UNIVERSIDADE NOVE DE JULHO – UNINOVE
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO

ERIKA MIDORI KINJO

MODELAGEM E SIMULAÇÃO PARA ESTIMATIVA DE RISCO DE FALHA EM REDES IOT POR MEIO DE REDES BAYESIANAS E MÉTODO MONTE CARLO

SÃO PAULO
2024

ERIKA MIDORI KINJO

MODELAGEM E SIMULAÇÃO PARA ESTIMATIVA DE RISCO DE FALHA EM REDES IOT POR MEIO DE REDES BAYESIANAS E MÉTODO MONTE CARLO

Tese 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 Doutorado.

Professor Dr. André F. H. Librantz - Orientador

SÃO PAULO
2024

Kinjo, Erika Midori.
Modelagem e simulação para estimativa de risco de falha em redes IOT por meio de redes bayesianas e método Monte Carlo. / Erika Midori Kinjo. 2024.
113 f.
Tese (Doutorado)- Universidade Nove de Julho - UNINOVE, São Paulo, 2024.
Orientador (a): Prof. Dr. André Felipe Henriques Librantz.
1. Internet das coisas. 2. Redes bayesianas. 3. Monte Carlo. 4. Risco. 5. Modelagem. 6. Simulação.

I. Librantz, André Felipe Henriques. II. Título

CDU 004

PARECER – EXAME DE DEFESA

Parecer da Comissão Examinadora designada para o exame de defesa do Programa de Pós-Graduação em Informática e Gestão do Conhecimento a qual se submeteu a aluna Erika Midori Kinjo.

Tendo examinado o trabalho apresentado para obtenção do título de “Doutor(a) em Informática e Gestão do Conhecimento”, com Tese intitulada “MODELAGEM E SIMULAÇÃO PARA ESTIMATIVA DE RISCO EM REDES IOT POR MEIO DE REDES BAYESIANAS E MÉTODO MONTE CARLO”, a Comissão Examinadora considerou o trabalho:

(X) Aprovada **( ) Aprovada condicionalmente**

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

EXAMINADORES

Prof. Dr. André Felipe Henriques Librantz - Uninove (Orientador)

_____

Prof. Dr. Fellipe Silva Martins - Mackenzie (Membro Externo)

_____

Prof. Dr. Edson Melo de Souza - UNINOVE (Membro Externo)

_____

Prof. Dr. Cleber Gustavo Dias - Uninove (Membro Interno)

_____

Prof. Dr. Sidnei Alves de Araújo - Uninove (Membro Interno)

_____

São Paulo, 02 de maio de 2024

AGRADECIMENTO

Gostaria de expressar minha mais profunda gratidão à minha mãe, Suely, pela sua paciência, compreensão e força foram fundamentais para que eu pudesse enfrentar os desafios e seguir em frente, mesmo nos momentos mais difíceis. Sem seu apoio inabalável, este trabalho não teria sido possível. Sua presença ao meu lado é uma fonte constante de inspiração e motivação.

Agradeço também aos meus amigos e colegas de trabalho, cujo apoio foi indispensável durante este período de intensas atividades acadêmicas. Agradeço pelas conversas encorajadoras, distrações bem-vindas e apoio moral, ajudaram a tornar esta jornada mais suportável e enriquecedora. Suas palavras de incentivo e sua companhia foram uma fonte vital de força e alegria.

Gostaria de expressar minha profunda gratidão ao meu orientador Professor Dr. André F. H. Librantz, cuja orientação e apoio foram fundamentais para a realização desta tese. Obrigado por acreditar no meu potencial e por me guiar com tanta dedicação. Este trabalho é, em grande parte, resultado do seu apoio e da sua orientação experiente.

A todos vocês, minha sincera gratidão por serem parte tão essencial desta realização.

RESUMO

O avanço da tecnologia da Internet das Coisas (IoT) tem revolucionado diversas áreas, tais como: auxílio no monitoramento de pessoas idosas, melhoria de salas de aulas, automação de casas inteligentes, monitoramento de plantações, entre outros. No entanto, há pesquisas de mercado que relatam números preocupantes relacionados a falhas na implantação de projetos de IoT, inclusive falhas que inviabilizam o seu uso. Como consequência, a questão da privacidade e segurança de dados recebeu destaque como um dos temas mais citados dos trabalhos na área. Diante desse cenário, a proposta desse trabalho é modelar um sistema, combinando técnicas de Redes Bayesianas com Monte Carlo, que possibilite simular e mensurar o risco nas redes de Internet das Coisas – IoT. A metodologia empregada foi a abordagem mista, ao aplicar os métodos escolhidos. O modelo desenvolvido neste trabalho incluiu componentes externos à rede IoT em um modelo já estabelecido na representação de redes de sistemas, e foi denominado OSI*. A falta de padronização ao representar uma rede aliada a não inclusão de componentes externos corroborando com a análise da criticidade levantada neste trabalho. O modelo desenvolvido permitiu avaliar o risco de falha da rede IoT no contexto de privacidade e segurança dos dados.

Palavras-chave: Internet das coisas, Redes Bayesianas, Monte Carlo, Risco, Modelagem, Simulação

ABSTRACT

The advancement of Internet of Things (IoT) technology has revolutionized several areas, such as: helping to monitor elderly people, improving classrooms, smart home automation, monitoring crops, among others. However, there are market researches that report worrying numbers regarding failures in the implementation of IoT projects, including failures that even make their use unfeasible. As a result, the subject of privacy and data security was highlighted as one of the most cited subjects in works in the area. So, in this scenario this work aims to contribute, by using Bayesian Networks combined with Monte Carlo to model a system that makes possible to simulate and measure risk in the internet of things network - IoT. The methodology used was a mixed approach, when applying the chosen methods. The model developed in this work included components external to the IoT network in a model already established in the representation of systems networks and was called OSI*. The lack of standardization when representing a network combined with the non-inclusion of external components corroborates the analysis of the criticality raised in this work. The model developed allowed us to evaluate the risk of failure of the IoT network in the context of data privacy and security.

Key words: Internet of things, Bayesian networks, Monte Carlo, Risk, Modeling, Simulation

Lista de Siglas

5G – 5ª Geração da tecnologia de celular sem fio
ABINC - Associação Brasileira de Internet das Coisas
CCPA - California Consumer Privacy Act (Lei de Proteção de Privacidade do Consumidor da Califórnia)
CIA - Concepção, Implementação e Análise
CI – Critério de Inclusão
CE – Critério de Exclusão
CRC - Verificação Cíclica de Redundância (Cyclic Redundancy Check)
DAG – Grafo Acíclico Direcionado (Directed Acyclic Graph)
DDoS - Distributed Denial of Service
GDPR - Regulamento Geral de Proteção de Dados
GPS - Global Positioning System (Sistema de Posicionamento Global)
ISO - International Organization for Standardization
IoT – Internet of Things (Internet das Coisas)
IIoT – Industrial Internet of Things
Ipv4 - Internet Protocol versão 4
iPV6 - Internet Protocol versão 6
MMC – Método de Monte Carlo
OSI - Open System Interconnection
PII – Informação de identificação pessoal (Personally identifiable information)
PPQR - Privacy-Preserving MAX/MIN Range Queries
PRISMA - Preferred Reporting Items for Systematic reviews and Meta-Analyses
RSL – Revisão Sistemática da Literatura
RB – Redes Bayesianas (Bayesian Network)
RFID – Identificação por Radiofrequência
RPPSD – Risco de Perda de Privacidade e Segurança dos Dados
SIoT - Social Internet of Things
TPC – Tabela de Probabilidade Condicional
TCP - Transmission Control Protocol/Internet Protocol
TLS/SSL - Transport Layer Security /Secure Sockets Layer
UDP - User Datagram Protocol

Lista de Ilustrações

Lista de Tabela

SUMÁRIO

1. INTRODUÇÃO

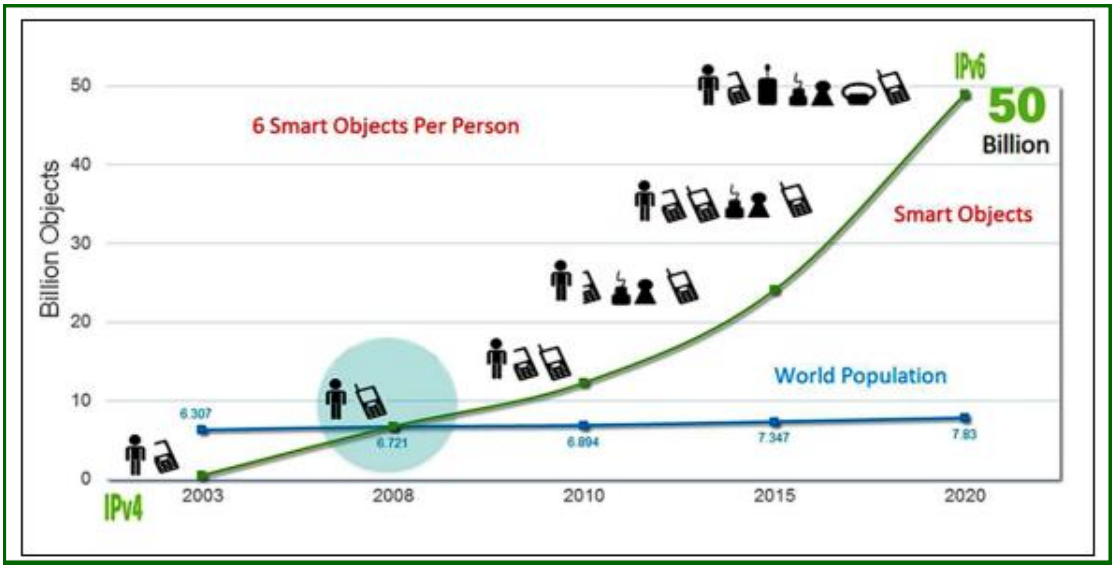
A Internet das Coisas (IoT, do inglês *Internet of Things*) é um conceito que reflete a interconexão de pessoas e objetos a qualquer hora e em qualquer lugar, podendo impactar diversos aspectos dos negócios. Trata-se da interconexão de objetos e dispositivos inteligentes identificáveis dentro da infraestrutura de uma rede, estendendo os benefícios para além da relação entre máquinas (ISLAM, 2015).

