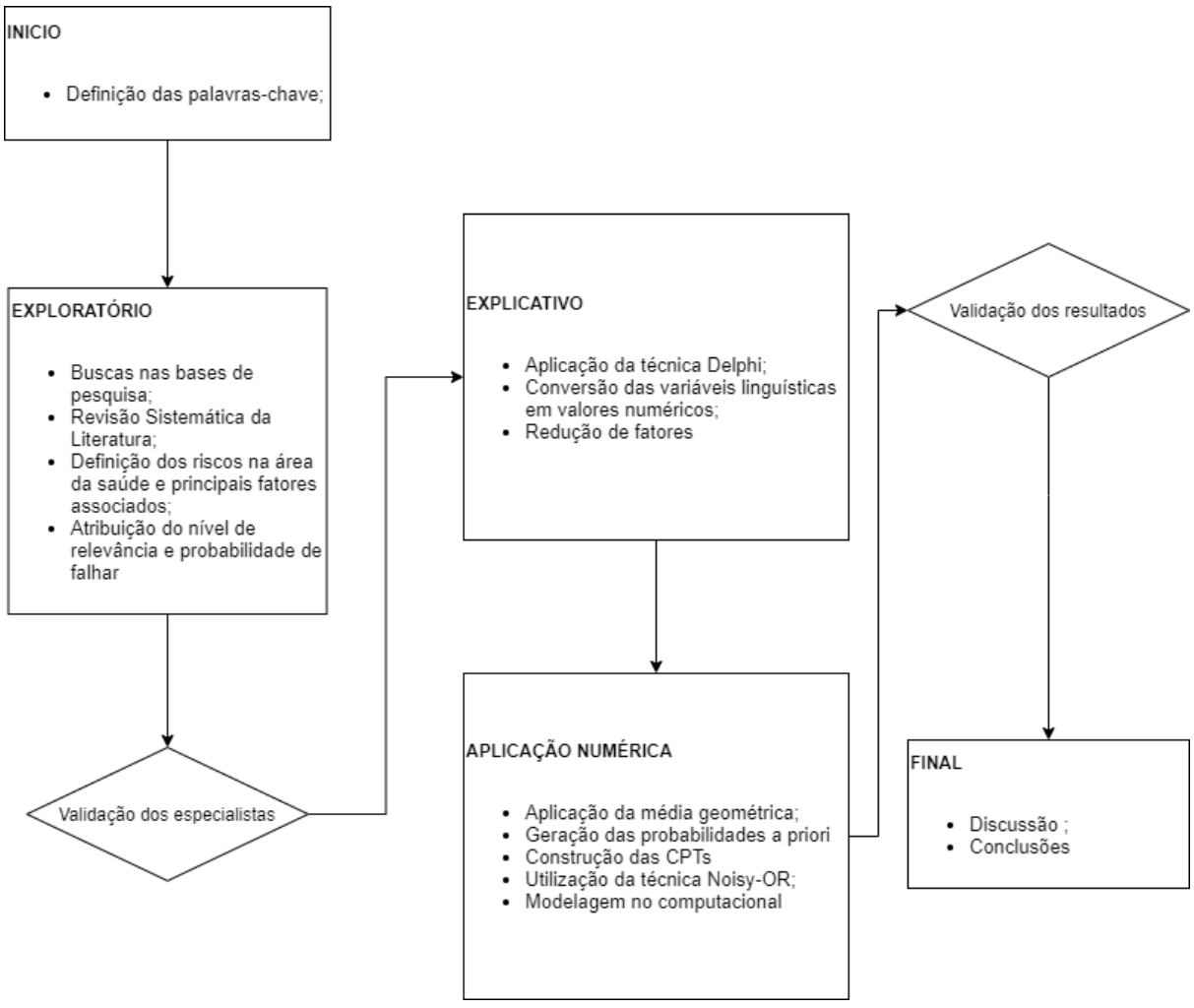
Ao utilizar uma abordagem qualitativa para obtenção dessas informações tende-se a diminuir a quantidade de erros adversos. Cada uma das variáveis linguísticas foi convertida em valores numérico, por meio de uma escala. Posteriormente esses valores numéricos foram empregados em uma abordagem quantitativa, ao utilizar como parametrização inicial no Delphi e nas redes Bayesianas.

Segundo KUMAR (2011), a pesquisa ainda pode ser classificada quanto ao propósito. Esta pesquisa inicialmente teve carácter exploratório, uma vez que o foco inicial era fornecer contexto sobre o problema estudado. Em um segundo momento, o estudo se tornou preponderantemente descritivo, no qual há o aprofundamento sobre o tema. É nesta etapa que o conhecimento prévio obtido na exploração da situação problema é considerado.

4.2. PROCESSO DA METODOLOGIA DE PESQUISA

Para o desenvolvimento deste estudo, o trabalho foi dividido em três etapas para obtenção de um resultado mais consistente. Com isso, para melhor visualização das etapas foi elaborado um fluxograma, conforme a Figura 6.

Figura 6 - Etapas de metodologia aplicada ao estudo



Fonte: Autor

As etapas são explicadas a seguir, a partir da definição das falhas na área da saúde e principais componentes associado, visto que a etapa inicial já foi detalhada na revisão da literatura.

4.2.1. ETAPA EXPLORATÓRIA

4.2.1.1. IDENTIFICAÇÃO DE FALHAS NA UTILIZAÇÃO DE IoT NA SAÚDE E COMPONENTES ASSOCIADOS

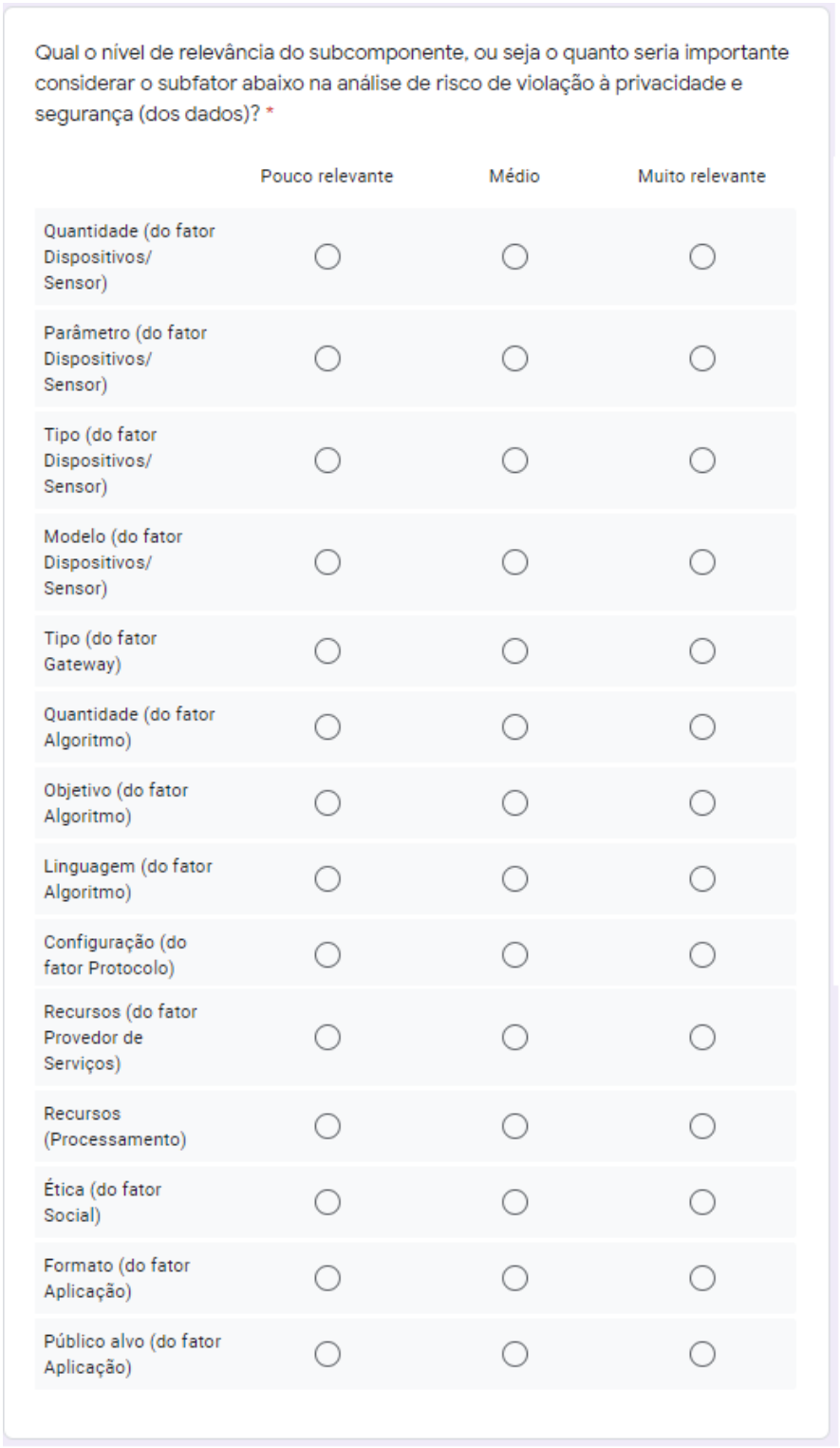
Na revisão de literatura foram selecionados 75 artigos, nos quais foram identificados 8 componentes e 14 subcomponentes associados a estes no contexto da área de IoT na área da saúde. Além disso, no processo de revisão da literatura, foram identificados 2 principais desafios associados à utilização da rede IoT, são eles: (1) violação à privacidade e segurança dos dados e (2) perda de integridade dos dados. A violação à privacidade e segurança é predominante entre os artigos selecionados, portanto, se optou por explorá-lo.

4.2.1.2. ATRIBUIÇÃO DE PROBABILIDADE DE OCORRÊNCIA E NÍVEL DE IMPORTÂNCIA

Com a finalidade de compreender melhor os componentes que podem ocasionar falhas identificados na literatura, foi necessário que estes fossem avaliados em relação à probabilidade de falha e nível de impacto na rede IoT. Um formulário no Google Forms foi criado para auxiliar nesta etapa e o conteúdo completo encontra-se no APÊNDICE A. O recorte do formulário encaminhado a cada um dos especialistas, é apresentado na Figura 7.

Na primeira etapa a probabilidade de falha e nível de importância foram determinadas por 12 especialistas, sendo a probabilidade de falha um valor entre 0 e 100% e a avaliação do nível de relevância, um valor de 0 à 10.

Figura 7 - Trecho do formulário para atribuição de relevância dos subcomponente



Qual o nível de relevância do subcomponente, ou seja o quanto seria importante considerar o subfator abaixo na análise de risco de violação à privacidade e segurança (dos dados)? *

	Pouco relevante	Médio	Muito relevante
Quantidade (do fator Dispositivos/ Sensor)	○	○	○
Parâmetro (do fator Dispositivos/ Sensor)	○	○	○
Tipo (do fator Dispositivos/ Sensor)	○	○	○
Modelo (do fator Dispositivos/ Sensor)	○	○	○
Tipo (do fator Gateway)	○	○	○
Quantidade (do fator Algoritmo)	○	○	○
Objetivo (do fator Algoritmo)	○	○	○
Linguagem (do fator Algoritmo)	○	○	○
Configuração (do fator Protocolo)	○	○	○
Recursos (do fator Provedor de Serviços)	○	○	○
Recursos (Processamento)	○	○	○
Ética (do fator Social)	○	○	○
Formato (do fator Aplicação)	○	○	○
Público alvo (do fator Aplicação)	○	○	○

A figura representa somente um dos componentes, sendo que o formulário completo encaminhado aos especialistas encontra-se no APÊNDICE A.

4.2.2. ETAPA EXPLICATIVA

4.2.2.1. APLICAÇÃO DA TÉCNICA DELPHI

A técnica Delphi, permite a coleta de opiniões de especialistas com domínio no assunto. Deste modo, para este trabalho foram convidados 12 especialistas, cuja experiência média em projetos de automação supera 10 anos, demonstrando-se ser adequada para este trabalho. Os formulários online tinham como objetivo agilizar e organizar as opiniões de um grupo de especialistas no campo investigado, sendo utilizada como ferramenta de consolidação dos julgamentos individuais realizados de forma anônima e separadamente, evitando confronto direto e influência de noções pré-concebidas entre os especialistas (ROWE e WRIGHT, 2011).

Os especialistas atribuíram pesos a cada um dos 8 componentes e seus respectivos 14 subcomponentes, que conforme mencionado anteriormente, foram extraídos da literatura. Entre as opções de pesos atribuídos estavam: 1 – Pouco Relevante, 2 - Médio, 3 - Muito Relevante. Logo, após a atribuição do grau de importância, utilizando a técnica Delphi foi possível identificar 3 subcomponentes de menor impacto no modelo, são eles: (1) o modelo do dispositivo/ sensor; (2) linguagem, do algoritmo e, (3) recursos, associados ao processamento.

E para mensurar o menor impacto, foi utilizado um método já consagrado na área da saúde para avaliação do conteúdo (HYRKAS *et al*, 2003). O Índice de Validade de Conteúdo - IVC, mede a proporção ou porcentagem de juízes que estão em concordância sobre determinados aspectos do instrumento e de seus itens. O IVC é calculado pela soma dos valores positivos de concordância divido pelo número total de especialistas participantes (ALEXANDRE, N.M.C e COLUCI, M.Z.O., 2011; BELLUCCI JÚNIOR, J. A. B.; MATSUDA, L. M, 2012).