De acordo com a Associação Brasileira de Internet das Coisas (ABINC) e Nižetić *et al.* (2020), as transformações advindas do uso dessa tecnologia já são amplamente observadas e novas mudanças ainda estão por vir. Essa tecnologia faz parte do cotidiano das pessoas, viabilizando uma ampla gama de aplicações e benefícios, como casas inteligentes, eficiência no transporte, melhoria nos cuidados com a saúde (SALAGARE, 2020), auxílio no processo de aprendizado (ELSAADANY, 2017) e otimização na agricultura (LIN, 2019; FAROOQ, 2019).

Em 2022, a IoT Analytics estimou a quantidade global de dispositivos conectados, demonstrando que essa tecnologia está cada vez mais presente no cotidiano das pessoas. Espera-se que mais de 125 bilhões de dispositivos IoT estejam conectados até 2030, e que os investimentos em tecnologias de IoT alcancem mais de 120 bilhões de dólares até 2021, com uma taxa de crescimento anual de aproximadamente 7,3% (NIŽETIĆ *et al.*, 2020).

Segundo Al-Sarawi (2020), a previsão é que o mercado global de IoT cresça 39% ao ano entre 2026 e 2030. Dessa forma, a expectativa é que o setor de saúde invista 34,538 bilhões de dólares, seguido pelo setor de energia, com um investimento previsto em torno de 16 bilhões de dólares em IoT até 2030. A CISCO (2017) prevê que a quantidade de dispositivos conectados aumente quase seis vezes até 2051. A Figura 1 destaca o crescimento do uso dos dispositivos inteligentes:

Figura 1 - Crescimento do Uso de Dispositivos Inteligentes



Fonte: Aydos (2019)

Como mencionado anteriormente, à medida que a quantidade de dispositivos conectados aumenta, a complexidade da rede também cresce, e questões técnicas precisam de atenção durante a implantação dos projetos de IoT (NIŽETIĆ *et al.*, 2020). A CISCO (2017) aponta que 60% das iniciativas de IoT param no estágio de viabilidade técnica e apenas 26% das empresas obtiveram sucesso total nos projetos de implantação dessa tecnologia. Além disso, um terço dos projetos concluídos não foram considerados bem-sucedidos.

A pesquisa da CISCO foi conduzida com o objetivo de obter informações sobre o sucesso de projetos de IoT, contando com a participação de 1.845 tomadores de decisão de TI e negócios. Os participantes, oriundos dos Estados Unidos, do Reino Unido e da Índia, estavam distribuídos em diversos setores – manufatura, governo local, varejo/hospitalidade/esportes, energia e saúde – e todos os decisores estavam envolvidos na estratégia geral ou na direção de pelo menos uma das iniciativas de suas organizações.

Para apoiar o rápido desenvolvimento das tecnologias de IoT, bem como explorar novas áreas de aplicações potenciais, é necessário resolver questões técnicas específicas. Entre essas questões, podemos citar: ferramentas para o monitoramento

operacional da rede (KAKKAVAS, 2020), bugs de software, manutenção e problemas com o gerenciamento de segurança (ALMUSAYLIM, 2020).

A compreensão dos componentes da rede IoT e de sua organização (a arquitetura) é essencial para auxiliar na elaboração dos projetos e superar os desafios técnicos dessas tecnologias (SANTOS, 2020; NIKOUI, 2021; BRINGHENTI, 2023). Uma rede IoT é composta por elementos como sensores, gateways, algoritmos, protocolos, provedores de serviços e processamento (KINJO, 2022; SOOD, 2017; SHARMA, 2018; MUHAMMED, 2018; WANG, 2018).

De acordo com Alshohoumi (2019), não existe uma arquitetura padrão para representar uma rede IoT. No entanto, os trabalhos analisados mostram que a rede é representada por um modelo de camadas que varia em termos de quantidade e nomenclatura das camadas. Em alguns casos, até mesmo as políticas de segurança do local onde as redes estão inseridas podem impactar a arquitetura adotada (VIBHUTE, 2019).

Ao compreender como os componentes da rede estão organizados torna-se possível simular projetos e, possivelmente, minimizar perdas antes de sua implementação. A pesquisa IoT Signals da Microsoft aponta que uma das principais causas de falhas na implementação de redes de IoT são os altos custos para escalar os projetos. Tran-Dang (2020) destacou esses custos elevados ao implantar tecnologias IoT no transporte logístico, como, por exemplo, etiquetas RFID, GPS e sensores.

Entre os desafios técnicos enfrentados na implantação da rede, destaca-se a necessidade de medidas de segurança. E o fator humano está associado a essas medidas, que requerem atenção especial. Portanto, questões éticas e sociais relacionadas aos indivíduos que interagem com a rede podem influenciar o sucesso da aplicação da rede IoT (NAYAK, 2022).

Com o objetivo de auxiliar no sucesso da implantação dos projetos e na utilização das redes IoT, este trabalho desenvolveu um modelo que possibilitou a identificação de possíveis falhas na rede IoT e a mensuração dos riscos. Conforme destacado na literatura e na pesquisa da CISCO, a privacidade e a segurança dos dados trafegados nessas redes foram identificadas como preocupações críticas ao utilizar a rede. É

nesse contexto que este trabalho abordou o risco de perda da privacidade e segurança dos dados na rede IoT.

Para compreender o funcionamento das redes IoT, foram utilizadas técnicas de modelagem e simulação para avaliar o risco de perda de privacidade e segurança dos dados, combinando técnicas de Redes Bayesianas com o Método de Monte Carlo. A inclusão da técnica de Monte Carlo no modelo proporcionou uma melhor compreensão da problemática da privacidade e segurança dos dados em redes IoT, permitindo a mensuração do problema.

1.1. CONTEXTUALIZAÇÃO DO TEMA

O termo "Internet das Coisas" não é novo. Foi apresentado, primeiramente, por Kevin Ashton em 1999 (GREENGARD, 2015). No entanto, somente a partir de 2009, com o avanço das conexões via web, começou a ser utilizado na prática (ASSOCIAÇÃO BRASILEIRA DE INTERNET DAS COISAS). Atualmente, com a melhoria das conexões móveis, como o 5G, o conceito está ganhando mais força, pois essas tecnologias oferecem maior capacidade e disponibilidade dos dispositivos conectados à rede (PRAKASAM, 2021; HUANG, 2020).

Na teoria, a discussão sobre a Internet das Coisas tem se intensificado. A primeira publicação sobre o tema surgiu com Schoenberger (2002), que se preocupava em entender como a Internet das Coisas poderia ajudar os computadores a compreenderem o mundo. Em seguida, Qiu (2003) apresentou um projeto de recuperação de dados em tempo real, apoiado por etiquetas de identificação por radiofrequência (RFID).

Somente seis anos após a primeira publicação sobre a Internet das Coisas (IoT), Lahlou (2008) abordou a temática da privacidade e segurança dos dados. Em 2010, Atzori se propôs a estudar a implementação de técnicas e aplicações da Internet das Coisas. Mais tarde, em 2014, Borgia propôs tecnologias e protocolos para avançar no desenvolvimento da Internet das Coisas.

Os trabalhos citados demonstram que o assunto continua relevante e que o tema tem recebido cada vez mais contribuições e complexidades à medida que a tecnologia evolui (LI, 2019; HASSOUN, 2023; ECARDT, 2024).

Além disso, a temática das falhas nas redes IoT foi abordada em vários campos de pesquisa por Liu (2012), Luo (2014), Solaiman (2016), Furfaro (2017), Liao (2017), Sahi (2018), Hasan (2019) e Kirchhof (2022).

Entre esses campos de pesquisa, alguns propuseram a criação de modelos com a aplicação de técnicas, como Willers (2016), Pacheco (2018), Byrnes (2019), Coccia (2022) e Zhang (2023).

O modelo proposto por Willers (2016), por exemplo, utilizou a técnica de Monte Carlo para complementar as medições realizadas nos dispositivos da rede e, com isso, gerar chaves criptografadas, garantindo a segurança da rede.

Por outro lado, Pacheco (2018) empregou análises de dados para propor novas arquiteturas para a rede, avaliando o atraso de pacotes de dados e o consumo de energia. Neste trabalho, todas as camadas da rede foram abordadas, e foram aplicados protocolos diferentes em cada uma delas para posterior comparação.

Em contrapartida, o trabalho de Byrnes (2019) utilizou redes bayesianas e a técnica de Monte Carlo para propor uma solução para as falhas na rede. No entanto, ao aplicar essas técnicas, os autores não consideraram os demais componentes da rede nem a relação de dependência entre eles.

Sharma (2021) analisou o problema da integridade dos dados devido ao congestionamento do tráfego na rede e propôs um modelo para auxiliar na solução desse problema utilizando a técnica de Monte Carlo. Neste trabalho, o modelo proposto focou especialmente nos dispositivos/sensores. No entanto, as camadas de apresentação não foram contempladas.

Coccia (2022) utilizou redes bayesianas e a técnica de Monte Carlo para abordar a problemática do monitoramento da temperatura dos sensores na rede. Foi aplicada uma combinação de técnicas para propor um modelo que garantisse o uso eficaz da

energia, evitando altas tensões. Além disso, a técnica de Monte Carlo foi empregada na validação do modelo, com foco nos dispositivos/sensores.

Por sua vez, Mejjaouli (2022) utilizou a técnica de Monte Carlo para apoiar a tomada de decisão em caso de falhas na rede IoT utilizada na cadeia de suprimentos, com o objetivo de mitigar perdas financeiras. No entanto, o resultado proposto não desenvolveu um modelo que incluísse todos os componentes da rede, mas sim uma ferramenta de apoio em caso de falha.

A técnica de redes bayesianas foi empregada por Kinjo *et al*(2022) para avaliar todos os componentes da rede IoT, com o objetivo de identificar possíveis cenários de falhas. O modelo proposto considerava, inclusive, a relação de interdependência entre os componentes da rede. Zhang (2023), por sua vez, abordou a problemática relacionada ao consumo de energia na rede IoT e à perda ou atraso de pacotes. Para validar o experimento, o autor utilizou a teoria estatística e a técnica de Monte Carlo.

Zhang (2023), por sua vez, abordou a problemática relacionada à energia dispendida na rede IoT e a perda ou o atraso de pacotes. Assim, o autor utilizou-se da teoria estatística e Monte Carlo para validar o experimento.

Todos os trabalhos mencionados exemplificam a diversidade de aplicações. Conforme indicado na introdução pela IoT Analytics, a quantidade de dispositivos conectados à rede IoT continuará a crescer, possibilitando uma variedade crescente de aplicações.

No entanto, o alto percentual de falhas em projetos de implantação de redes IoT, evidenciado no estudo da Cisco (Capítulo 1 deste trabalho), destaca a necessidade de implantar projetos gradualmente e sem falhas, dada a alta demanda de investimento.

Não foram encontrados, até o momento, trabalhos que simulem o risco nas redes IoT de forma sistêmica, abordando todos os componentes internos e externos da rede e suas relações de interdependência, e que também reduzam a subjetividade da percepção de especialistas na área utilizando o método de Monte Carlo.

Nos trabalhos existentes, a rede IoT é utilizada e várias problemáticas emergem de sua utilização, tais como: gerenciamento de energia, perda de pacotes de dados, integridade dos dados, privacidade e segurança dos dados. No entanto, privacidade e segurança dos dados foram as questões mais frequentemente citadas.

A poucos trabalhos abordando a avaliação dos riscos na rede IoT de modo sistêmico, mas a quantidade de publicações relacionada aos problemas da utilização da rede IoT é crescente (conforme será detalhado no Capítulo 3 – Revisão da literatura), demonstrando que há interesse da academia pelo tema proposto.

1.2. PERGUNTA DE PESQUISA

Diante do exposto, este trabalho se propõe a responder a seguinte pergunta: como mensurar o risco de falha de redes IoT no contexto de perda de privacidade e segurança de dados de modo sistêmico e reduzindo a subjetividade dos parâmetros de entrada do modelo (percepção dos especialistas)?

1.3. OBJETIVOS GERAIS E ESPECÍFICOS

Neste item são apresentados os objetivos gerais e específicos:

1.3.1. OBJETIVO GERAIS

O objetivo geral deste trabalho é modelar um sistema capaz de simular o risco de falhas em uma rede IoT, substituindo a percepção dos especialistas anteriormente utilizada. Para isso, será empregada a técnica de Redes Bayesianas combinada com o método de Monte Carlo.

1.3.2. OBJETIVOS ESPECÍFICOS

Como objetivo específico, este trabalho apresenta a seguinte proposta:

- Comparar os modelos de representação de uma arquitetura de redes IoT.
- Desenvolver um modelo em camadas para representar uma rede avaliando o contexto de privacidade e segurança de dados.
- Substituir entradas determinísticas (percepção dos especialistas) por métodos estocásticos como parâmetros de entrada.

- Combinar a técnica de redes bayesianas e Monte Carlo para obter modelo capaz de simular a problemática de segurança dos dados

1.4. ESTRUTURA DO TRABALHO

Esta tese foi estruturada em 7 capítulos. No Capítulo 1 há a apresentação da introdução, do problema e da pergunta da pesquisa, bem como os objetivos, as 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 apresenta a metodologia da pesquisa. Continuando, o capítulo 5 mostra os Resultados e as Discussões, contendo a apuração dos valores finais e como foram alcançados. E, finalizando, o Capítulo 6 apresenta as Conclusões.

2. FUNDAMENTAÇÃO TEÓRICA

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

2.1. INTERNET DAS COISAS

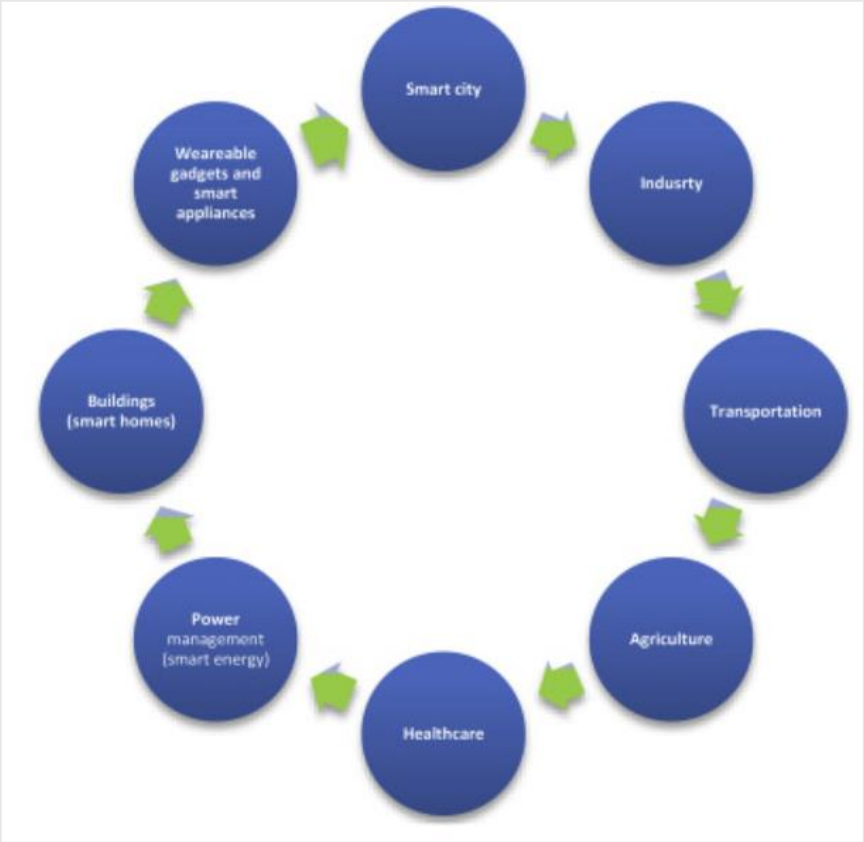
A Internet das Coisas é um fenômeno tecnológico originado de desenvolvimentos inovadores e conceitos em tecnologia da informação e comunicação, associados à: Comunicação ubíqua, computação pervasiva e inteligência ambiental (KÜHNER, 2007), no qual:

- Comunicação Ubíqua: refere-se à prática de incorporar o processamento de informações e a comunicação em rede nos ambientes humanos cotidianos para fornecer continuamente serviços, informações e comunicação. Com isso não se restringe a um só ambiente, podendo estar em movimento constante juntamente com o usuário
- Computação Pervasiva: implica em tornar o comutador “transparente” ao usuário
- Inteligência ambiental: refere-se à capacidade do dispositivo se identificar mudanças no ambiente e com isso se adaptar

Normalmente, dispositivos com capacidade de ubiquidade, pervasividade e inteligência ambiental são descritos como objetos inteligentes. Assim, a internet das coisas é descrita como a rede de objetos físicos (coisas) com inteligência para detectar e interagir com dispositivos associados através da Internet (PRAKASAM, 2021). É a possibilidade de conexão à internet permite o controle remoto desses dispositivos, além de possibilitar seu uso como provedores de serviços.

Essas características criam diversas oportunidades, tanto no setor acadêmico quanto na indústria (SANTOS, 2016). Os objetos que fazem parte da Internet das Coisas incluem computadores, televisores, veículos, smartphones, eletrodomésticos, câmeras, equipamentos médicos, sistemas industriais, além de pessoas, animais e edifícios (Associação Brasileira de Internet das Coisas, 2023[b]). A Figura 2 representa algumas dessas aplicações:

Figura 2 - Aplicações de IoT



Fonte: Nižetić *et al.* (2020)

Essa nova forma de interação propiciada pela IoT representa uma solução em potencial para melhoria da vida das pessoas. Um exemplo é na área médica, onde sensores vestíveis são utilizados para monitorar pacientes à distância.

2.1.1. COMPONENTES DA REDE IoT

Como mencionado anteriormente, há vários dispositivos inteligentes diferentes conectados na rede, como exemplos podemos citar:

- Wearables: dispositivos vestíveis (roupas inteligentes, pulseiras)
- Eletrodomésticos: dispositivos de ventilação e iluminação de uma casa, por exemplo

- Carros: dispositivos instalados em carros/caminhões que auxiliam no processo de transporte e produção

No entanto, esses dispositivos conectados à rede podem causar vulnerabilidades (VALDIVIA, 2020), que estão associadas a possíveis violações da política de segurança, podendo ocorrer devido a fraquezas nas regras de segurança ou a problemas com o sistema. Dessa forma, compreender o funcionamento da rede e sua arquitetura pode ser crucial para analisar os riscos e possíveis vulnerabilidades. Isso permite que os stakeholders façam uma avaliação mais informada sobre as decisões do projeto antes da implementação (SANTOS, 2020).