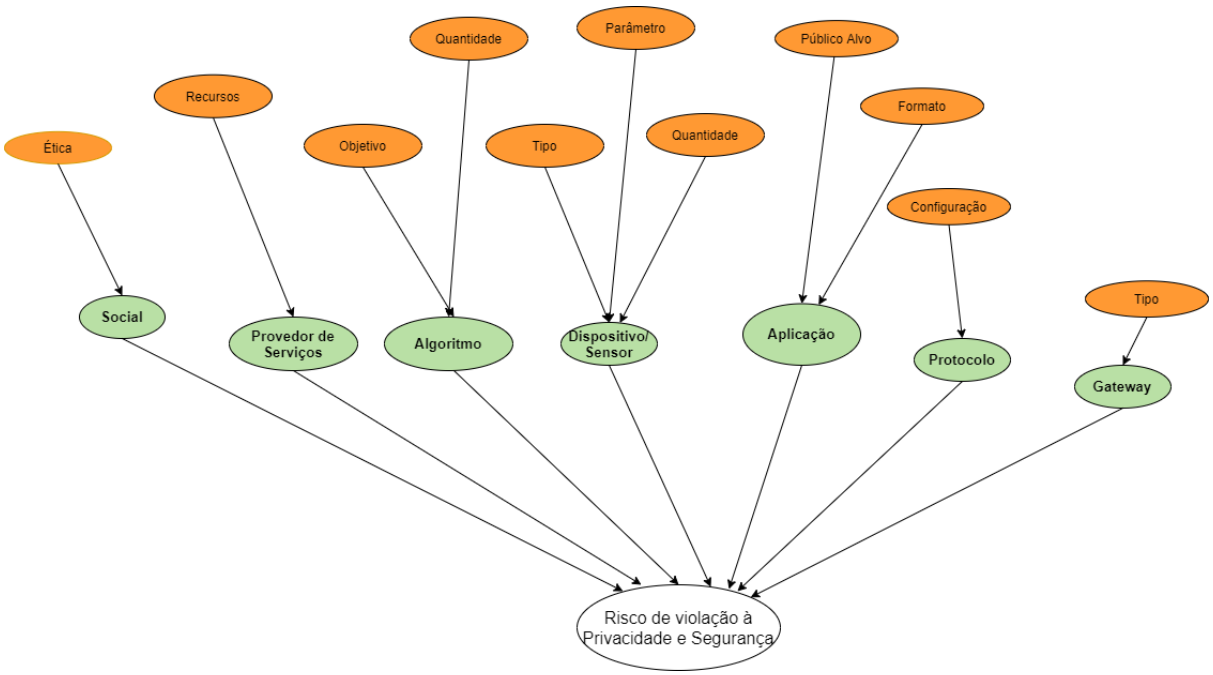
O índice foi calculado por meio da soma de concordância dos itens marcados por 2 ou 3 pelos especialistas e os itens marcados como 1 foram desconsiderados, obtendo-se, com isso, a seguinte fórmula:

$$IVC = \frac{quantidade\ de\ respostas\ 2\ ou\ 3}{quantidade\ total\ de\ especialistas\ participantes} \qquad (3)$$

Alguns autores utilizam uma escala com pontuações de 1 à 4 , na qual: 1 - não relevante ou não representativo, 2 - item necessita de grande revisão para ser representativo, 3 - item necessita de pequena revisão para ser representativo, 4 - item relevante ou representativo. Outros autores sugerem opções mais simples (ALEXANDRE, N.M.C e COLUCI, M.Z.O., 2011). Neste trabalho optou-se pela abordagem mais simples, com apenas 3 opções: 1 – Pouco relevante, 2 – Médio e 3 – Muito Relevante.

Os 11 componentes que vieram da literatura e suas dependências, devidamente validadas pelos especialistas (APÊNDICE C) foram reunidos e usados para criar um modelo de rede bayesiana para o cálculo de probabilidade de falha na violação a privacidade e segurança (RVPS) conforme ilustrado na Figura 8.

Figura 8 - Modelo, após aplicação da técnica Delphi



Fonte: Autor

Na referida Figura, os subcomponentes representam nós independentes (pais), sendo destacados na cor laranja. E os nós dependentes (filhos) referem-se aos componentes que dependem dos seus respectivos subcomponentes.

4.2.2.2. CONVERSÃO DAS VARIÁVEIS LINGUISTICAS EM VALORES NUMÉRICOS

Após a aplicação da técnica Delphi e seleção dos subcomponentes foi necessário determinar as probabilidades relacionadas às falhas. Para tanto, foram utilizadas as variáveis linguísticas com valores numéricos equivalentes, conforme Tabela 7.

Tabela 7 - Escala de conversão

Escala	Valor
Muito Alta	0,9
Alta	0,7
Mediana	0,5
Baixa	0,3
Muito Baixa	0,1

Fonte: Adaptado de NAMAZIAN (2019)

Uma vez convertida em valores numéricos a percepção do especialista no que se refere a probabilidade de falha dos componentes, foi possível a aplicação do próximo passo: o cálculo da média geométrica

4.2.3. APLICAÇÃO NUMÉRICA

4.2.3.1. GERAÇÃO DAS PROBABILIDADES A PRIORI

As probabilidades a priori foram inicialmente atribuídas pelos 12 especialistas. Existem vários métodos para agregação de opiniões de grupos, porém, a média geométrica tornou-se uma das mais aceitas entre os acadêmicos, uma vez que este cálculo permite refletir os julgamentos dos especialistas sem a interferência de normalizações, ou seja, possui maior consistência (KREJCÍ, J e STOKLASA, J., 2018).

Com isso, a consolidação das opiniões dos especialistas neste estudo foi realizada por meio da aplicação do cálculo de média geométrica a partir das probabilidades definidas pelos especialistas. A média geométrica de um conjunto de números é estabelecido pela raiz enésima (n) do produto de todos os membros do conjunto (DOUGLAS, 2004). A equação da média geométrica é apresentada a seguir:

$$P = \sqrt[n]{p1\ x\ p2\ x\ p3\ x\ \ldots .\ x\ pn} \qquad (4)$$

, na qual *n* é quantidade de termos da multiplicação.

4.2.3.2. GERAÇÃO DAS TABELAS DE PROBABILIDADES CONDICIONAIS (TPC)

Uma vez definidas as probabilidades a priori as TPCs podem ser desenvolvidas. Neste trabalho as TPCs foram geradas usando o método noisy-OR (PEARL, 1986), conforme explicado anteriormente (no item técnicas e métodos). Suponha que cada causa B_{ij} possa produzir o efeito E_i, que é nó filho com probabilidade f_{ij}. O efeito de todos os pais (nós raiz) com dependências diretas e indiretas pode ser representado da seguinte forma:

$$P(E_i \backslash par(E_i \backslash B_{1,} \ldots, B_{n,}) \qquad (5)$$
$$= 1 - \prod_j (1 - P(Ei \backslash Bj)$$
$$= 1 - \prod_j (1 - fij)$$

Na qual $P(Ei \backslash par(Ei \backslash B1, \ldots, Bn)$ é a probabilidade, que é a probabilidade condicional do iésimo componente ligado às causas B.

Com o intuito de ilustrar o funcionamento da técnica Noisy-OR, considere a probabilidade de o dispositivo falhar ou não dadas algumas características do mesmo, tais como: quantidade, parâmetros e o tipo. A probabilidade a priori e o nível de importância foram utilizados como input inicial para a cálculo da TPC.

Na sequência a distribuição dos valores para as probabilidades de o Dispositivo/Sensor falhar dado as probabilidades de falha dos respectivos subcomponentes. A Tabela 8, representa a distribuição de probabilidade condicional do Dispositivo/ Sensor, utilizando a técnica Noisy-Or. A letra (verdadeiro) indica a presença de determinada característica e F (falso) quando não apresenta. Na coluna da probabilidade de 'Não Existir' foram lançadas as probabilidades a priori. E nas demais colunas, onde encontra-se mais características presentes (marcadas com o V) multiplicou-se os valores correspondentes a cada situação (Linha 1).

Tabela 8 - Distribuição da probabilidade condicional do Dispositivo/Sensor

	QUANTIDADE	PARÂMETRO	TIPO	N. EXISTIR	EXISTIR
1	V	V	V	24,00%	76,00%
2	V	V	F	40,06%	59,94%
3	V	F	V	37,84%	62,16%
4	V	F	F	63,16%	36,84%
5	F	V	V	38,00%	62,00%
6	F	V	F	63,42%	36,58%
7	F	F	V	59,91%	40,09%
8	F	F	F	100,00%	0,00%

Fonte: Autor

A partir desses conceitos, as tabelas de distribuições dos demais componentes foram também construídas e anexadas no APÊNDICE B.

4.2.3.3. MODELAGEM COMPUTACIONAL NO SOFTWARE

Com a definição do grupo de componentes passíveis de falha e a relação de interdependência deles validada, foi possível modelar a Rede Bayesiana, utilizando o software *Genie 3.0 Academic*.

5. RESULTADOS E DISCUSSÕES

5.1 ETAPAS DO DESENVOLVIMENTO DO MODELO PROPOSTO

5.1.1. SELEÇÃO DOS ESPECIALISTAS

A fim de chegar ao objetivo proposto neste estudo foram convidados 12 especialistas cujos perfis foram detalhados na Tabela 9. Esta coleta da percepção dos especialistas em relação ao nível de relevância para o modelo permitiu a aplicação da técnica Delphi e consequentemente reduzir a quantidade de componentes que não são relevantes para o modelo.

Tabela 9 - Perfil dos especialistas

Formação	Experiência (em anos)	Profissional	Conhecimento
Nível técnico em eletrônica	20	Trabalha com diversos protocolos de comunicação e programação na indústria.	Conhecimento superficial em IoT, principalmente com o protocolo MQTT
Engenheiro eletricista	20	Trabalha em uma fabricante da área	Tem experiência em IoT há aproximadamente 5 anos.
Engenheiro eletricista	10 a 15	Trabalha em uma fabricante da área	Tem experiência em IoT há aproximadamente 5 anos.
Engenheiro eletricista	25	-	Tem conhecimento em IoT com experiência de 4 anos.
Nível técnico em eletrônica com graduação em engenharia de controle e automação	10	Trabalha com diversos protocolos de comunicação e programação na indústria.	Tem conhecimento em IoT, mas não trabalha efetivamente com isso.
Engenheiro eletricista	12	Trabalha no setor público	Tem conhecimento em IoT com experiência de 4 anos.
Engenheiro eletricista	12	Trabalha no setor público	Tem conhecimento em IoT com experiência de 4 anos.
Engenheiro computação	10	Trabalha em laboratório de inovação colaborativa	Tem conhecimento em IoT com experiência de 6 anos.
Ciência da computação	20	-	Tem conhecimento em IoT com experiência de 8 anos.
Engenheiro eletricista	10	-	Tem experiência em IoT há aproximadamente 5 anos.
Nível superior em Redes	12	Trabalha com redes	Tem experiência em IoT há aproximadamente 7 anos.
Engenheiro eletricista	10	-	Tem conhecimento em IoT com experiência de 5 anos.

Fonte: Autor

5.2. TÉCNICA DELPHI

Os especialistas atribuíram o nível de relevância para cada um dos componentes identificados na literatura, conforme o modelo proposto. Entre as opções poderiam classificar como:

- Pouco relevante,
- Relevância Média,
- Muito relevante.

Para cada uma das opções foram atribuídos os pesos: 1, 2 e 3, respectivamente. Isso permitiu a identificação dos componentes de maior relevância listados na Tabela 10.

Tabela 10 - Pesos atribuídos aos subcomponentes pelos especialistas

		Esp. 1	*Esp. 2*	*Esp. 3*	*Esp. 4*	*Esp. 5*	*Esp. 6*	*Esp. 7*	*Esp. 8*	*Esp. 9*	*Esp. 10*	*Esp. 11*	*Esp. 12*	*Total*
Dispositivo/ Sensor	**Quantidade**	2	2	1	1	3	2	2	2	2	2	1	1	21
	Parâmetro	2	2	3	1	3	2	3	2	1	2	1	2	24
	Tipo	2	3	3	1	2	2	3	2	3	2	1	1	25
	Modelo	2	1	1	1	2	2	2	3	3	2	1	1	21
Gateway	**Tipo**	3	3	3	1	2	2	1	3	1	2	1	3	25
Algoritmo	**Quantidade**	3	3	2	1	2	2	1	2	2	2	1	1	22
	Objetivo	3	2	3	3	2	2	2	2	1	1	1	1	23
	Linguagem	3	1	3	1	1	2	1	1	1	3	1	1	19
Protocolo	**Configuração**	2	3	3	1	3	2	1	2	2	3	2	1	25
Provedor de Serviços	**Recursos**	3	3	3	3	2	2	3	1	3	3	3	2	31
Processamento	**Recursos**	1	2	2	2	1	2	2	1	2	1	2	1	19
Social	**Ético**	1	2	2	3	1	2	2	2	3	3	2	3	26
Aplicação	**Formato(tipo)**	2	3	2	3	1	2	2	1	1	2	3	3	25
	Público Alvo	2	3	2	3	1	2	3	1	3	2	3	3	28

Fonte: Autor

Para os subcomponentes que foram avaliados pelos especialistas como ‘Média relevância’ ou ‘Muita relevância’ para o modelo, receberam o valor 1. Conforme a Tabela 11.

Tabela 11 - Subcomponentes de Muita ou relevância Média

		Esp. 1	*Esp. 2*	*Esp. 3*	*Esp. 4*	*Esp. 5*	*Esp. 6*	*Esp. 7*	*Esp. 8*	*Esp. 9*	*Esp. 10*	*Esp. 11*	*Esp. 12*	*Total*
Dispositivo/ Sensor	**Quantidade**	1	1	0	0	1	1	1	1	1	1	0	0	8
	Parâmetro	1	1	1	0	1	1	1	1	0	1	0	1	9
	Tipo	1	1	1	0	1	1	1	1	1	1	0	0	9
	Modelo	1	0	0	0	1	1	1	1	1	1	0	0	7
Gateway	**Tipo**	1	1	1	0	1	1	0	1	0	1	0	1	8
Algoritmo	**Quantidade**	1	1	1	0	1	1	0	1	1	1	0	0	8
	Objetivo	1	1	1	1	1	1	1	1	0	0	0	0	8
	Linguagem	1	0	1	0	0	1	0	0	0	1	0	0	4
Protocolo	**Configuração**	1	1	1	0	1	1	0	1	1	1	1	0	9
Provedor de Serviços	**Recursos**	1	1	1	1	1	1	1	0	1	1	1	1	11
Processamento	**Recursos**	0	1	1	1	0	1	1	0	1	0	1	0	7
Social	**Ético**	0	1	1	1	0	1	1	1	1	1	1	1	10
Aplicação	**Formato(tipo)**	1	1	1	1	1	1	1	0	0	1	1	1	10
	Público Alvo	1	1	1	1	0	1	1	0	1	1	1	1	10