Por exemplo, uma arquitetura IoT pode ser considerada um sistema que consiste em inúmeros ativos físicos, atuadores, serviços, protocolos, usuários e algoritmos (HUSEYIN, 2018), sendo que cada bloco de uma arquitetura é responsável por funções específicas, como captar dados, transportar dados e comunicar informações para um público específico.

Assim, para cada arquitetura, os elementos internos e externos à rede que podem impactar são: Dispositivo/Sensor, Gateway, Algoritmo, Protocolo, Provedor de Serviços, Social e Aplicação (KINJO *et al.*, 2022).

Tabela 1 - Componentes da Rede IoT

Componentes	Conceito	Exemplo
Dispositivo/ Sensor	Responsável por coletar dados de 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*
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)
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 e algoritmo genético
Protocolo	Permite a interoperabilidade nas redes heterogêneas e permita permite a troca de dados sem interrupções em todo o sistema da Internet das Coisas	Compartilhamento secreto Shamir, *LEACH protocol* (cluster), IKEv2, IPv6, oneM2M
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 forneça infraestrutura para armazenamento e análise.	Nuvem pública e privada
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 pacientes e médicos no atual sistema de monitoramento de saúde	Website, Chat

Fonte: adaptado de (KINJO *et al*, 2022)

2.1.2. ARQUITETURAS DA REDE

Segundo Yaqoob (2017), são necessárias arquiteturas interoperáveis, energeticamente eficientes e seguras para conectar centenas, milhares ou até mesmo milhões de componentes na rede.

Essa arquitetura diz respeito à alocação de funcionalidades, ou seja, à definição da função de cada elemento com a finalidade de organizar o sistema. Ao contrário dos campos tecnológicos mais maduros, como a computação serial, a comunicação digital e a própria Internet, nas quais as bases arquitetônicas são fortes e consolidadas, ainda se buscam princípios arquitetônicos para muitos sistemas emergentes e aplicações, como IoT, sistemas ciberfísicos e inteligência artificial incorporada (CHIANG, 2016; SANTOS, 2020).

Para isso, o termo "IoT architecture" ou "Internet of Things Architecture" foi pesquisado nas bases de dados Web of Science e Scopus, ordenando os resultados de acordo com o número de citações. Essa pesquisa foi relevante para demonstrar que os componentes da rede eram organizados em camadas e que os trabalhos abordavam as limitações em pelo menos uma dessas camadas, ou seja, em um conjunto de componentes.

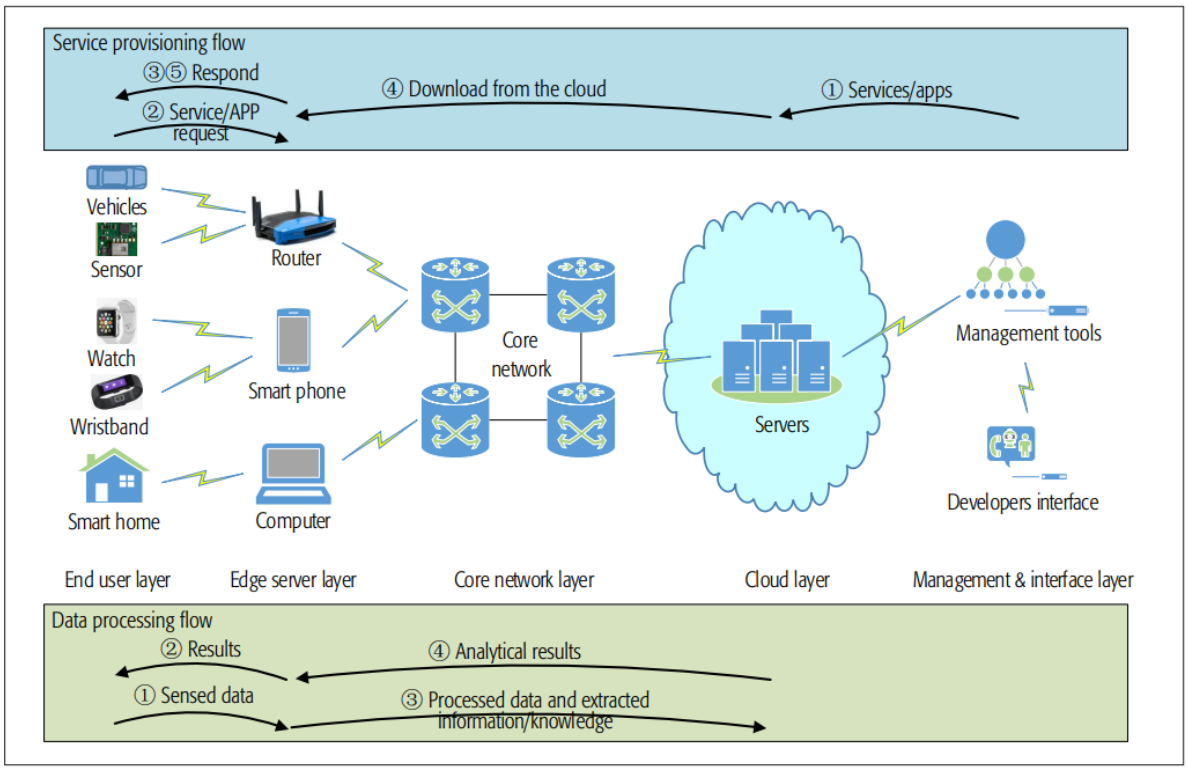
2.1.2.1. PROPOSTA DE ARQUITETURAS

Segundo Yaqoob (2017), a arquitetura de uma rede IoT genérica é composta pelas seguintes camadas: aplicação, transporte e detecção/sensores. A camada de aplicação utiliza computação inteligente para extrair informações valiosas do processamento de grandes volumes de dados e fornece uma interface entre usuários e a rede. A camada de transporte, por sua vez, é responsável pelas operações de rede, enquanto a camada de detecção/sensores tem a função de coletar as informações.

Apesar de facilitar o gerenciamento da rede, existem limitações em relação à segurança na camada de aplicação proposta por Yaqoob (2017).

A proposta de Ren (2017), por sua vez, refere-se a uma arquitetura baseada em nuvem, conforme ilustrado na Figura 3.

Figura 3 - Arquitetura Baseada em Nuvem



Fonte: Ren (2017)

Observamos a existência de 4 camadas principais na arquitetura baseada em nuvem, como segue:

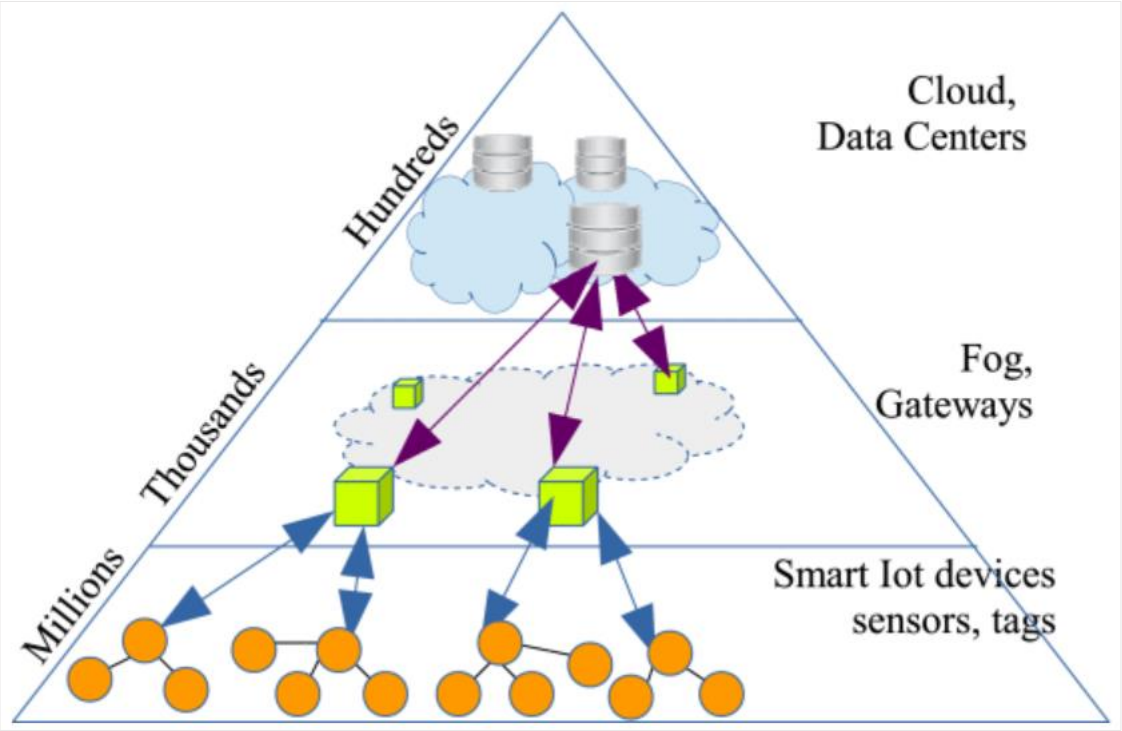
- Camada de usuário final: A camada de usuário final é composta por uma ampla variedade de dispositivos IoT. Por exemplo, nós de sensores, wearables e veículos, com o objetivo de fornecer ou obter dados para usuários finais
- Camada de servidor de borda: responsável pela distribuição de computação, controle, e armazenamento para dispositivos de usuários finais na borda da rede. São exemplos de componentes dessa camada: gateways e roteadores
- Camada de rede principal: é o núcleo da tecnologia de comunicação de longa distância.
- Camada de Nuvem: são responsáveis pelo processo maciço dos dados
- Camada de gerenciamento e interface: A camada de gerenciamento e interface fornece ferramentas de gerenciamento para controlar toda a plataforma IoT e interfaces para desenvolvedores de serviços IoT criarem e publicarem novos serviços/aplicativos

A arquitetura proposta por Ren (2017) é escalável, reduzindo os atrasos nas respostas, utilizando servidores próximos (por meio de serviços locais) e centralizando os recursos. No entanto, ainda existem desafios, como a necessidade de uma plataforma unificada para o gerenciamento de dispositivos heterogêneos.