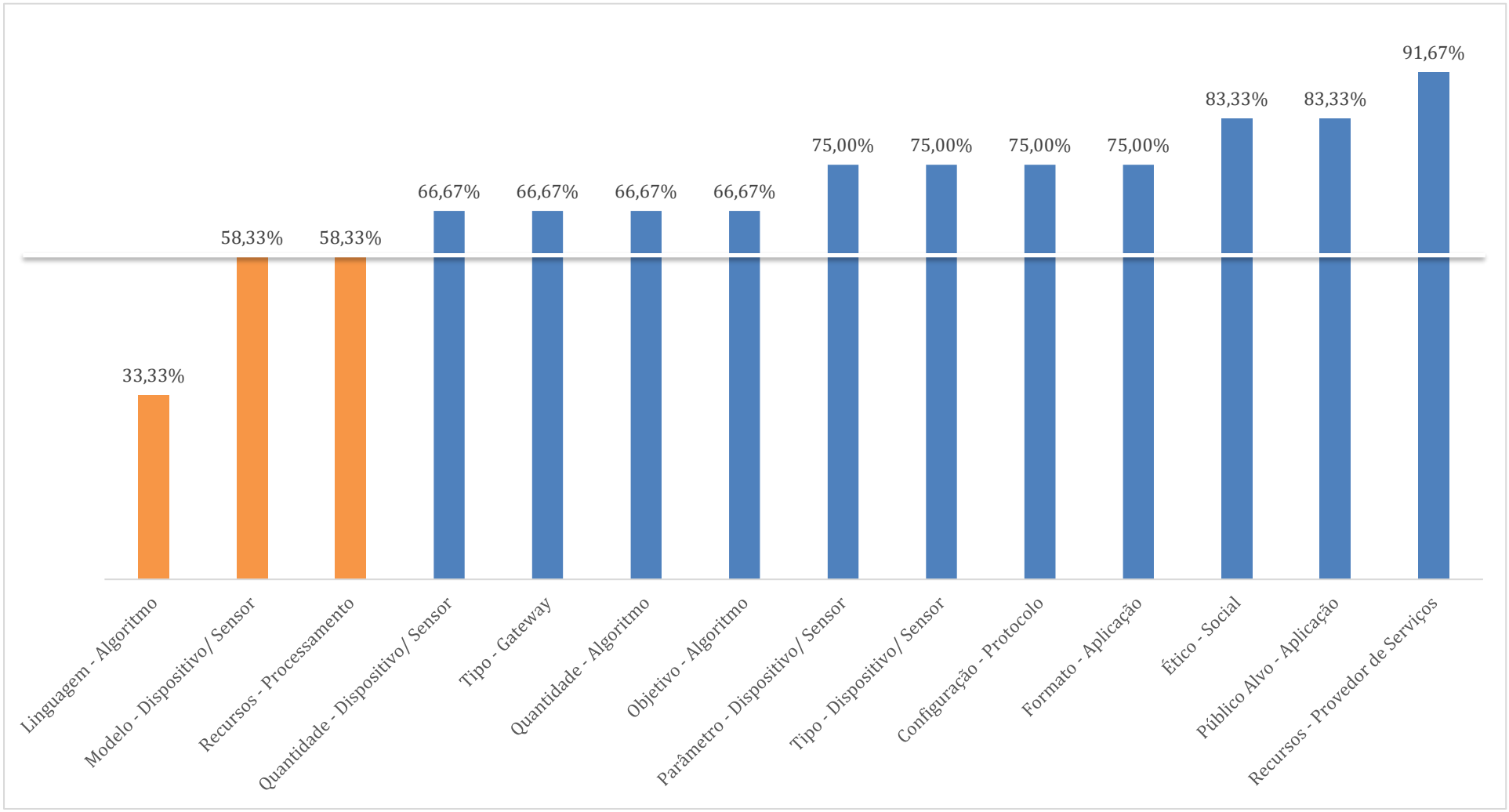
Fonte: Autor

Considerando que cada subcomponente, foi possível definir a posição do ranking de cada subfator dividindo-se o somatório de percepções relevante pelo total de especialistas. Exemplificando: 11 especialistas consideram o subcomponente recursos do provedor de serviços relevante para o modelo, com isso dividiu-se o 11 por 12 obtendo-se 91, 67% de relevância. Representando o subcomponente de maior relevância para o modelo.

5.2.1. REDUÇÃO DO NÚMERO DE COMPONENTES DO MODELO

A coleta e análise desses dados permitiu, de acordo com a visão dos especialistas, excluir do modelo os componentes classificados como menor possibilidade de falha na violação à privacidade e segurança (dos dados), conforme ranking apresentado na Figura 9.

Figura 9 - Ranking do IVC



Fonte: Autor

Conforme destacado anteriormente ao analisar os dados coletados o Provedor de serviços se mostrou o fato de maior relevância, seguido dos componentes Sociais e da Aplicação, corroborando o que foi destacado no capítulo de Revisão da Literatura, no qual o Provedor de Serviços apareceu entre os componentes mais citados.

Apesar de poucos trabalhos publicados sobre questões éticas no contexto deste trabalho, na percepção dos especialistas trata-se de um dos componentes mais relevantes para o modelo. Publicações, até então, avaliavam questões internas dos sistemas IoT.

Entre os componentes considerados de menor importância, após a aplicação da técnica IVC, encontra-se o modelo do Dispositivo/Sensor, a linguagem do algoritmo e os recursos utilizados no processamento. Somente 1 trabalho detalhou o tipo do processamento, classificando-o como processamento distribuído.

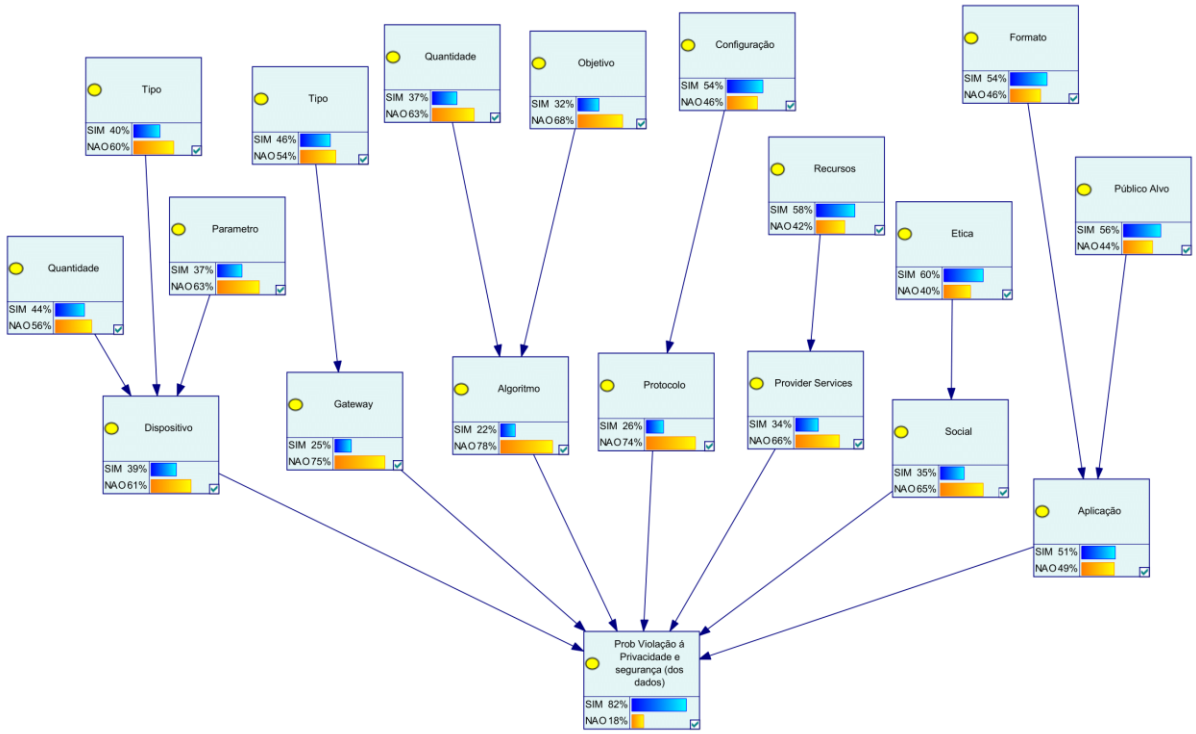
No ranking dos componentes de importância, representado na Figura 9, foi destacado os três componentes que foram excluídos do nosso modelo por não atingirem o limite de IVC estabelecidos. O valor limite considerado nesta pesquisa foi de 60%, de modo que resultado do nível de importância foi reduzido para 11 subcomponentes.

A partir desta etapa passou-se a implementação computacional do modelo bayesiano conforme descrito na sequência.

5.3. IMPLEMENTAÇÃO COMPUTACIONAL DO MODELO BAYESIANO

O modelo foi implementado no software *Genie 3.0 Academic,* ou *GeNIe Modeler* que é uma interface gráfica de usuário (GUI), que permite a construção e aprendizagem de modelos interativos(Figura 10). A principal vantagem da utilização dessa ferramenta é, desde o início permitir a liberdade de modelagem completa, além de ter ampla aceitação tanto na academia quanto na indústria.

Figura 10 - Grafo da Rede Bayesiana produzido no *Genie*



Fonte: Autor

5.4. GERAÇÃO DAS PROBABILIDADES A PRIORI

As informações prévias captadas dos especialistas sobre o problema abordado gerou, juntamente com aplicação da escala de conversão e a média geométrica, a probabilidade a priori que foi utilizada no modelo e estão representadas na Tabela 11.

Tabela 12 - Pesos atribuídos aos subcomponentes pelos especialistas

		Esp. 1	*Esp. 2*	*Esp. 3*	*Esp. 4*	*Esp. 5*	*Esp. 6*	*Esp. 7*	*Esp. 8*	*Esp. 9*	*Esp. 10*	*Esp. 11*	*Esp. 12*	*Probab.*
Dispositivo/ Sensor	**Quantidade**	0,5	0,7	0,5	0,7	0,9	0,3	0,1	0,7	0,1	0,5	0,5	0,5	44%
	Parâmetro	0,5	0,1	0,5	0,3	0,5	0,3	0,3	0,7	0,1	0,5	0,5	0,5	37%
	Tipo	0,5	0,1	0,9	0,3	0,7	0,3	0,7	0,5	0,1	0,5	0,3	0,5	40%
	Modelo	0,5	0,1	0,3	0,5	0,7	0,3	0,7	0,7	0,1	0,5	0,3	0,3	39%
Gateway	**Tipo**	0,5	0,7	0,5	0,3	0,5	0,3	0,3	0,5	0,5	0,5	0,3	0,5	46%
Algoritmo	**Quantidade**	0,5	0,3	0,5	0,5	0,5	0,3	0,1	0,3	0,1	0,5	0,7	0,5	37%
	Objetivo	0,5	0,1	0,7	0,5	0,5	0,3	0,1	0,3	0,1	0,3	0,5	0,3	32%
	Linguagem	0,5	0,3	0,9	0,3	0,5	0,3	0,1	0,3	0,1	0,7	0,5	0,1	37%
Protocolo	**Configuração**	0,5	0,7	0,7	0,3	0,5	0,3	0,3	0,3	0,9	0,7	0,7	0,5	52%
Provedor de Serviços	**Recursos**	0,5	0,5	0,7	0,7	0,3	0,3	0,9	0,3	0,9	0,7	0,7	0,7	58%
Processamento	**Recursos**	0,5	0,5	0,3	0,3	0,5	0,3	0,3	0,3	0,5	0,5	0,5	0,5	43%
Social	**Ético**	0,5	0,7	0,5	0,7	0,9	0,3	0,5	0,3	0,9	0,9	0,5	0,3	60%
Aplicação	**Formato(tipo)**	0,5	0,5	0,7	0,5	0,9	0,3	0,3	0,3	0,9	0,5	0,7	0,3	54%
	Público Alvo	0,5	0,5	0,7	0,7	0,9	0,3	0,7	0,1	0,9	0,7	0,7	0,3	56%

Fonte: Autor

5.5. CONSTRUÇÃO DAS TPC

A partir das probabilidades a priori, definidas anteriormente para nó do modelo foi construída uma tabela de probabilidade condicional. A Tabela 13 representa a TPC do nó Dispositivo.

Tabela 13 - TPC do Dispositivo/ Sensor

	Dispositivo				
	Quantidade	Parâmetro	Tipo		
P(f)	0,368408921	0,36580377	0,40087		
Q(f)	0,631591079	0,63419623	0,59913	NÃO EXISTIR	EXISTIR
	T	T	T	0,240	0,760
	T	T	F	0,401	0,599
	T	F	T	0,378	0,622
	T	F	F	0,632	0,368
	F	T	T	0,380	0,620
	F	T	F	0,634	0,366
	F	F	T	0,599	0,401
	F	F	F	1,000	0,000

Fonte: Autor

Para cada nó foi criado uma TPC, conforme o modelo apresentado para o Dispositivo.

5.6. VALIDAÇÃO DO MODELO

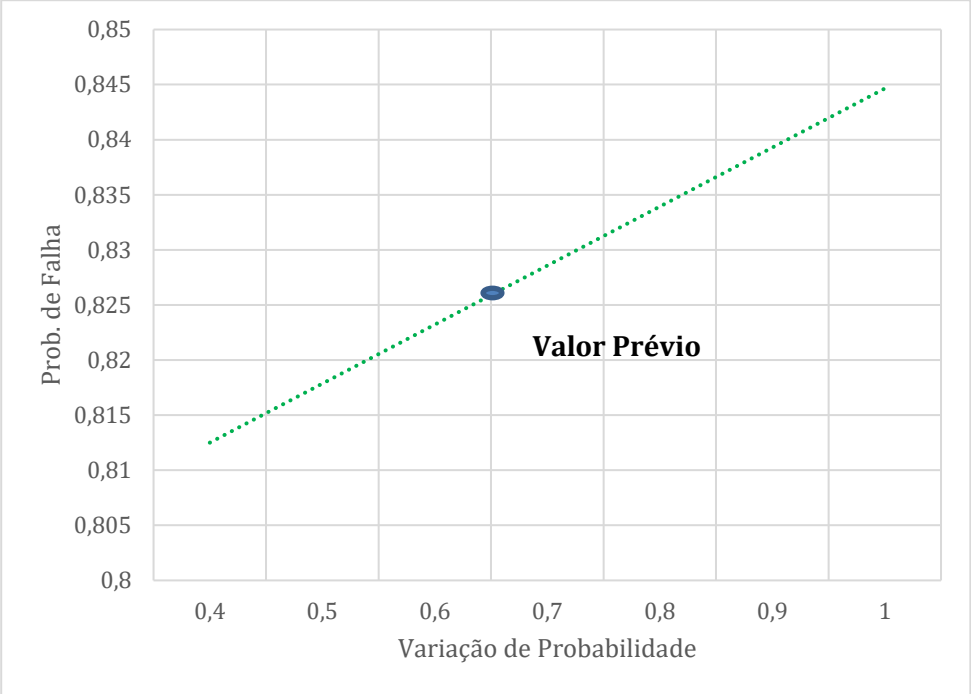
A validação do modelo permite considerável garantia da utilidade do modelo. Existem algumas abordagens para realizar tal tarefa e em uma análise razoável necessita de dados históricos, compreendidos, se possível, em longos períodos de tempo., o que pode tornar a validação completa muito difícil. Segundo Librantz,*et al* (2020), a utilização de dois axiomas é utilizada para a validação parcial do modelo. Os axiomas são:

1. Um ligeiro aumento/diminuição no nó pai resulta um aumento/ diminuição no nó filho. Ou seja, são diretamente proporcionais.