Por outro lado, Chiang (2016) utilizaram a computação nevoeiro (Fog Computing) para representar a rede IoT. A proposta da computação nevoeiro é estender a computação em nuvem para a borda da rede, permitindo o processamento de dados mais próximo dos usuários finais. O objetivo dessa proposta é reduzir a latência, otimizar o uso da largura de banda e melhorar a eficiência na entrega de serviços em ambientes distribuídos.

Há uma diferença significativa de escala entre a arquitetura nevoeiro e a nuvem, de modo que a nuvem possui enormes capacidades computacionais, de armazenamento e de comunicação em comparação com o nevoeiro. A Figura 4 ilustra os papéis dos data centers em nuvem e os Gateways da computação nevoeiro.

Figura 4 – Arquitetura em Nuvem e Nevoeiro



Fonte: Al-Fuqaha (2015)

A computação em névoa possui os seguintes recursos em uma rede IoT (AL-FUQAHA, 2015):

- Localização: os recursos do Fog são posicionados entre os objetos inteligentes e os data centers em nuvem; proporcionando, assim, melhor desempenho de atraso.
- Escalabilidade: à medida que o número de usuários finais aumenta, o número de “micro” centros de nevoeiro implantados também aumenta para lidar com a carga crescente.
- Tempo real: fornece melhor desempenho para serviços interativos em tempo real.
- Resiliência e Confiabilidade: proporciona a descentralização do processamento e aumenta a resiliência do sistema, tornando-o menos dependente de conexão estável

Entre os maiores desafios na utilização da arquitetura em nevoeiro estão: gerenciamento de recursos, segurança e privacidade dos dados e a integração com a nuvem.

A norma ISO/IEC 30141, "Internet das Coisas (IoT) - Arquitetura de referência", essa norma fornece uma arquitetura de referência de IoT padronizada, que inclui um modelo conceitual genérico que descreve os conceitos das entidades comuns de um sistema de IoT e seus relacionamentos. O modelo conceitual é derivado de um modelo de referência de alto nível, dividido em cinco visões arquitetônicas: funcional, sistema, informação, comunicação e uso (Erazo-Garzón, 2022).

Entre as vantagens de utilizar o modelo proposto pela ISO em redes, destacam-se:

- Padronização: A ISO/IEC 30141 estabelece um conjunto claro de diretrizes e requisitos internacional para avaliações independentes de software. E isso ajuda a garantir consistência e qualidade nos processos de avaliação.
- Confiança do Usuário: adotar padrões reconhecidos internacionalmente, como a ISO/IEC 30141, demonstra um compromisso com a qualidade e a melhoria contínua. Ao adotar um padrão pode acarretar maior confiança dos usuários e parceiros.

No modelo OSI, por exemplo, define as camadas de comunicação em sistema de rede de computadores e foi desenvolvido pela ISO (International Organization for Standardization) com o objetivo de promover a padronização e interoperabilidade de sistemas de redes (PALATTELLA, 2013).

Entre as vantagens de utilizar o modelo OSI em redes, destacam-se:

- Estrutura Organizada: fornece uma estrutura organizada e hierárquica para entender as redes de computadores. Isso é especialmente útil em IoT, onde há uma variedade de dispositivos interconectados. O modelo OSI permite uma análise sistemática e organizada desses sistemas complexos.

- Padronização e Interoperabilidade: promove a padronização e a interoperabilidade entre dispositivos IoT. Ao seguir as diretrizes do modelo, os desenvolvedores podem garantir que seus dispositivos sejam compatíveis com outros dispositivos e protocolos, facilitando a integração e comunicação em ambientes IoT heterogêneos (Tao, 2018).
- Análise e Desenvolvimento: fornece uma estrutura para analisar e desenvolver sistemas IoT, possibilitando examinar como diferentes protocolos e tecnologias se encaixam em cada camada do modelo OSI. E, posteriormente, identificando áreas de melhoria e oportunidades para inovação em sistemas IoT (JAFRI , 2023).

As camadas do modelo OSI foram descritas conforme Tabela 2.

Tabela 2 - Camadas da Rede

Camada	Conceito
Aplicação	Este é o nível com o qual o usuário geralmente interage. É aqui que os dados se transformam em sites, programas de bate-papo e assim por diante.
Apresentação	Formata os dados a serem apresentados à camada de aplicação. Ele pode ser visto como o tradutor
Sessão	Lida com a configuração da sessão, trocas de dados ou mensagens e desativa quando a sessão termina. E monitora a identificação da sessão para que apenas as partes designadas possam participar
Rede	Encarregada de determinar o caminho e o endereçamento lógico. Essa camada fornece endereços lógicos aos pacotes recebidos, o que os ajuda a encontrar seu caminho.
Transporte	Fornece comunicação de ponta a ponta entre processos em execução em diferentes máquinas.
Enlace	Fornece transmissão confiável de dados (quadros) entre nós adjacentes, construída sobre um serviço de transmissão de bit bruto e não confiável fornecido pela camada física. Para conseguir isso, a camada de enlace de dados realiza detecção e controle de erros, geralmente implementados com uma verificação de redundância cíclica (CRC).
Física	Define as especificações elétricas e físicas da conexão de dados. Ele define a relação entre um dispositivo e um meio físico de transmissão (por exemplo, um cabo de cobre ou fibra ótica). Isso inclui o layout de pinos, tensões, impedância de linha, especificações de cabo, sincronismo de sinal, hubs, repetidores, adaptadores de rede, adaptadores de barramento de host (HBA usado no armazenamento) e muito mais

Fonte: KUMAR (2014); MIGLIORE (2021)

A partir dessa descrição, os componentes listados na tabela 3 foram classificados conforme Kumar (2014); Migliore (2021).

Tabela 3 - Relação Componente X Camada

Componente	Camada
Social	
Aplicação	Apresentação e Aplicação
Processamento	Sessão
Provedor de Serviços	Rede
Algoritmo	Transporte
Protocolo	Enlace
Gateway	Enlace
Dispositivo/ Sensor	Física

Fonte: elaborado pelo autor

Na classificação realizada, nota-se que o componente Social foi desconsiderado pois elementos externos à rede não entraram na classificação proposta por Kumar (2014). No entanto, questões Sociais poderiam impactar direta ou indiretamente a camada de Aplicação pois os fatores sociais poderiam estar implícitos no usuário que interage com a rede.

Uma vez que mais dispositivos e, consequentemente, mais pessoas estão conectadas nessa rede, é preciso entender o seu funcionamento para propor políticas ou ferramentas que melhorem o uso (PRAKASAM, 2021).

2.2. PRIVACIDADE E SEGURANÇA DOS DADOS

Conforme destacado anteriormente e ressaltado por Tran-Dang (2020) e Nižetić *et al.* (2020) a Internet das Coisas (IoT) cresceu exponencialmente nos últimos anos, devido a diversos fatores como avanços tecnológicos (IPV6, redes 5G, demanda de mercado, custos). No entanto, essa expansão trouxe vários desafios significativos em relação à privacidade e segurança dos dados. A garantia da privacidade e da segurança dos dados é fundamental por diversas razões tais como:

- Proteção da Privacidade do Usuário: dispositivos IoT coletam uma grande quantidade de dados pessoais e sensíveis dos usuários, como informações de localização, hábitos de consumo, padrões de comportamento e até mesmo dados biométricos. Garantir a privacidade dessas informações é crucial para proteger os direitos e a dignidade dos usuários.

- Conformidade com Regulamentações: muitas regiões do mundo têm leis e regulamentos rigorosos sobre a proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei de Proteção de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos. Empresas que não cumprem essas regulamentações estão sujeitas a multas pesadas e danos à reputação. Portanto, garantir a privacidade e segurança dos dados em redes IoT é necessário para cumprir essas regulamentações.
- Proteção da Infraestrutura Crítica: Em setores como saúde, energia e transporte, dispositivos IoT estão integrados à infraestrutura crítica. Violações de segurança nessas redes podem ter consequências devastadoras, desde a interrupção de serviços essenciais até riscos à segurança pública. Portanto, proteger a segurança dos dados nessas redes é crucial para proteger a infraestrutura crítica e a segurança pública.

A privacidade e a segurança dos dados em redes IoT são essenciais para proteger os direitos e a segurança dos usuários, cumprir regulamentações e proteger a infraestrutura crítica. Empresas e organizações devem implementar medidas robustas de privacidade e segurança para garantir que os benefícios da IoT sejam realizados sem comprometer a segurança e a privacidade dos usuários.

2.3. SOCIAL

As questões de segurança e privacidade são um grande desafio para a IoT. No entanto, são também grandes facilitadores para a criação de um “ecossistema de confiança” (Frustaci, 2018; Nižetić *et al.*, 2020).