2. A influência nas probabilidades de variações nos nós filhos no desafio de violação à privacidade e segurança dos dados deve ser maior que os parâmetros dos pais.

O gráfico mostrado na Figura 11 corrobora o Axioma 1, no qual a probabilidade de falha é diretamente proporcional à variação do Provedor de Serviços. Assim como diminuirá conforme o nó pai diminui.

Figura 11 - Probabilidade de falha do componente Recursos (do Provedor de Serviços)



Fonte: Autor

A Tabela 14 apresenta os resultados do segundo experimento realizado para validação. Nesta tabela está representado que a medida que a medida que componentes são acrescentados a variação da probabilidade de falha também aumenta. Além disso, quando outro componente é adicionado, a probabilidade de falha é ainda maior do que o anterior.

Tabela 14 - Validação do modelo (axioma 2)

	Desafio Viol. à Privac. e Seg. (dos dados)	Variação (%)
Prévia	0,82	0
Configuração (Protocolo)	0,83	1,2%
Configuração (Protocolo): Parâmetros (Dispositivo)	0,85	3,6%
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços)	0,87	6,0%
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços): Ética (Social)	0,89	7,1%

Fonte: Autor

Esses resultados estão em boa concordância com o Axioma 2 descrito anteriormente, o que permitiu uma validação parcial do modelo proposto.

5.7. EXEMPLOS DE APLICAÇÃO

A eficácia do modelo proposto pode ser melhor verificada a partir de dois experimentos criados com a ajuda de um especialista. No primeiro deles a estimativa de falha de 3 redes IoT é calculada a partir da estimativa de falha dos componentes pai, conforme os cenários abaixo:

Cenário 1: Monitoramento de sala climatizada

- Seis parâmetros são configurados, sendo que cinco deles definem os limites mínimos, máximos e o ideal para a temperatura e um para o controle de umidade.
- O ambiente conta com cinco sensores de temperatura e umidade integrados, modelo Am2315 com protocolo I2c;
- Gateway: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão via protocolo UDP para o servidor;
- Algoritmo: São utilizados dois algoritmos um para processamento dos dados e outro para geração de alertas.
- Objetivo do Algoritmo: Verificar os dados coletados no intervalo de cinco minutos pelos sensores, realizar um cálculo sobre a média das cinco leituras e informar a necessidade de ajustes na temperatura e controle da umidade de acordo com os parâmetros definidos em um painel.
- Configuração do Protocolo: O protocolo utiliza configurações básicas, priorizando a velocidade na transmissão dos dados.
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS.
- Éticas: Conscientização sobre a importância em seguir os protocolos de verificação de alertas e aplicação de correções quando necessárias.
- Formato de aplicação: Ocorre de forma automática por temporização, informando a necessidade de intervenção humana.

Cenário 2: Monitoramento de Polissonografia Home Care

- Sete parâmetros são configurados para receber os dados sobre atividade elétrica cerebral e muscular, movimento dos olhos, fluxo de ar pelo nariz e boca, esforço respiratório e saturação do oxigênio.
- Sete sensores são posicionados no corpo do paciente por meio de eletrodos e canolas para captura de ar;
- Gateway: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão com o protocolo TCP para o servidor via internet;

- Algoritmo: São utilizados dez algoritmos para o processamento e checagem dos dados de cada um dos sensores.
- Objetivo do Algoritmo: Verificar a integridade das leituras, armazena localmente os dados para segurança, realizar encriptação e fazer a transmissão para um servidor.
- Configuração do Protocolo: Utiliza criptografia com os protocolos TLS/SSL, garantindo uma comunicação segura.
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS.
- Éticas: Proteção à privacidade dos dados do paciente, tanto sobre as leituras quanto a sua identificação.
- Formato de aplicação: Ocorre de forma automática, coletando os dados e transmitindo para o centro de monitoramento.

Cenário 3: Monitoramento e Controle de Gotejamento de Medicação

- Seis parâmetros são configurados para verificação do volume da medicação, contagem de gotas e monitoramento dos sinais vitais (temperatura, frequência respiratória, frequência cardíaca e pressão arterial).
- Sete dispositivos são utilizados, sendo quatro sensores posicionados no corpo do paciente para monitoramento dos sinais vitais, dois acoplados no suporte que abriga a medicação e um atuador para regulagem do controle do fluxo da medicação.
- Gateway: Realiza a coleta dos dados dos sensores (supervisório) e faz a transmissão com o protocolo TCP para o servidor via internet;
- Algoritmo: São utilizados seis algoritmos para o processamento e checagem dos dados de cada um dos sensores e um para o atuador de controle de fluxo.
- Objetivo do Algoritmo: Verificar a integridade das leituras, armazenar localmente os dados para segurança, tomar a decisão de alterar o fluxo do gotejamento, realizar encriptação e fazer a transmissão para um servidor.
- Configuração do Protocolo: Utiliza criptografia com os protocolos TLS/SSL, garantindo uma comunicação segura.
- Recursos do provedor de serviços: Utilização de firewall para proteção contra invasões e algoritmos de suporte para verificação de ataques do tipo DDoS.

- Éticas: Proteção à privacidade dos dados do paciente, tanto sobre as leituras quanto a sua identificação, além do controle do acesso físico ao paciente quando necessário para a reposição ou ajustes de equipamentos e/ou medicação.
- Formato de aplicação: Ocorre de forma automática, coletando os dados para realização do monitoramento, atuação sobre a regulagem da aplicação da medicação e transmissão para o centro de monitoramento.

Os cenários acima citados foram resumidos nas probabilidades de falha, conforme a Tabela 15.

Tabela 15 - Cenários de Aplicação

		Probabilidade de Falha		
		Cenário 1	**Cenário 2**	**Cenário 3**
Dispositivo/Sensor	Quantidade	BAIXO	MUITO ALTO	ALTO
	Parâmetro	BAIXO	MÉDIO	ALTO
	Tipo	MÉDIO	ALTO	ALTO
	Modelo	BAIXO	MÉDIO	MÉDIO
Gateway	Tipo	ALTO	ALTO	MUITO ALTO
Algoritmo	Quantidade	BAIXO	MÉDIO	MÉDIO
	Objetivo	BAIXO	ALTO	MUITO ALTO
	Linguagem	BAIXO	BAIXO	BAIXO
Protocolo	Configuração	BAIXO	ALTO	ALTO
Provedor de Serviços	Recursos	BAIXO	ALTO	MUITO ALTO
Processamento	Recursos	BAIXO	MÉDIO	ALTO
Social	Ético	ALTO	ALTO	MUITO ALTO
Aplicação	Formato (tipo)	MÉDIO	MÉDIO	ALTO
	Público Alvo	MÉDIO	ALTO	MUITO ALTO

Fonte: Autor

Para efeitos de análise de falha, valores até 60% foram considerados toleráveis. No quadro abaixo os três sistemas foram classificados conforme a probabilidade de falha.

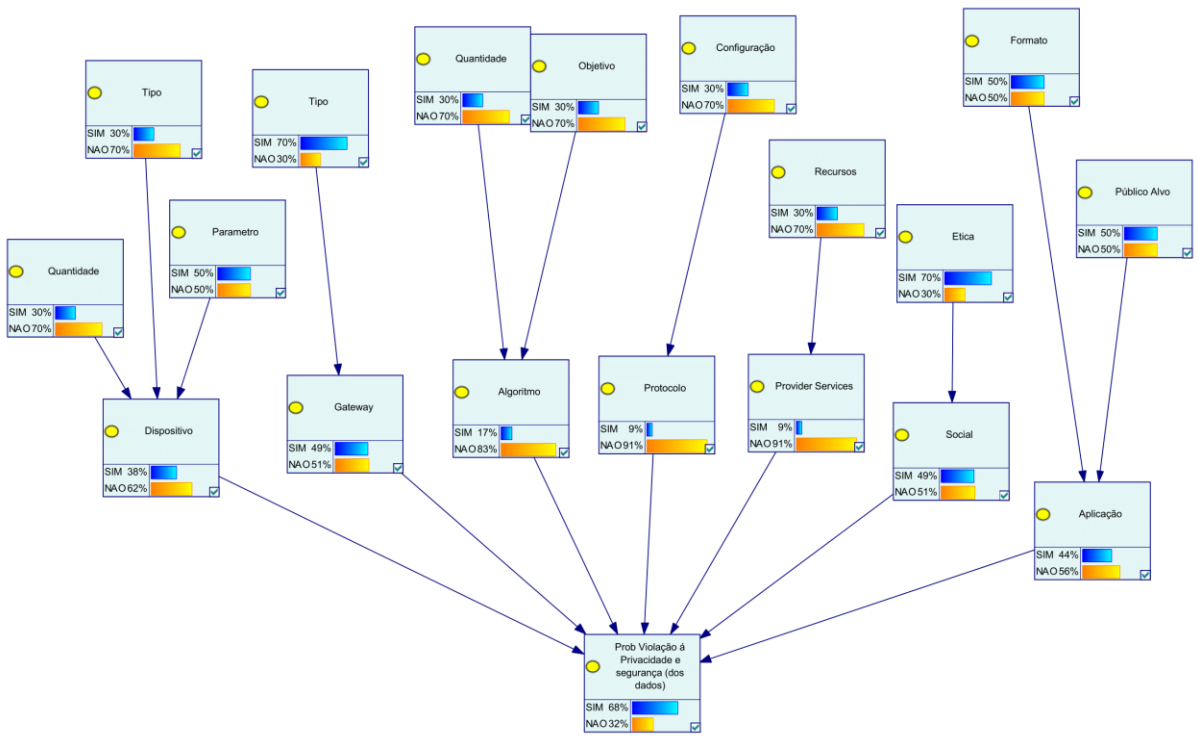
Tabela 16 - Classificação dos Cenários

Sistema	**Classificação**
Cenário 3	1
Cenário 2	2
Cenário 1	3

Fonte: Autor

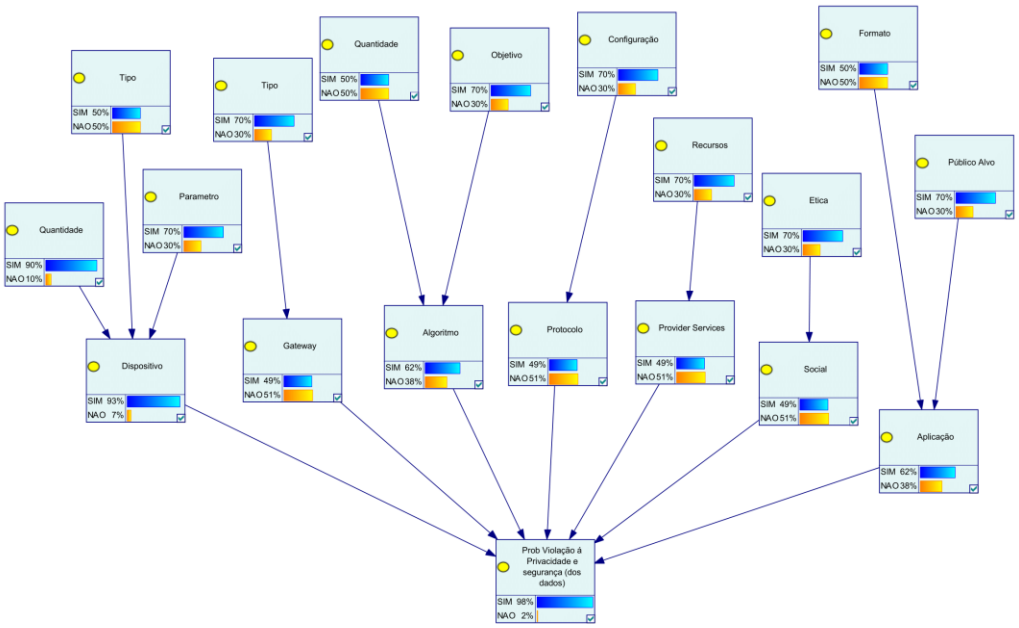
Os cenários foram simulados no GeNIe, sendo representados na Figura 12, 13 e 14.

Figura 12 – Experimento 1 - Cenário 1



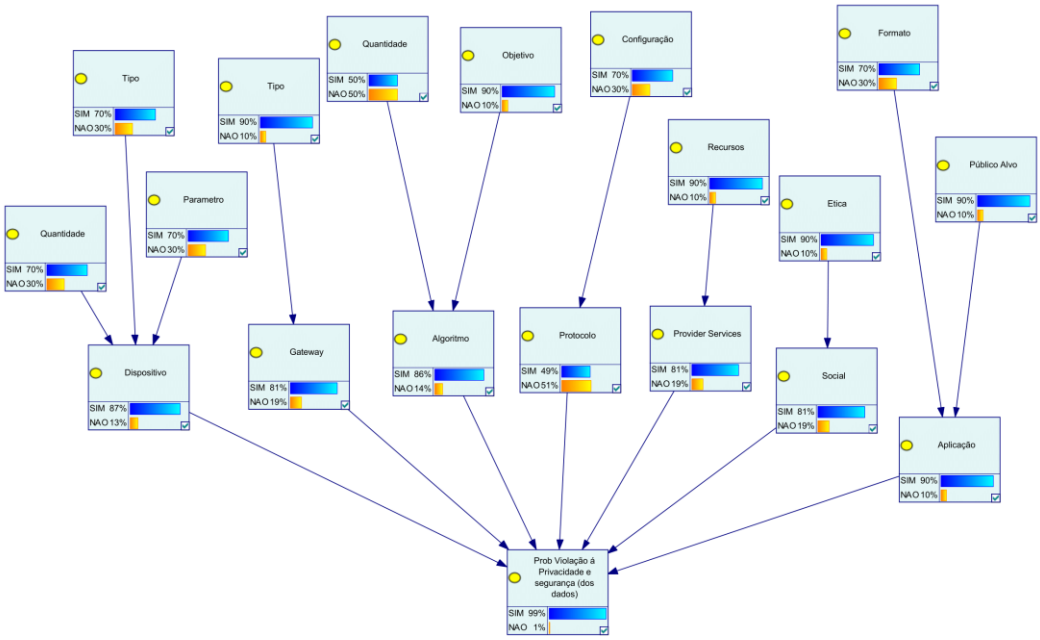
Fonte: Autor

Figura 13 – Experimento 1 - Cenário 2



Fonte: Autor

Figura 14 – Experimento 1 - Cenário 3



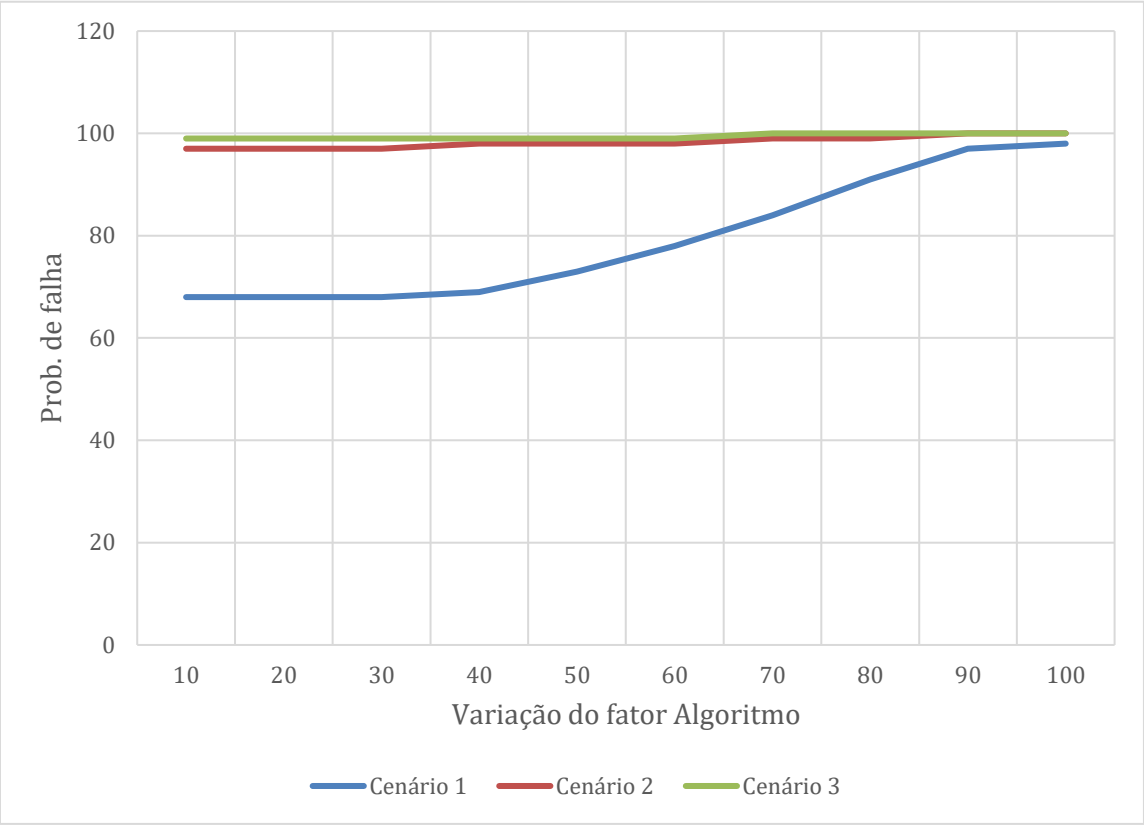
Fonte: Autor

A análise dos cenários permitiu a verificação da aplicação do modelo proposto, uma vez que identificou corretamente as probabilidades de falhas envolvidas. No cenário três ao envolver vidas humanas, foi classificada pelo modelo como nível 1. Essa classificação permitiu verificar que os componentes relacionados à coleta dos dados, gateway, atuadores, questões éticas e nível de aplicação são críticos. Em comparação com os outros dois modelos, verifica-se que neste cenário a intervenção de um profissional da área da saúde se faz necessária, bem como indica quais são os pontos vulneráveis e que devem ter maior atenção. O modelo proposto se mostrou efetivo e coerente nas situações onde foi aplicado e, se mostra útil para identificação de pontos críticos e na remediação dos mesmos.

Baseando-se no cenário 2, uma alteração nos sensores pode provocar danos críticos ao sistema, na medida em que a leitura dos dados, uma vez não realizada ou realizada de forma inconsistente, prejudicará o resultado. Entretanto, podem ser anexados novos sensores para redundância, garantindo a coleta correta dos dados. Neste sentido, os algoritmos envolvidos devem ser aprimorados, tanto nas questões de controle sobre as redundâncias como na quantidade, a fim de garantir que os demais componentes funcionem adequadamente.

Portanto, no segundo experimento o componente algoritmo variou de 0 a 100%, simulando o efeito da variação deste fator na classificação de falhas dos sistemas (Figura 15).

Figura 15 - Experimento 2 - Variação da prob. de falha do Algoritmo

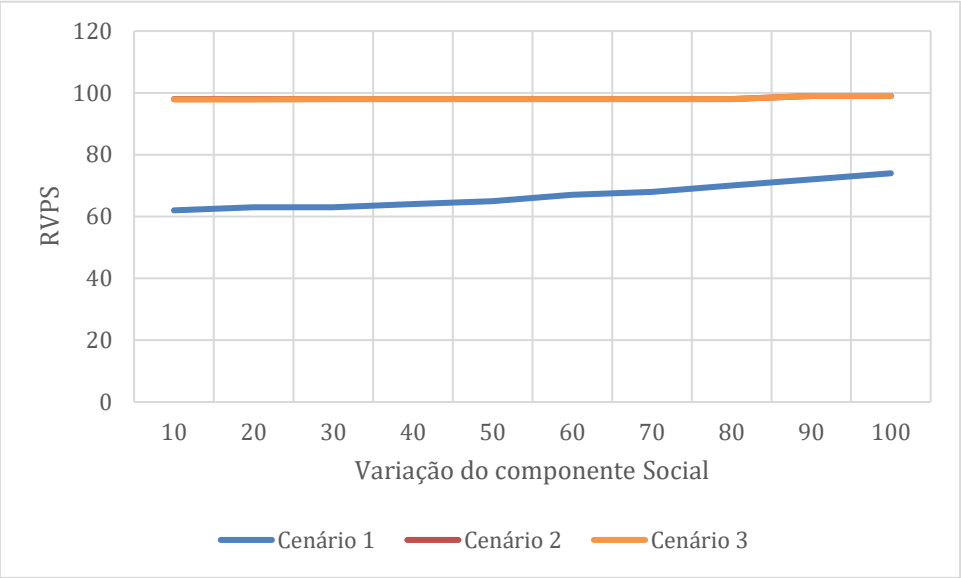


Fonte: Autor

No experimento 2, nota-se que a classificação dos sistemas não se altera, permanecendo Cenário 3, Cenário2, Cenário 1.

Uma vez que na revisão da literatura há escassez de trabalhos incluindo o componente social em uma análise sistêmica e também se trata de um fator classificado entre os mais impactantes após a aplicação da técnica Delphi. Este componente foi escolhido também para o Experimento 2.

Figura 16 - Experimento 2 – Variação da prob. de falha do componente Social



Fonte: Autor

No experimento 2 reforçou o impacto para os cenários propostos, no cenário 2 e 3 o impacto fica próximo de 100%, demostrando a seriedade dos cenários.

6. CONCLUSÕES

Neste trabalho a modelagem usando redes Bayesianas é proposta para avaliar a probabilidade de falha em redes IoT. Os componentes foram identificados na revisão sistemática da literatura e validados por especialistas.

A aplicação de métodos numéricos facilita a variação da probabilidade de falhas do desafio abordado, principalmente no processo de verificação de falhas em sistemas complexos, pois se trata de uma tarefa árdua e onerosa. As técnicas delphi e noisy-OR foram utilizadas para reduzir a quantidades de componentes, identificando os de maior relevância. A principal vantagem dessa combinação de métodos é permitir a conciliação dos aspectos quantitativos e qualitativos para simulação de cenários característicos dos sistemas IoT.

A utilização de Redes Bayesiana neste trabalho, mostrou que uma vez que um dos componentes venha a sofrer modificações em seus parâmetros, é possível demostrar, para avaliar cada cenário, toda a relação de dependência entre os componentes.

Os primeiros resultados demonstram que o modelo proposto pode ser utilizado satisfatoriamente para avaliar a probabilidade de falha em sistemas IoT.

A participação dos 12 especialistas proporcionou ao modelo uma visão real, permitindo a identificação de componentes relevantes. Da mesma maneira os cenários simulados compreendem situações práticas que podem ocorrer no dia a dia desses sistemas de Internet das Coisas e, os resultados obtidos certamente são pertinentes para analisar as falhas recorrentes, e consequentemente darão suportarão decisões no segmento.

Para a teoria, este estudo contribuiu ao abordar de forma sistêmica um conjunto de componentes inerentes às redes IoT por meio de uma combinação de técnicas até então não utilizadas para esse tema.

Como limitação da pesquisa encontra-se a abordagem de apenas um dos desafios que cercam esses sistemas.

Para trabalhos futuros, pretende-se incluir a análise de sensibilidade para avaliar a consistência dos resultados gerados.

Uma outra opção para a continuidade do trabalho seria a inclusão do impacto no modelo desenvolvido, permitindo assim o cálculo de risco nas diferentes aplicações.

7. REFERÊNCIAS

ANJUM. A.; AHMED, T.; KHAN, A.; AHMAD, N.; AHMAD, M. A, M.REDDY, A G.; SABA, T.; FAROOQ, N. Privacy preserving data by conceptualizing smart cities using MIDRAngelization. **SUSTAINABLE CITIES AND SOCIETY**, v. 40, p. 326-334. 2018.

ALBAHRI, O.S.; ALBAHRI, A.S.; ZAIDAN, A.A.; ZAIDAN, B.B.; ALSALEM, M.A.; MOHSIN, A.H.; MOHAMMED, K.I.; ALAMOODI, A.H.; NIDHAL, S.; ENAIZAN, O.; CHYAD, M.A.; ABDULKAREEM, K.H.; ALMAHDI, E.M.; AL SHAFEEY, G.A.; BAQER, M.J.; JASIM, A.N.; JALOOD, N.S.; SHAREEF, A.H. Fault-Tolerant mHealth Framework in the Context of IoT Based Real-Time Wearable Health Data Sensor, **IEEE Access**, v. 7, p.50052-50080, 2019.

ALEXANDRE, N.M.C.; COLUCI, M.Z.O. Validade de conteúdo nos processos de construção e adaptação de instrumentos de medidas. **Ciência & Saúde Coletiva**, v.16, n.7, p.3061-3068, 2011

ALI, F.; KHAND, P.; KWAK, D.; ISLAM, S.M.; ULLAHE, N.; YOO, S.; KWAK, K.S. Type-2 fuzzy ontology-aided recommendation systems for IoT-based healthcare. **Computer** Communications, vol. 119, p. 138-155, 2018.

ATZORI, L.; IERA, A.; MORABITO G.; Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. **AD HOC NETWORKS**, v.56, p. 122-140, 2017.

AZIMI, I.; PAHIKKALA T.; RAHMANI A. M.; NIELA-VILÉN H.; AXELIN, A.; LILJEBERG, P. Missing data resilient decision-making for healthcare IoT through personalization: A case study on maternal health, **Future Generation Computer Systems**, v. 96, p. 297-308, 2019.

BELLUCCI JÚNIOR, J. A. B.; MATSUDA, L. M. Construção e validação de instrumento para avaliação do acolhimento com Classificação de Risco. **Rev Bras Enferm**, vol. 65, n. 5, p. 751–757, 2012.

BEN-DAYA, M.; HASSINI, E.; BAHROUN, Z. Internet of things and supply chain management: a literature review. **International Journal of Production Research**, v. 57, ed. 15-16, 2019.

BISWAS, A; GIAFFREDA, R. IoT and cloud convergence: Opportunities and challenges. **2014 IEEE World Forum on Internet of Things (WF-IoT)**, 2014.

EL BOUANANI, S.; EL KIRAM, M. A.; ACHBAROU, O.; OUTCHAKOUCHT, A. Pervasive-Based Access Control Model for IoT Environments. IEEE ACCESS v. 7 p.54575-54585, 2019.

CAVINATO, J. L. Supply chain logistics risks: from the back room to the board room**. International Journal of Physical Distribution & Logistics Management**, v. 34, n. 5, p. 383-389, 2004.

CALLADO, A. L. C.; CALLADO, A. A. C.; ALMEIDA, M. A. A utilização de Indicadores Gerenciais de Desempenho Industrial no Âmbito de Agroindústrias. **Revista Eletrônica Sistemas & Gestão**, v. 2, ed. 2, p.102-118, 2007.

CERVANTES, C.; Poplade, D.; Nogueira, M.; Santos, A. Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. **IFIP/IEEE International Symposium on Integrated Network Management**, 2015

CHANG, She-I; CHANG, Li-Min; LIAO, Jhan-Cyun. Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. **INFORMATION & MANAGEMENT** , v.57, n.6, 2020.

CHWIF, L. Redução de modelos de simulação de eventos discretos na sua concepção: uma abordagem casual. **Tese (Doutorado em Engenharia) – Escola Politécnica da Universidade de São Paulo**, São Paulo, 1999.

CHUNG-LEE, L; WEI, W. J. Action Research on Collaborative Design: A case study. **12th International Conference on Computer Supported Cooperative Work in Design**, 2008.

CRESWELL, J. W.; CLARK, V. L. P. **Pesquisa de Métodos Mistos**. Editora Penso, 2ª ed, 2013

DOMINGUES, F.; Alberto, N.; Leitão, C.; Tavares, C.; Lima, E.; Radwan, A.; Sucasas, V.; Rodriguez, J.; André, P.; Antunes, P. Insole Optical Fiber Sensor Architecture for Remote Gait Analysis-An e-Health Solution, **IEEE Internet of Things Journal** , vol.6, ed. 1, p. 207-214, 2019.

DOUGLAS, W. M. More on spreads and non-arithmetic means, **The Mathematical Gazzete**, v. 88: p-142-144, 2004

ELSAADANY, A.; SOLIMAN, M. Experimental Evaluation of Internet of Things in the Educational Environment. **International Journal of Engineering Pedagogy**, vol. 7 ed.3, p. 50-60, 2017

FEDERAÇÃO DE CIENTISTAS AMERICANOS (FCA). DISRUPTIVE CIVIL TECHNOLOGIES: SIX TECHNOLOGIES WITH POTENTIAL IMPACTS ON US INTERESTS OUT TO 2025, disponível em <https://fas.org/irp/nic/disruptive.pdf>, acessado em: 11/10/2020.

FENTON, N. E.; NOGUCHI, T.; NEIL, M. An Extension to the Noisy-OR Function to Resolve the 'Explaining Away' Deficiency for Practical Bayesian Network Problems.

IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, v. 31, n. 1, p. 2441-2445, 2019

GUERRERO-RODRIGUEZ, J.M.; COBOS-SANCHEZ, C.; GONZALEZ-DE-LA-ROSA, J.J.; SALES-LERIDA, D. An Embedded Sensor Node for the Surveillance of Power Quality. **ENERGIES**. v. 1 . ed. 8, n. 1561, 2019.

GREENGARD, S. The Internet of Things. **Massachusetts Institute of Technology**, 2015.

GIA, T.N; SARKER, V.K; TCARENKO, I; RAHMANI, A.M.; WESTERLUND, T.; LILJEBERG, P.; TENHUNEN, H. Energy efficient wearable sensor node for IoT-based fall detection systems. **MICROPROCESSORS AND MICROSYSTEMS**, 2018.