Conforme destacado na introdução desse trabalho, o fator ético/social foi considerado um desafio nos projetos de implantação de redes IoT e questões de segurança precisam ser desenvolvidas para supri-las.

Alguns autores referem-se à Internet das Coisas Social (SIoT) como um novo paradigma onde a Internet das Coisas se funde com o conceito de conexões sociais. Desta forma, pessoas e dispositivos interagem e, consequentemente, aumentam/facilitam o compartilhamento de informações (FRUSTACI , 2018; ATZORI, 2012)

Um campo desafiador de implementação de tecnologias de IoT foi detectado no sistema de saúde em geral. No qual o aumento na qualidade do serviço dos sistemas de saúde poderia ser facilitado com o suporte de IoT (principalmente coleta de dados de saúde do paciente).

O monitoramento de várias funções humanas vitais e valiosas, como frequência cardíaca, temperatura da pele, monitoramento de movimento, etc. No entanto esses dados sempre vão para a nuvem remota, muitos tipos de relatórios de análises são produzidos na nuvem e enviam os resultados relevantes para o paciente ou equipe de saúde usando telefone celular ou outros dispositivos ativos.

Dados médicos de pacientes podem ser considerado de alto valor comercial. E algoritmos de mineração de dados podem ser aplicados à IoT para expor informações desconhecidas desses dados (AHMED, 2017).

2.4. RISCO

O conceito de risco surgiu no século XVII e estava relacionado à teoria da probabilidade e aos jogos de azar (BINMORE, 2020). Risco foi definido por Nieto-Morote (2011) como a probabilidade ou frequência de um evento não previsto ocorrer em um determinado intervalo de tempo.

Sendo assim, para avaliar a ocorrência de eventos críticos faz-se necessário a análise do risco. Essa análise existe há quase quatro décadas e consiste na reunião de informações suficientes sobre os riscos para estimar a probabilidade de ocorrência e a consequência da ocorrência (XAVIER, 2009; KERZNER, 2011).

O objetivo principal da análise é revelar e identificar pontos de falha e perigos potenciais em sistemas e operações, permitindo que o tomador de decisão possa corrigi-los antes que se manifestem (ZIO, 2016). Na análise de risco há alguns termos básicos (CIECHANOWICZ, 1997) como:

- Ativo: algo de valor para a organização (computador ou software, rede, informação/dados);
- Impacto: as consequências de um incidente indesejado que afeta um ou mais dos ativos;

- Ameaça: a potencial violação à segurança. As ameaças podem ser ambientais (terremotos ou inundações) ou de origem humana (intencionais ou não);
- Vulnerabilidade: é a característica do ativo ou grupo de ativos que pode ser explorada pela ameaça
- Risco: é a aptidão que uma determinada ameaça explorará da(s) vulnerabilidade(s) de um ativo ou grupo de ativos para causar perdas ou danos ao ativo
- Resguarda: é o mecanismo ou procedimento para reduzir o risco

Segundo Martins e Santos (2005), a possibilidade de perda de disponibilidade, integridade ou confiabilidade está intimamente relacionada ao contexto da segurança da informação. A confiabilidade da rede está ligada à forma como os componentes do sistema interagem entre si, ou seja, à interdependência dos componentes. A análise da interdependência dos componentes (questões internas da rede), aliada às interações humanas (questões externas), possibilita a melhoria do funcionamento da rede, proporcionando maior confiabilidade, disponibilidade e integridade (WEBER, 2012).

De modo geral, existem duas formas de analisar esses riscos: quantitativa e qualitativa. Na análise qualitativa, os cálculos são mais simples e os resultados tendem a ser subjetivos.

Por outro lado, a análise quantitativa fornece resultados mais objetivos e é mais adequada para resolver problemas relacionados à segurança da informação (KARABACAK, 2005).

Segundo Karabacak (2005), o método de análise de risco ISRAM (Information Security Risk Analysis Method) é o mais adequado quando o risco está relacionado à segurança das informações. Esse método propõe a aplicação de uma fórmula matemática simples (1) para retirar a subjetividade de questionários aplicados à especialistas no assunto.

$$Risco = [Probabilidade\ do\ evento\ ocorrer] \times [Impacto\ da\ Ocorrência] \quad (1)$$

Verifica-se que o risco está associado à probabilidade do evento (o componente da rede falhar) ocorrer multiplicado pelo impacto da ocorrência, ou seja, o ISRAM, auxilia também no processo de condução da pesquisa para avaliar o Risco de Segurança dos dados.

2.5. MODELAGEM E SIMULAÇÃO

Segundo Sokolowski (2009), modelo é a representação de um sistema do mundo real, podendo fazer referência a um evento e/ou objeto. Para produzir um modelo é necessário abstrair os aspectos do sistema desejado da realidade e, ainda, o modelo pode representar apenas um ponto ou múltiplos níveis de abstração que tem como objetivo a modelagem de um sistema de forma matematicamente confiável.

Continuando, Sokolowski define simulação como a imitação de um processo ou sistema em um intervalo de tempo (2009). Com isso, a simulação computacional pode ser entendida como a tentativa de replicação do comportamento de um sistema (VIEIRA, 2004). Assim sendo, 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.

A modelagem e simulação são amplamente utilizadas em diversas disciplinas para entender e analisar sistemas complexos. Através da construção de modelos que representam a realidade, é possível simular o comportamento dos sistemas sob diferentes condições e cenários, proporcionando insights valiosos para a tomada de decisões e o planejamento estratégico.

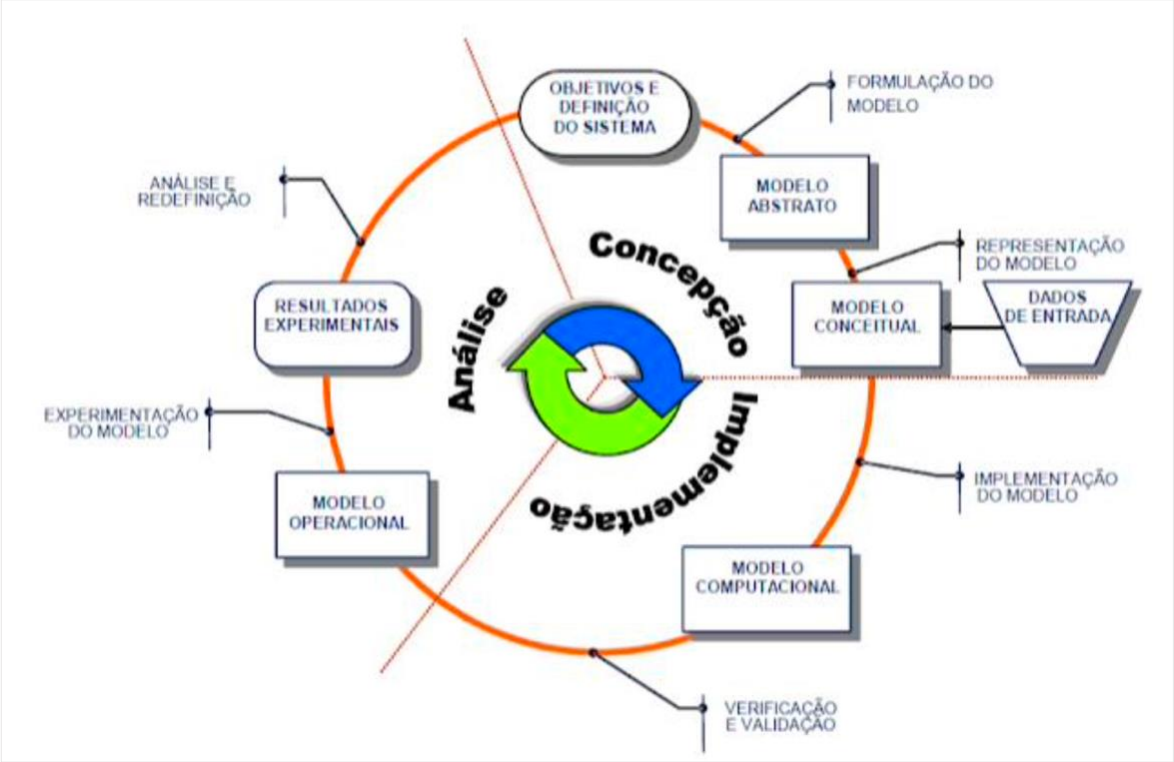
E, ainda, VIEIRA (2004), ao realizar a modelagem e simulação, destacaram algumas vantagens como:

- Desenvolvimento de modelos realísticos, mostrando como realmente o sistema opera;
- Desenvolvimento de cenários e avaliação do comportamento sob diversas condições
- Análise do comportamento sistêmico em um curto período.

- Simulação de um sistema que possa ainda não existir;
- Possibilidade de redução de custos ao identificar variáveis controláveis.

A simulação computacional é dividida em três etapas importantes: concepção, implementação e análise (CIA), conforme exibido na Figura 5.

Figura 5 - Modelagem e Simulação



Fonte: CHWIF (1999)

Segundo Robinson (2008), na etapa de concepção ocorre a definição do problema, dos objetivos e do escopo do modelo. Além da: (1): identificação das variáveis relevantes (importantes para descrever o modelo) e formalização das equações do modelo (como essas variáveis se relacionam em expressões matemáticas); (2) ocorre a coleta e o tratamento dos dados de entrada

O plano de implementação O modelo é programado em alguma linguagem genérica ou de modelagem. E ocorre a Verificação e validação: nessa etapa o modelo computacional é comparado com o modelo conceitual e alguns testes devem ser realizados para verificar se o modelo se aproxima do real ou do esperado – validação. (THIOLLENT, 2005).