GYAMFI K.S.; BRUSEY J. ; GAURA, E. ; WILKINS, R. Heartbeat design for energy-aware IoT: Are your sensors alive?. **Expert Systems with Applications**. v. 128, p. 124-139, 2019.

HECKERMAN, D.; MAMDANI, A.; WELLMAN, M.P.REAL-WORLD APPLICATIONS OF BAYESIAN NETWORKS. **COMMUNICATIONS OF THE ACM**, v.38, ed. 3, p-24-25, 1995

HOU, R; KONG, Y.Q.; CAI, B; LIU, H. Unstructured big data analysis algorithm and simulation of Internet of Things based on machine learning. **NEURAL COMPUTING & APPLICATIONS**. v. 32, ed.10, p.5399-5407, 2020.

HU, Z.; BAI Z. ; YANG, Y. ; ZHENG Z. ; BIAN K. ; SONG, L., UAV Aided Aerial-Ground IoT for Air Quality Sensing in Smart City: Architecture, Technologies, and Implementation, **IEEE Network**, vol. 33, 2019.

HYRKAS, K; APPELQVIST-SCHMIDLECHNER, K; OKSA, L. Validating an instrument for clinical supervision using an expert panel. **INTERNATIONAL JOURNAL OF NURSING STUDIES**, v.40, ed.6. p.619-625, 2003.

ISLAM, S. M. R.; Kwak, D.; Kabir, Md. H; Mahmud, H.; Kyung-Suo, K. The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, v.3, p. 678-708, 2015

KITCHENHAM, B. A.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Technical Report – Department of Computer Science, University of Durham, Durham, 2007

KREJCÍ, J.; STOKLASA, J. Aggregation in the analytic hierarchy process: Why weighted geometric mean should be used instead of weighted arithmetic mean. **Expert Systems With Applications.** v. 114, p.97-106, 2018

KUMAR, R. **Research Methodology: a step-by-step guide for beginners**. SAGE Publication Inc, 3th edition, 2011.

LIAO, Y.; DESCHAMPS, F.; ROCHA LOURES, E.; RAMOS, L. Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal. **International Journal of Production Research**, vol. 55, ed. 12, p. 3609-3629, 2017

LIBRANTZ, A. F. H.; COSTA, I.; SPINOLA, M. M.; OLIVEIRA NETO, G.C.; ZERBINATTI, L. Risk assessment in software supply chains using the Bayesian method. **INTERNATIONAL JOURNAL OF PRODUCTION RESEARCH**, 2020.

LIN, Yi-Bing; Lin Yun-Wei; Lin, Jiun-Yi ; Hung, Hui-Nien. SensorTalk: An IoT Device Failure Detection and Calibration Mechanism for Smart Farmin, **Sensors**, vol. 19, ed. 21, 2019

LOMOTEY, R.K.; PRY J.; SRIRAMOJU S. Wearable IoT data stream traceability in a distributed health information system. **Pervasive and Mobile Computing**, v. 40. p. 692-707, 2017

MALI, A.D, Recent Domain-Specific Applications of Artificial Intelligence Using IoT. **International Journal On Artificial Intelligence Tools** , v.28, ed. 7, 2019

MITTELSTADT, B. [a], Ethics of the health-related internet of things: a narrative review. **Ethics and Information Technology**, v.19, n.3, p.157-175, 2017

MITTELSTADT, B. [b], Designing the health-related internet of things: Ethical principles and guidelines. **Information**, v. 8, 2017

MUHAMMED, T.; MEHMOOD, R. ; ALBESHRI, A.; KATIB, I. UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities, **IEEE ACCESS**, v.6, 2018

NAMAZIAN, A.; YAKHCHALI, S. H. ; YOUSEFI, V ; TAMOŠAITIENE, V. Combining Monte Carlo Simulation and Bayesian Networks Methods for Assessing Completion Time of Projects under Risk. **INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH**., v. 16, ed. 24. n. 5024, 2019

OLIVEIRA NETO, G. C.; DE OLIVEIRA, J. C.; LIBRANTZ, A. F. H. Selection of Logistic Service Providers for the transportation of refrigerated goods. **PRODUCTION PLANNING & CONTROL.** v. 28. n. 10. p.813-828, 2017

Organização das Nações Unida News. OMS: custos com saúde já representam 10% do PIB mundial. disponível em: <https://news.un.org/pt/story/2019/02/1660781>, acessado em: 20 de janeiro de 2021.

PATTERSON, R.E.; ENG, C ; HOROWITZ, S.F. ; GORLIN, R ; GOLDSTEIN, S.R. Bayesian comparison of cost-effectiveness of different clinical approaches to diagnose coronary artery disease. **JOURNAL OF THE AMERICAN COLLEGE OF CARDIOLOGY**, v.4, ed.2, p.278-289, 1984.

PEARL, J., FUSION, PROPAGATION, AND STRUCTURING IN BELIEF NETWORKS. **ARTIFICIAL INTELLIGENCE** . v.29, n. 3, p 241-288, 1986.

PURI, V.; KATARIA, A.; SHARMA, V., Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. **TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES** , 2021.

QINGPING S.; JIAN K., RONG W.; HANG Y.; YUN, L.; JIE W. A Framework of Intrusion Detection System based on Bayesian Network in IoT [J]. **INTERNATIONAL JOURNAL PERFORMABILITY ENGINEER**. v.14, n.10, p. 2280-2288, 2018.

RAY, P. Understanding the role of internet of things towards smart e- healthcare services**. Biomedical Research India**, v.28, ed. 4, p. 1604–1609, 2017

ROBINSON, S. Conceptual modelling for simulation Part I: definition and requirements. **JOURNAL OF THE OPERATIONAL RESEARCH SOCIETY.** v. 59, n. 3, p. 278 – 290, 2008

ROUSE, W. B. Failure Management: malfunctions of technologies, organizations and society. **OXFORD**, United Kingdom, 2021.

ROWE, G.; WRIGHT, G. The Delphi Technique: Past, Present, and Future Prospects – Introduction to the Special Issue. **TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE**, v.78, ed.9, p.1487–1490, 2011

RUSSEL, S.J.; NORVING, P. Artificial Intelligence: a Modern Approach. **Upper** Saddle River, New Jersey, 1995

SAREEN, S.; SOOD, S. K.; GUPTA, S. K. Secure Internet of Things-based Cloud Framework to Control Zika Virus Outbreak. **INTERNATIONAL JOURNAL OF TECHNOLOGY ASSESSMENT IN HEALTH CARE**. v.33 n. 1 p.11-18, 2017

SELVAN, N.S.; VAIRAVASUNDARAM, S.; RAVI, L. Fuzzy ontology-based personalized recommendation for internet of medical things with linked open data. **JOURNAL OF INTELLIGENT & FUZZY SYSTEMS**. v. 36, n.5, p.4065-4074, 2019

SHARMA, S.; Chen K.; Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. **IEEE Internet Computing**, vol. 22, ed. 2, p.42-51, 2018

SIRYANI, J; TANJU, B; EVELEIGH, T.J. A Machine Learning Decision-Support System Improves the Internet of Things' Smart Meter Operations. **IEEE INTERNET OF THINGS JOURNAL**, v. 4, ed. 4, 2017.

SOOD, S.K.; MAHAJAN, I. Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus, **Computers in Industry**, v.91, p.33-44, 2017

SUN, F.F.; Wu, C; Sheng, D, Bayesian Networks for Intrusion Dependency Analysis in Water Controlling Systems, **JOURNAL OF INFORMATION SCIENCE AND ENGINEERING**, v. 33, ed 4, 2017.

TAN, E.; HALIM, Z. Health care Monitoring System and Analytics Based on Internet of Things Framework. **IETE Journal of Research**, v.65, ed. 5, 2019.

THIOLLENT, M. Metodologia da pesquisa-ação. **Cortez Editora**, 14 ed. São Paulo 2005.

VHADURI, S.; POELLABAUER, C. Multi-Modal Biometric-Based Implicit Authentication of Wearable Device Users. **IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY**. v.14, n.12, p.3116-3125, 2019.

VIEIRA, G.E.; SOARES, H. F. Simulação Computacional na Análise de um Sistema de Testes de Desempenho Funcional em Empresa de Refrigeradores Domésticos: Um Estudo de Caso. **XI Simpósio de Engenharia de Produção UNESP**, 2004

WANG, L. Environment supervision system for chemical industry park based on IOT. **Chemical Engineering Transactions**, v. 67, 2018.

WANG, X.; MCGILL, T.J; KLOBAS, J.E. I Want It Anyway: Consumer Perceptions of Smart Home Devices. **JOURNAL OF COMPUTER INFORMATION SYSTEMS**. v.60, n. 5, p.437-447, 2020.

WILKERSON, G.; Gupta, A.; Colston, M. Mitigating Sports Injury Risks Using Internet of Things and Analytics Approaches. **Risk Analysis**, v. 38, ed. 7, p.1348-1360, 2018

WOO, M.W.; LEE, J.; PARK, K.. A reliable IoT system for Personal Healthcare Devices. **FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE**. v.78, 2017.

ZAGORECKI, A.; DRUZDZEL, M. J. Knowledge Engineering for Bayesian Networks: How Common Are Noisy-MAX Distributions in Practice?. **IEEE TRANSACTIONS ON SYSTEMS MAN CYBERNETICS-SYSTEMS**, v.43, n. 1, p.186-195, 2013.

ZHANG, H.; ZHANG, Q.; LIU, J.; GUO, H. Fault Detection and Repairing for Intelligent Connected Vehicles Based on Dynamic Bayesian Network Model. **IEEE INTERNET OF THINGS JOURNAL.**v. 5. ed 4, 2018.

ZHANG, Q; XU, DL. Security authentication technology based on dynamic Bayesian network in Internet of Things, **JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING**, v. 11, ed 2, 2020.

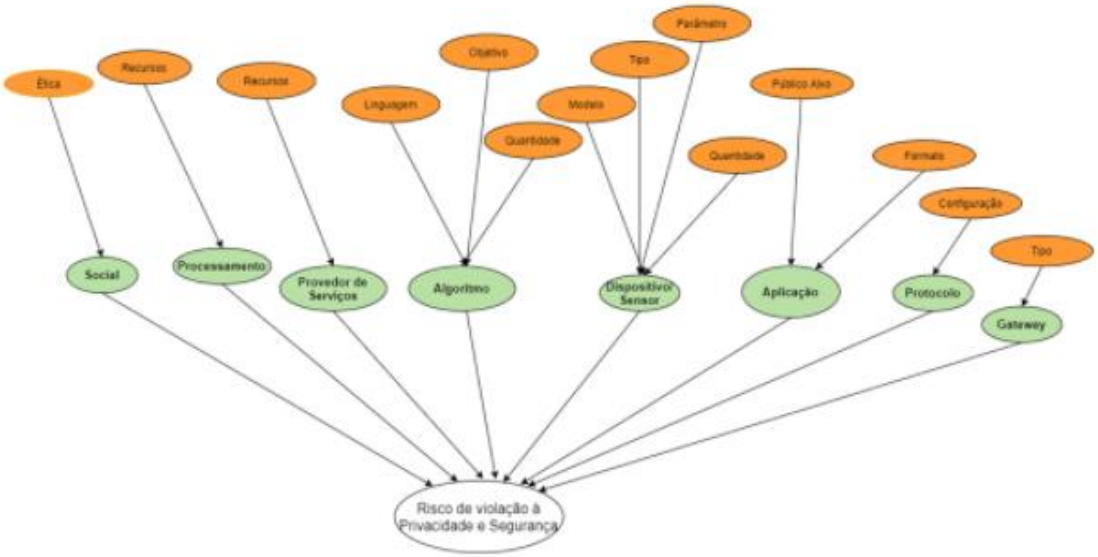
APÊNDICE A - FORMULÁRIO DE COMPONENTES E SUBCOMPONENTES EM PRIVACIDADE E SEGURANÇA DOS DADOS

Componentes e subcomponentes em uma rede IoT na saúde

Objetivo da pesquisa: A rede Internet of Things (IoT) na área da saúde proporcionou diversas facilidades ou conveniências, pois permite a comunicação entre máquinas como acompanhar o desenvolvimento de doenças crônicas, disseminar o controle de doenças, monitorar a queda de idosos. No entanto, essa comunicação pode trazer alguns riscos associados, como a violação de privacidade e segurança dos dados. Assim, neste contexto, este estudo procura identificar os principais componentes e subcomponente extraídos da literatura que interferem na ocorrência desse risco, bem com suas respectivas probabilidades de ocorrência.