Na etapa de análise ocorre: (1) Experimentação do modelo: são realizados experimentos com o modelo computacional (várias rodadas), dando origem ao modelo operacional e; (2) e os resultados são analisados e documentados. Caso os resultados não sejam satisfatórios, o modelo pode ser modificado, e o ciclo é reiniciado.

A etapa de concepção deste trabalho identificou dois métodos que melhor se adequam ao objetivo proposto e estão descritos a seguir:

2.6. TÉCNICAS E MÉTODOS

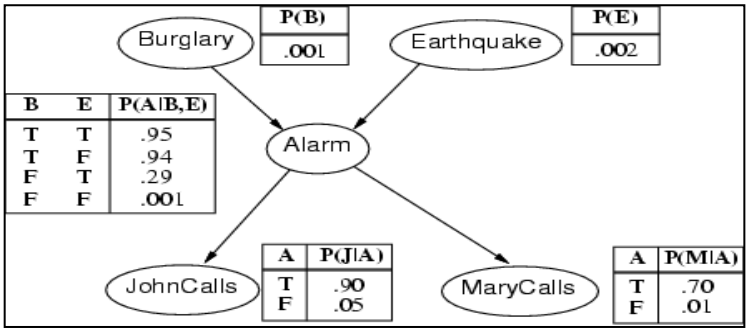
2.6.1. REDES BAYESIANAS

Redes Bayesianas (RB) são grafos acíclicos 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 gráfico acíclico direcionado (GAD) e a parte quantitativa é a probabilidade atribuída aos nós que representam as variáveis. Ao estabelecer a relação de causa e efeito, fornecem resultados animadores no que se refere ao diagnóstico, à previsão e classificação de falhas e análise de riscos (LIBRANTZ, 2020).

Segundo LIBRANTZ (2020), esta abordagem permite que conhecimentos de especialistas sejam incluídos na modelagem por meio do Teorema de Bayes, representando uma boa estratégia para lidar com problemas que tratam incertezas.

A RB é caracterizada por grafos acíclicos em que os vértices representam os nós e as ligações representam a relação de dependência entre esses nós. São representados, respectivamente, por elipse e setas. Os nós que não possuem dependência de outros nós são denominados nós pais, conforme mostrado na Figura 6.

Figura 6 - Exemplo de Rede Bayesiana



Fonte: Librantz (1999)

Essas variáveis podem ser valores observáveis, variáveis ocultas ou parâmetros desconhecidos. As bordas do RB 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, 2013). O teorema de Bayes expressa a relação entre as variáveis dependentes, como segue:

$$P(\mathrm{H/E}) = \frac{P(E/H).P(H)}{P(E)} \qquad (2)$$

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, posteriormente, apresenta um número estimado para a hipótese após as observações.

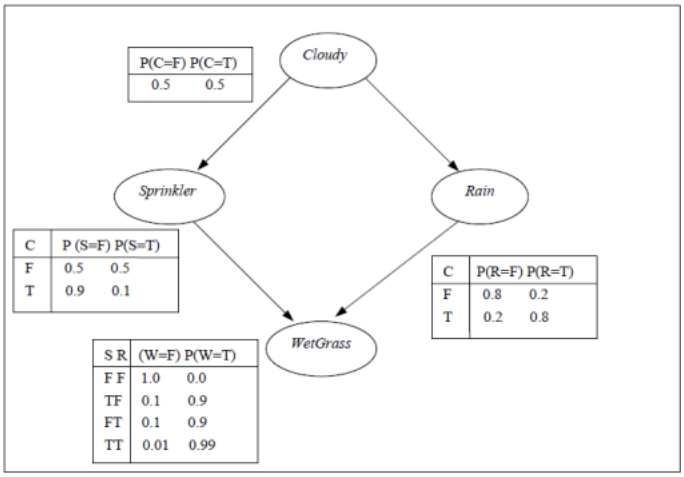
Patterson (1984) relata que a primeira aplicação prática da RB foi o clássico problema do diagnóstico médico. Empresas como a Microsoft(R), por exemplo, usaram essas redes para diagnóstico de falhas, principalmente, na solução de

problemas de impressora (HECKERMAN,1995). Assim, as habilidades preditivas e diagnósticas das RB a tornaram uma ferramenta poderosa para a tomada de decisão sob incerteza

2.6.1.1. EXEMPLO DE REDE BAYESIANA

Para elucidar a rede bayesiana, utilizaremos o exemplo popular da grama molhada. Neste exemplo, observa-se que a grama de um jardim está molhada pela manhã. E se estiver molhada (W) pode ser por causa do sprinkler (S) ou da chuva (R), pois o tempo está nublado (C). Essa relação de interdependência foi representada na Figura 7.

Figura 7 – Exemplo de Rede Bayesiana - Grama Molhada



Fonte: adaptado de MURPHY, K. (1998)

Neste caso, apesar de S e R serem independentes, tornam-se dependentes dada a evidência do estado de W, que é filho de ambos. Assim, para o cálculo de P(S|W) deve-se considerar P e vice-versa.

2.6.1.2. INFERÊNCIA BAYESIANA

Formalmente, uma rede bayesiana é definida como um conjunto de variáveis X = {X1, ..., Xn} 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:

$$\left(X_{1,} \dots X_{n,}\right) = \prod_{i=1}^{n} (P(X_i / P_a(X_i)) \qquad (3)$$

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

2.6.1.3. TABELA DE PROBABILIDADE CONDICIONAL (TPC)

A construção de tabelas de probabilidade condicional é uma etapa fundamental na modelagem de probabilidade de sistemas complexos, como as redes Bayesianas. Estas tabelas fornecem uma representação compacta das relações probabilísticas entre as variáveis e levam em consideração as dependências entre elas.

Uma tabela de probabilidade condicional associa cada combinação de valores das variáveis de entrada (variáveis pai) a uma distribuição de probabilidade das variáveis de saída (variável filha). Essas tabelas são estruturadas de forma que cada linha representa uma combinação única de valores das variáveis pai, e as colunas representam os possíveis valores da variável filha.

Assim, existem várias maneiras de construir uma tabela de probabilidade condicional, dependendo do contexto do problema e dos dados disponíveis:

- **Dados empíricos**: Em muitos casos, as probabilidades condicionais podem ser estimadas diretamente a partir dos dados observados. Isso envolve calcular a frequência de cada combinação de valores da variável pai e normalizar para obter probabilidades.
- **Teoria estatística**: Em alguns casos, as probabilidades condicionais podem ser derivadas de princípios teóricos ou modelos estatísticos. Isso

pode ser feito usando teoremas como o teorema de Bayes ou modelos probabilísticos mais complexos.

Uma vez definidas as probabilidades a priori, as TPCs podem ser desenvolvidas. Suponha que cada causa Bij possa produzir o efeito Ei, que é nó filho com probabilidade fij. O efeito de todos os pais (nós raiz) com dependências diretas e indiretas pode ser representado da seguinte forma:

$$P(E_i \backslash par(E_i \backslash B_{1,} \dots, B_{n,}) \quad (4)$$
$$= 1 - \prod_j (1 - P(Ei \backslash Bj)$$
$$= 1 - \prod_j (1 - fij)$$

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

2.7. MÉTODO MONTE CARLO

Simulações computacionais são uma forma de representar um sistema real. Essas simulações, dependendo do problema, podem ocorrer de maneira direta, tentando simular o problema como ele ocorre na realidade, ou, então artificialmente, no qual a resposta obtida na simulação corresponde a resposta do sistema real. É nessa última classificação que se encaixa o Método de Monte Carlo.

O Método de Monte Carlo desenvolvido a partir de conceitos de probabilidade e estatística e têm se tornado uma abordagem essencial para resolver uma variedade de problemas complexos em ciência, engenharia, finanças e outras áreas. Esse método numérico é utilizado para solucionar problemas por meio de números aleatórios ou variáveis aleatórias.

O método baseia-se na geração de números aleatórios para realizar simulações e análises estatísticas. O princípio básico envolve a execução de experimentos repetidos, onde cada experimento gera uma amostra que contribui para a estimativa do resultado final. A precisão dos métodos de Monte Carlo aumenta com o número de simulações realizadas, permitindo a convergência para o valor esperado ou para a solução do problema.

Existem diversas variações dos métodos de Monte Carlo, incluindo:

- **Monte Carlo Clássico:** Utiliza amostras aleatórias uniformemente distribuídas para estimar resultados em problemas determinísticos.
- **Monte Carlo com Variância Reduzida:** Técnicas que visam melhorar a precisão das estimativas, utilizando métodos como amostragem estratificada e amostragem de importância.
- **Monte Carlo Sequencial:** Um método que combina Monte Carlo com técnicas de otimização, permitindo uma atualização contínua das estimativas à medida que novos dados se tornam disponíveis.

Dessa maneira, o método é aplicável a uma variedade de problemas que envolvem incerteza, aleatoriedade e complexidade. Algumas das principais áreas de aplicação incluem:

- Física: O método é amplamente utilizado na simulação de sistemas físicos complexos, como o comportamento de partículas em reatores nucleares, a propagação de ondas eletromagnéticas, e a dinâmica de sistemas quânticos.
- Engenharia: o método é empregado na análise de risco estrutural, otimização de projetos, modelagem de sistemas dinâmicos e simulação de processos industriais.
- Finanças: o método é utilizado para precificação de opções, avaliação de riscos de carteiras de investimento, simulação de cenários econômicos e modelagem de preços de ativos financeiros.
- Biologia e Medicina: o método é aplicado em estudos de genética populacional, modelagem de interações moleculares, análise de dados de ensaios clínicos e simulação de processos biológicos.
- Ciências Sociais: o método é utilizado na modelagem de comportamento humano, previsão de tendências sociais, simulação de redes sociais e análise de dados demográficos.