*Obrigatório

Modelo



Componente	Conceito	Exemplo
Dispositivo/ Sensor	Responsável por coletar dados sobre sintomas relacionados à saúde e vários eventos dentro e ao redor do ambiente relacionados ao usuário. Os dados são coletados a partir dos dispositivos de hardware sem fio incorporados ao corpo do usuário, dentro e nos arredores do usuário.	Wearable, Dispositivo de saúde pessoal (PHD) vestível
Gateway	Plataforma de gerenciamento de interconexão e serviços; portanto, o gateway é necessário para funcionar como tradutores de protocolo, dispositivos de correspondência de impedância e conversores de	Access point, Wireless Transmission (SIM7000C (NB-IoT))
Algoritmo	Serviços de Provedor. É usado para processamento e análise em tempo real de dados acumulados de sensores baseados em IoT.	incorporado, criptografia, algoritmo genético
Protocolo	Permite a interoperabilidade nas redes heterogêneas e permita a troca de dados sem interrupções em todo o sistema da Internet das	Compartilhamento secreto Shamir, LEACH protocol
Provedor de Serviços	Armazenamento dos dados (criptografados, perturbados ou anonimizados e sem nenhuma informação de identificação pessoal (PIIs)).Podendo optar por terceirizar dados e computação para um provedor de nuvem que fornece infraestrutura para	Nuvem pública e privada
Processamento	estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis. Uma estrutura prática deve garantir que as partes com recursos limitados realizem tarefas de menor complexidade, enquanto as tarefas caras são	Paralelo, distribuído
Social	Interação social através da distância geográfica, participação em grupos e localização. Está conectado à privacidade física.	Ética
Aplicação	Responsável pelo controle e gerenciamento dos dados transferidos para o servidor a partir dos elementos de processamento. [...] Para resolver a falta de comunicação entre	Website, Chat

Qual o nível de relevância do componente, ou seja o quanto seria importante considerar o componente abaixo no contexto de violação à privacidade e segurança (dos dados)? *

	Pouco relevante	Médio	Muito relevante
Dispositivo/ Sensor	○	○	○
Gateway	○	○	○
Algoritmo	○	○	○
Protocolo	○	○	○
Provedor de Serviços	○	○	○
Processamento	○	○	○
Social	○	○	○
Aplicação	○	○	○

No contexto de risco de violação à privacidade e segurança (dos dados), qual a probabilidade do componente falhar? *

	Muito baixa	Baixa	Mediana	Alta	Muito alta
Dispositivo/ Sensor	◯	◯	◯	◯	◯
Gateway	◯	◯	◯	◯	◯
Algoritmo	◯	◯	◯	◯	◯
Protocolo	◯	◯	◯	◯	◯
Provedor de Serviços	◯	◯	◯	◯	◯
Processamento	◯	◯	◯	◯	◯
Social	◯	◯	◯	◯	◯
Aplicação	◯	◯	◯	◯	◯

No contexto de risco de violação à privacidade e segurança (dos dados), qual a importância desse componente dentro da rede? *

	Muito baixa	Baixa	Mediana	Alta	Muito alta
Dispositivo/ Sensor	◯	◯	◯	◯	◯
Gateway	◯	◯	◯	◯	◯
Algoritmo	◯	◯	◯	◯	◯
Protocolo	◯	◯	◯	◯	◯
Provedor de Serviços	◯	◯	◯	◯	◯
Processamento	◯	◯	◯	◯	◯
Social	◯	◯	◯	◯	◯
Aplicação	◯	◯	◯	◯	◯

componente	subcomponente	Conceito	Exemplo(s)
Dispositivo/ Sensor	Quantidade	Número de dispositivos que coletam informações dos pacientes, que podem ser valores extrínsecos e intrínsecos. As características extrínsecas são a temperatura, localização e assim por diante. As características intrínsecas são a pressão arterial, nível de glicose no sangue, batimento cardíaco e assim por diante que são coletados	1 sensor, 2 sensores
	Parâmetro	Refere-se à seleção do conjunto de dados e o que ele representa para o modelo	Dados de localização, saúde, ambiente, meteorológicos
	Tipo	Classificação do sensor em relação a forma como é captado os dados	Smartphone, Weareable
	Modelo	Atributos do dispositivo	Modelo, precisão/acurácia (alta, média, baixa)
Gateway	Tipo	Desempenhar os papéis das infraestruturas físicas e também poderia desempenhar os papéis das infraestruturas de transmissão	SIM7000C
Algoritmo	Quantidade	Número de combinações de algoritmos para atingir o objetivo	1 algoritmo 2 algoritmos
	Objetivo	Os algoritmos devem ser capazes de ajudar a identificar um problema específico e escolher a melhor técnica para isso	Criptografia
	Linguagem	Refere-se à linguagem de programação escolhida para o desenvolvimento da solução para atingir o objetivo	C, JAVA
Protocolo	Configuração	Refere-se ao padrão internacional para comunicação, especifica quando e como os dados são carregados para o servidor ou o comando é baixado pelos dispositivos de detecção e pode influenciar o consumo de energia	I2C de 7 bits
Provider Services	Recursos	Refere-se aos recursos usados na arquitetura de rede IoT, como tipo, escalabilidade e investimento	Cloud, On Premisses
Processamento	Recursos	Refere-se à distribuição da carga de trabalho total de estruturas de preservação de privacidade para seus participantes em relação aos recursos disponíveis para eles. Uma estrutura prática deve garantir que as partes com recursos limitados desempenhem de acordo com a complexidade	Paralelo, Distribuído
Social	Ético	Refere-se a problemas éticos decorrentes dos riscos inerentes à rede IoT, a sensibilidade dos dados relacionados à saúde e seu impacto na prestação de cuidados de saúde. Garantir tecnologia robusta e cientificamente confiável, ao mesmo tempo em que permanece eticamente responsável, confiável e respeitador dos direitos e interesses do usuário.	Direito de possuir e proteger o espaço pessoal. Sentimento de intimidade/ controle, autonomia
Aplicação	Formato(Tipo)	Refere-se a forma os usuários podem adquirir suas informações de interesse	API, Website, Chat
	Público Alvo	Refere-se a quem foi projetado para usar a interface, podendo ser um usuário comum ou o gerente do sistema	Médicos, Hospitais, Pacientes

Qual o nível de relevância do subcomponente, ou seja o quanto seria importante considerar o subfator abaixo na análise de risco de violação à privacidade e segurança (dos dados)? *

	Pouco relevante	Médio	Muito relevante
Quantidade (Dispositivos/ Sensor)	○	○	○
Parâmetro (Dispositivos/ Sensor)	○	○	○
Tipo (Dispositivos/ Sensor)	○	○	○
Modelo (Dispositivos/ Sensor)	○	○	○
Tipo (Gateway)	○	○	○
Quantidade (Algoritmo)	○	○	○
Objetivo (Algoritmo)	○	○	○
Linguagem (Algoritmo)	○	○	○
Configuração (Protocolo)	○	○	○
Recursos (Provedor de Serviços)	○	○	○
Recursos (Processamento)	○	○	○
Ética (Social)	○	○	○
Formato (Aplicação)	○	○	○
Público alvo (Aplicação)	○	○	○

No contexto de risco de violação à privacidade e segurança (dos dados), qual a probabilidade do subcomponente falhar? *

	Muito baixa	Baixa	Mediana	Alta	Muito alta
Quantidade (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Parâmetro (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Tipo (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Modelo (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Tipo (Gateway)	◯	◯	◯	◯	◯
Quantidade (Algoritmo)	◯	◯	◯	◯	◯
Objetivo (Algoritmo)	◯	◯	◯	◯	◯
Linguagem (Algoritmo)	◯	◯	◯	◯	◯
Configuração (Protocolo)	◯	◯	◯	◯	◯
Recursos (Provedor de Serviços)	◯	◯	◯	◯	◯
Recursos (Processamento)	◯	◯	◯	◯	◯
Ética (Social)	◯	◯	◯	◯	◯
Formato (Aplicação)	◯	◯	◯	◯	◯
Público alvo (Aplicação)	◯	◯	◯	◯	◯

No contexto de risco de violação à privacidade e segurança (dos dados), qual a importância desse subcomponente dentro da rede? *

	Muito baixa	Baixa	Mediana	Alta	Muito alta
Quantidade (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Parâmetro (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Tipo (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Modelo (Dispositivos/ Sensor)	◯	◯	◯	◯	◯
Tipo (Gateway)	◯	◯	◯	◯	◯
Quantidade (Algoritmo)	◯	◯	◯	◯	◯
Objetivo (Algoritmo)	◯	◯	◯	◯	◯
Linguagem (Algoritmo)	◯	◯	◯	◯	◯
Configuração (Protocolo)	◯	◯	◯	◯	◯
Recursos (Provedor de Serviços)	◯	◯	◯	◯	◯
Recursos (Processamento)	◯	◯	◯	◯	◯
Ética (Social)	◯	◯	◯	◯	◯
Formato (Aplicação)	◯	◯	◯	◯	◯
Público alvo (Aplicação)	◯	◯	◯	◯	◯

Há sugestão de outros subcomponentes?

Sua resposta

O quanto considera útil o modelo sugerido para análise de sistemas IoT? *

	1	2	3	4	5	
Muito baixa	◯	◯	◯	◯	◯	Muito alta

APÊNDICE B – TABELA DE PROBABILIDADE CONDICIONAL

Tabela B-1 - Distribuição da probabilidade condicional do Dispositivo/Sensor - Algoritmo

ALGORITMO

	Quantidade	Objetivo	N. Existir	Existir
1	T	T	43,67%	56,33%
2	T	F	64,66%	35,34%
3	F	T	67,54%	32,46%
4	F	T	100,00%	0,00%

Fonte: Autor

Tabela B-1 - Distribuição da probabilidade condicional do Dispositivo/Sensor - Aplicação

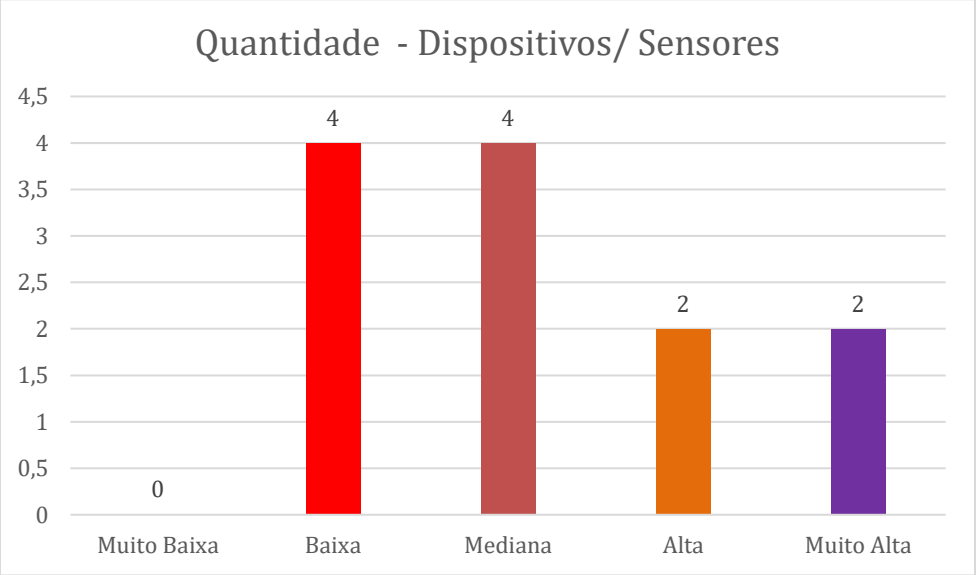
APLICAÇÃO

	Formato(tipo)	Público Alvo	N. Existir	Existir
1	T	T	21,05%	78,95%
2	T	F	46,05%	53,95%
3	F	T	45,70%	54,30%
4	F	T	100,00%	0,00%

Fonte: Autor

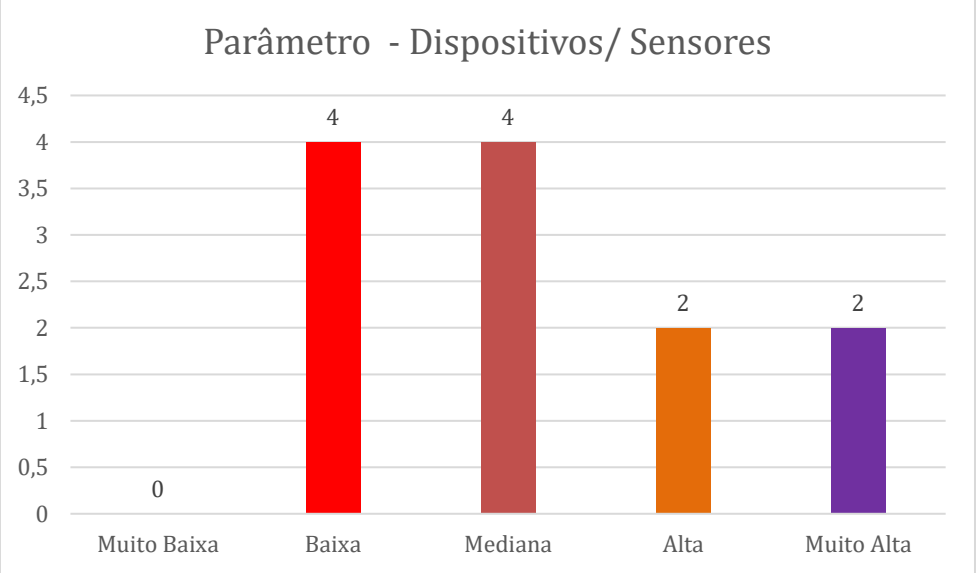
APÊNDICE C – PROBABILIDADE DE FALHA DOS SUBCOMPONENTES

Figura C-1 - Probabilidade de Falha – subcomponente Quantidade (do Dispositivo/ Sensor)



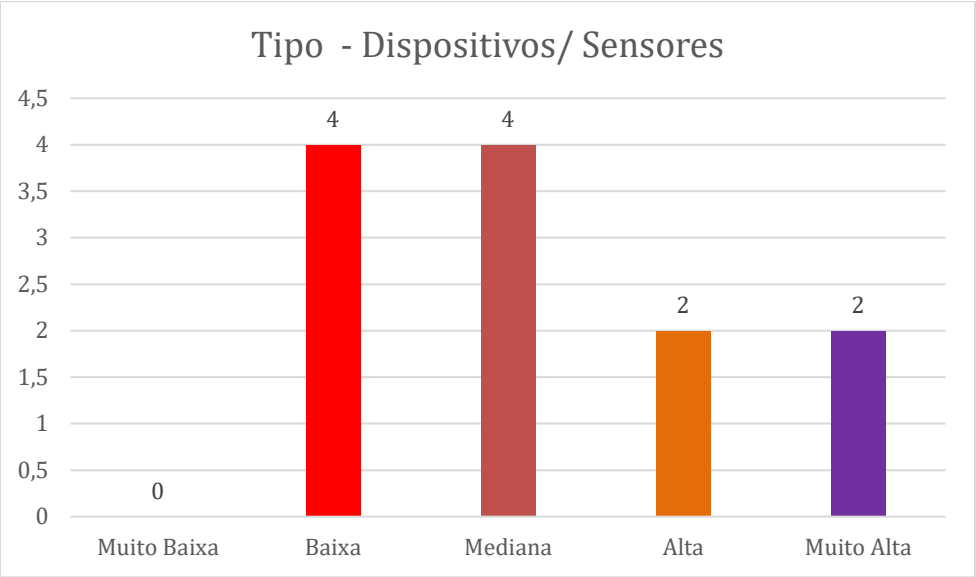
Fonte: Adaptado pela autora do Google Forms

Figura C-2 - Probabilidade de Falha – subcomponente Parâmetro (do Dispositivo/ Sensor)



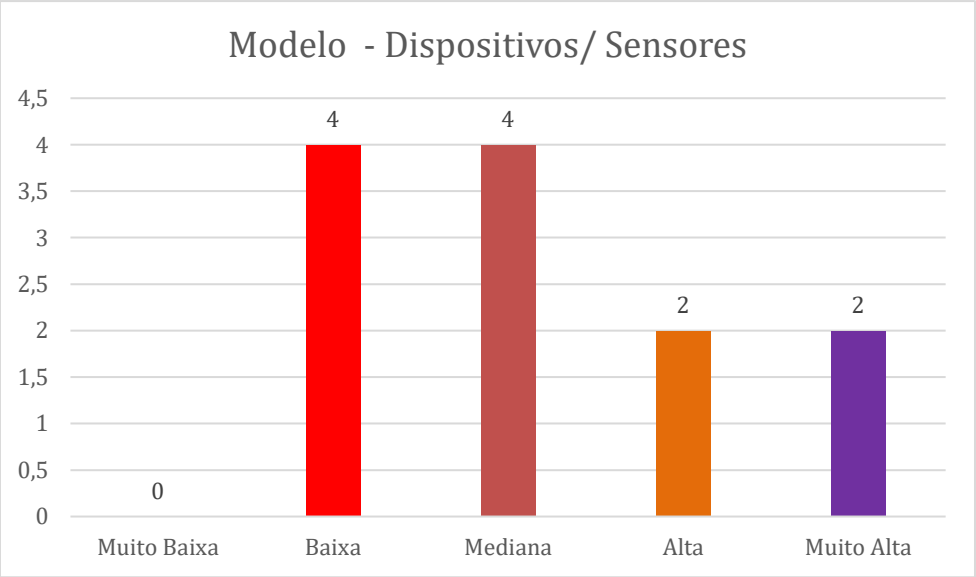
Fonte: Adaptado pela autora do Google Forms

Figura C-3 - Probabilidade de Falha – subcomponente Tipo (do Dispositivo/ Sensor)



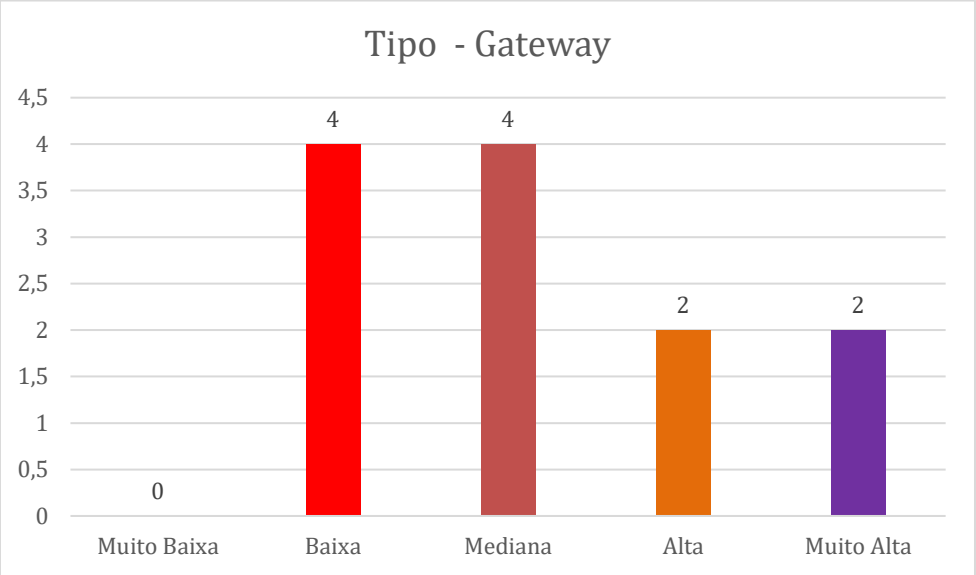
Fonte: Adaptado pela autora do Google Forms

Figura C-4 - Probabilidade de Falha – subcomponente Modelo (do Dispositivo/ Sensor)



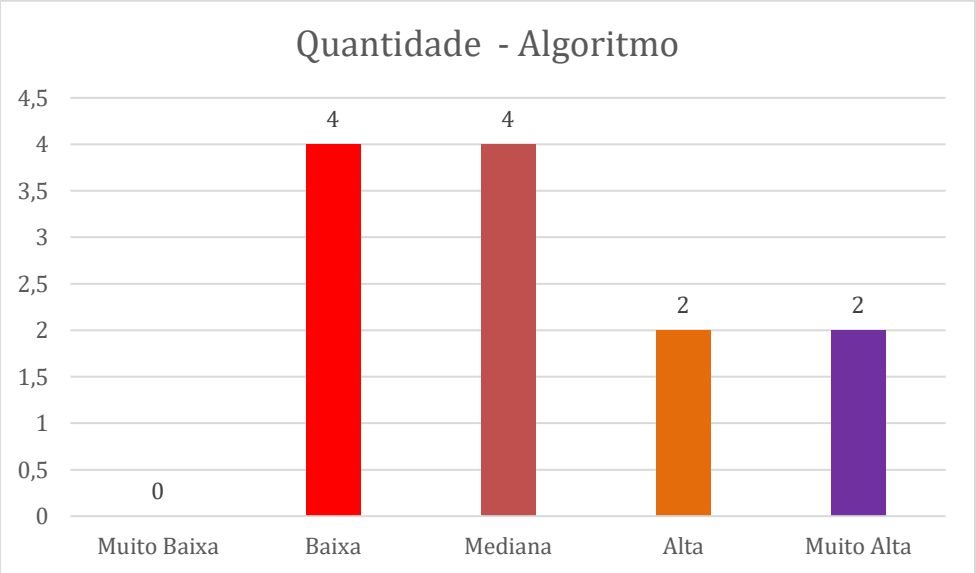
Fonte: Adaptado pela autora do Google Forms

Figura C-5 - Probabilidade de Falha – subcomponente Tipo (do Gateway)



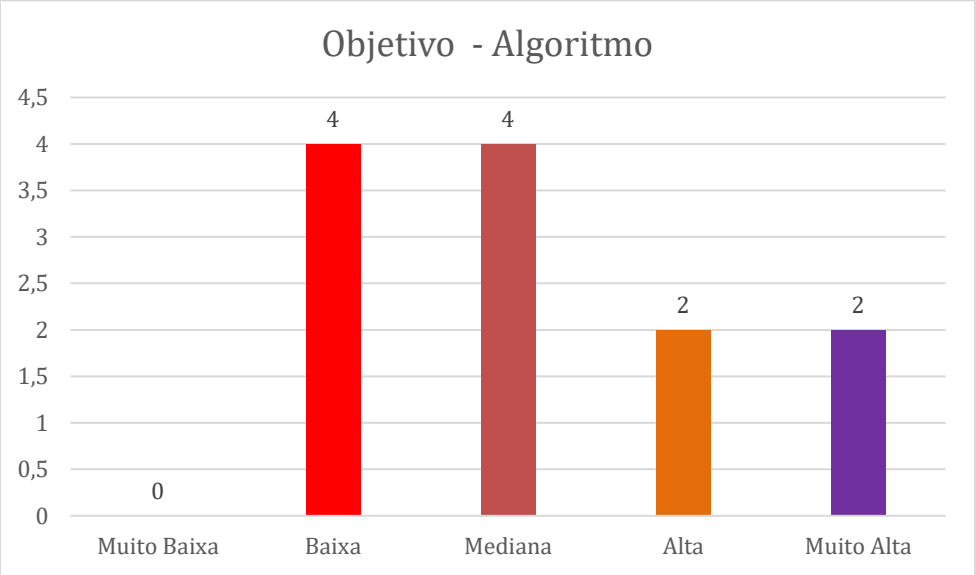
Fonte: Adaptado pela autora do Google Forms

Figura C-6 - Probabilidade de Falha – subcomponente Quantidade (do Algoritmo)



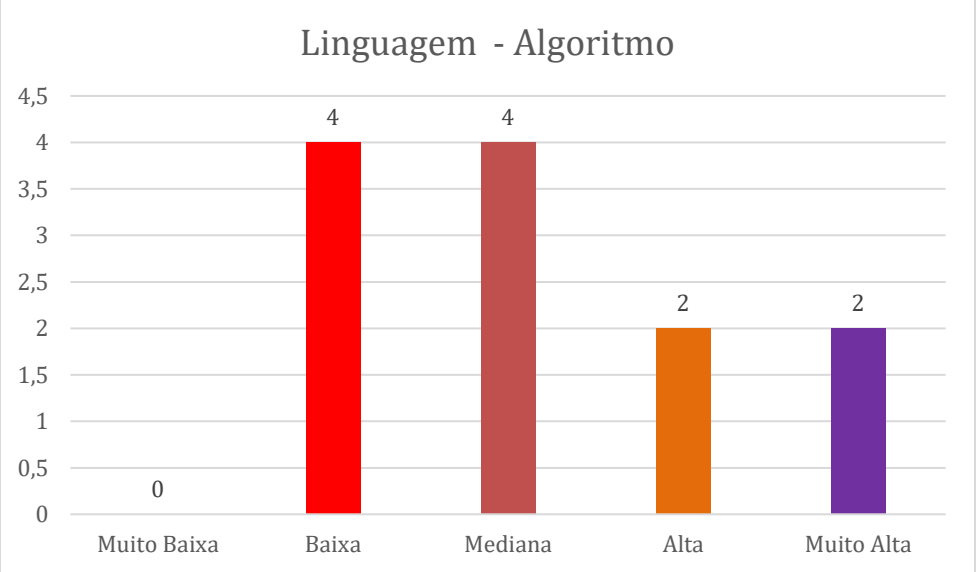
Fonte: Adaptado pela autora do Google Forms

Figura C-6 - Probabilidade de Falha – subcomponente Quantidade (do Algoritmo)



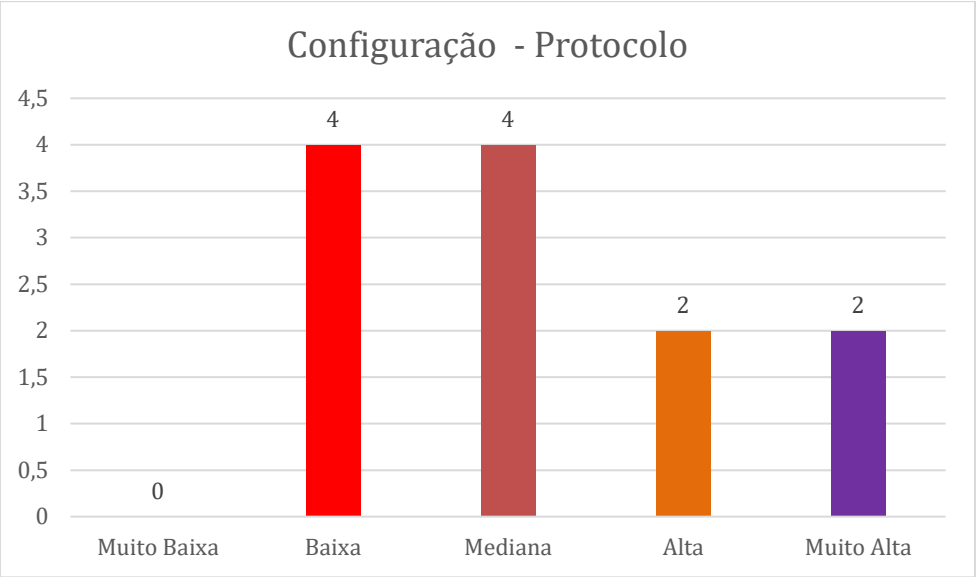
Fonte: Adaptado pela autora do Google Forms

Figura C-7 - Probabilidade de Falha – subcomponente Linguagem (do Algoritmo)



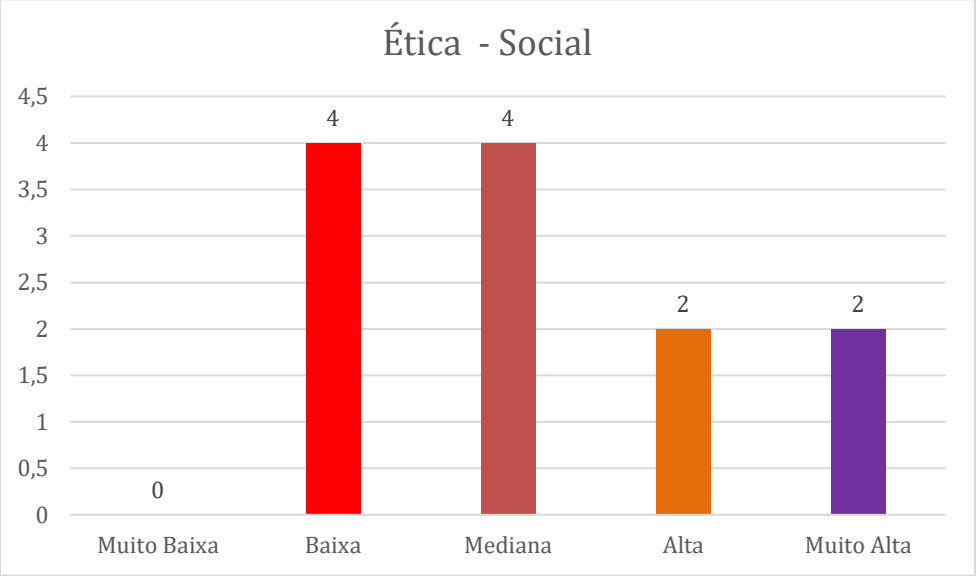
Fonte: Adaptado pela autora do Google Forms

Figura C-8 - Probabilidade de Falha – subcomponente Configuração (do Protocolo)



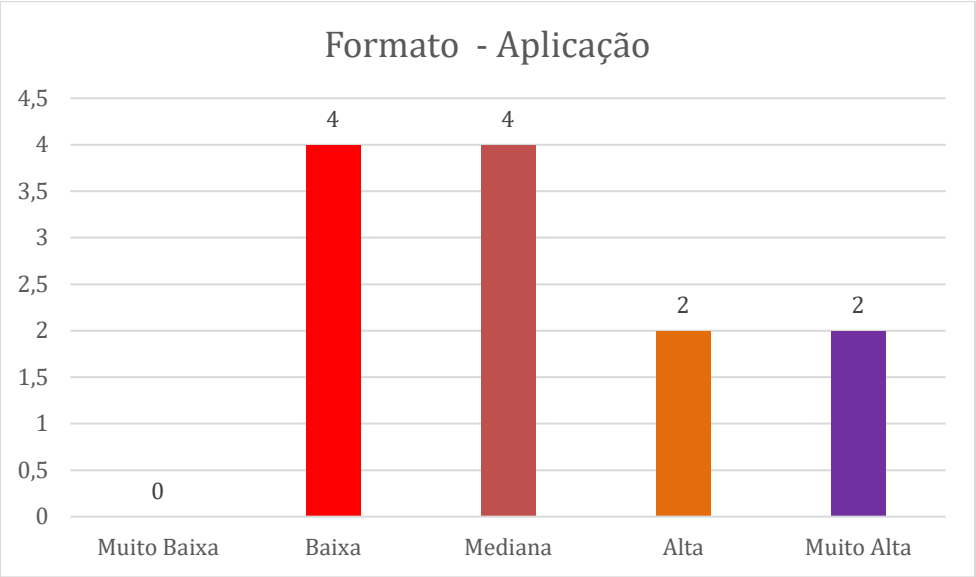
Fonte: Adaptado pela autora do Google Forms

Figura C-9 - Probabilidade de Falha – subcomponente Ética (do Social)



Fonte: Adaptado pela autora do Google Forms

Figura C-10 - Probabilidade de Falha – subcomponente Formato (da Aplicação)



Fonte: Adaptado pela autora do Google Forms