E a função inversa no contexto do Método de Monte Carlo é uma técnica utilizada para gerar amostras de uma distribuição de probabilidade específica a partir de uma distribuição uniforme. Essa abordagem é especialmente útil quando se deseja

simular variáveis aleatórias de distribuições não uniformes, como normal, exponencial, binomial, entre outras (Landau, D. P., & Binder, Y. B. J. (2014).). Dentre os processos envolvidos :

- **Distribuição Acumulada (CDF)**: A Função de Distribuição Acumulada (CDF) de uma variável aleatória XXX é dada por:

  F(x)=P(X≤x)F(x) = P(X \leq x)F(x)=P(X≤x)

A CDF fornece a probabilidade de que a variável aleatória XXX assuma um valor menor ou igual a xxx.

- **Função Inversa da CDF**: A função inversa da CDF, denotada como F−1(u)F^{-1}(u)F−1(u), é a função que transforma uma probabilidade uuu (uniformemente distribuída entre 0 e 1) em um valor correspondente da variável aleatória XXX. Isso significa que, para um dado uuu, temos:

  X=F−1(u)X = F^{-1}(u)X=F−1(u)

A função inversa é usada para "mapear" a variável uniforme para a distribuição desejada.

O processo de Geração de Amostras Usando a Função Inversa é descrito a seguir:

- **Definição da Distribuição**: Determine a distribuição de probabilidade da variável aleatória que você deseja simular (por exemplo, normal, exponencial, etc.). Isso inclui conhecer a CDF F(x)F(x)F(x) e, se possível, calcular sua função inversa F−1(u)F^{-1}(u)F−1(u).
- **Geração de Números Aleatórios**: Gere um número aleatório uuu a partir de uma distribuição uniforme no intervalo [0,1][0, 1][0,1]. Essa etapa é fundamental porque o método de Monte Carlo depende da geração de variáveis aleatórias uniformes.
- **Aplicação da Função Inversa**: Use a função inversa da CDF para obter uma amostra da variável aleatória XXX:

$X = F^{-1}(u)$

Isso transforma o número uniforme uuu em um valor que segue a distribuição desejada.

- **Repetição do Processo**: Repita os passos 2 e 3 para gerar múltiplas amostras da variável XXX. Quanto mais amostras você gerar, mais precisa será sua estimativa da distribuição.
- **Análise dos Resultados**: Utilize as amostras geradas para calcular estatísticas de interesse, como médias, variâncias, e outros parâmetros relevantes para sua análise.

Uma vez que o Método Monte Carlo é utilizado com sucesso em diversas áreas, demonstrando sua versatilidade e poder analítico, é necessário fazer uso de diversas distribuições estatísticas, dependendo do contexto do problema em questão.

Segundo Winston (2000), as distribuições de probabilidade comum incluem diferentes apresentações em gráficos, algumas delas estão listadas na tabela 4:

Tabela 4 - Distribuições Utilizadas em Monte Carlo

Distribuição	Descrição
Uniforme	Todos os valores possíveis têm a mesma probabilidade. É útil quando não há razão para acreditar que alguns valores são mais prováveis do que outros.
Normal (Gaussiana)	Uma distribuição simétrica em forma de sino, com a maioria dos valores em torno da média e uma cauda que se estende infinitamente em ambas as direções.
Exponencial	Modela o tempo entre eventos em um processo de Poisson, onde a taxa de ocorrência é constante. É útil para modelar tempos de espera ou intervalos de tempo.
Binomial	Modela o número de sucessos em um número fixo de tentativas independentes, onde cada tentativa tem a mesma probabilidade de sucesso. É útil em experimentos com resultados binários, como lançamento de moedas.
Multinomial	Uma generalização da distribuição binomial para o caso de mais de dois resultados possíveis. É útil para modelar experimentos com mais de dois resultados possíveis.

Fonte: Winston (2000)

Na simulação de cenários através do método Monte Carlo, os valores são exibidos de forma estocástica a partir das distribuições das probabilidades de entrada.

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 no tema pesquisado (KITCHENHAM, 2007).

Portanto, a Revisão Sistemática da Literatura é baseada em uma estratégia de pesquisa bem definida, cujo objetivo é extrair o máximo de literatura relevante possível referente ao tema pesquisado, reduzindo assim o viés de entendimento (KITCHENHAM, 2007).

Então, 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" também pode ser referido pela abreviatura IoT (Internet of Things), formando a combinação dessas palavras chaves em todos os tópicos de buscas das bases de pesquisa.

1. "Monte Carlo" AND "bayes" AND "Internet of things" AND “risk”;
2. "Monte Carlo" AND "bayes" AND "IoT" AND “risk”;
3. "Monte Carlo" AND "risk" AND "IoT";
4. "Monte Carlo" AND "risk" AND “IoT”;
5. "simulation" AND "Internet of things" AND “risk”;
6. "simulation" AND "IoT" AND “risk”;
7. "Stochastic" AND "Internet of things” AND “risk”;
8. "Stochastic" AND "IoT" AND “risk”;

A partir da definição das palavras chaves, combinadas pelo conector OR, aplicado a todos os campos de pesquisas, limitando-se apenas aos artigos dos últimos 5 anos.

Esses conjuntos de palavras-chave foram usados na RSL. Os dados foram coletados em 3 bases diferentes, incluindo SCOPUS, Web of Science, Compendex.

A etapa de revisão sistemática da literatura é uma etapa crucial em muitos processos de pesquisa, e o método PRISMA representa um papel importante na condução e apresentação de etapas transparentes da RSL.

O método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) é um conjunto de diretrizes desenvolvido para auxiliar na condução e elaboração de revisões sistemáticas e meta-análises na literatura biomédica e em outras áreas da saúde. Esse método garante mais transparência, qualidade e clareza na apresentação da revisão sistemática da literatura.

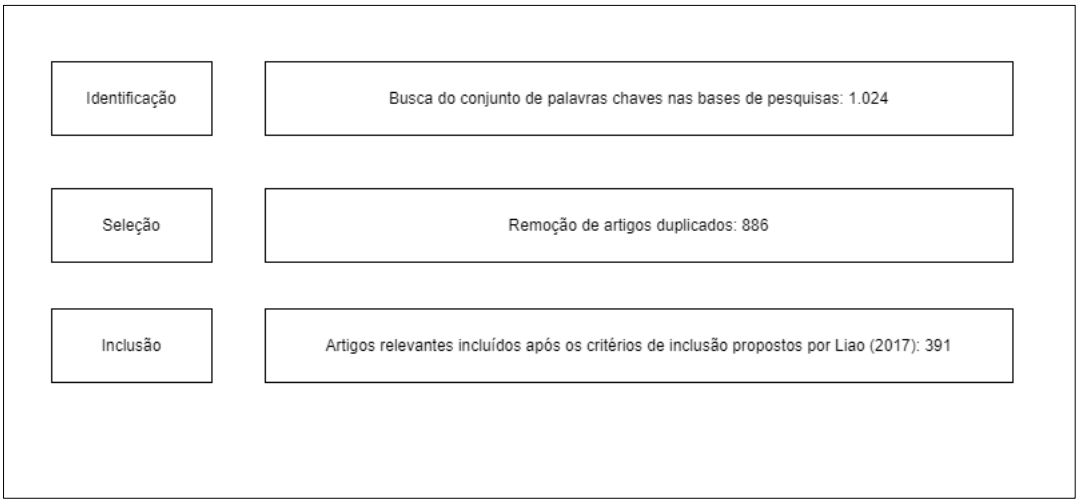
Assim sendo, o método PRISMA consiste em uma lista de verificação de 27 itens e um diagrama de fluxo de quatro fases (LIBERATI, 2009). A versão de 2009 do PRISMA listava 3 pontos principais:

- Descrever todas as fontes de informação (por exemplo, bases de dados com datas de cobertura, contato com autores de estudos para identificar estudos adicionais) na pesquisa
- Apresentar estratégia completa de busca eletrônica para pelo menos um banco de dados
- Fornecer o número de estudos selecionados e avaliados para elegibilidade e inclusão na revisão

Optou-se por utilizar o método PRISMA porque ele melhora a qualidade e a transparência das revisões sistemáticas, facilitando a replicação do estudo e a avaliação da confiabilidade das conclusões. Além disso, garante que todas as etapas importantes do processo de revisão sistemática sejam abordadas de maneira sistemática e abrangente.

Desse modo, os seguintes resultados foram obtidos a partir da adaptação do método PRISMA nesta pesquisa:

Figura 8 - Diagrama do Fluxo PRISMA



Fonte: elaborado pelo autor

Na etapa de identificação, a distribuição de artigos ao longo do tempo é apresentada na Tabela 5.

Tabela 5 - Quantidade de Artigos ao longo do tempo

Base de Dados	Ano	Quantidade de Artigos
web of science	2019	21
web of science	2020	53
web of science	2021	64
web of science	2022	84
web of science	2023	73
compendex	2019	26
compendex	2020	56
compendex	2021	56
compendex	2022	91
compendex	2023	97
scopus	2019	38
scopus	2020	51
scopus	2021	86
scopus	2022	113
scopus	2023	115

Fonte: elaborado pelo autor

Os critérios de inclusão (CI) e exclusão (CE), proposto por LIAO (2017), foram aplicados para selecionar os artigos encontrados nas bases de pesquisa citadas, conforme a Tabela 6:

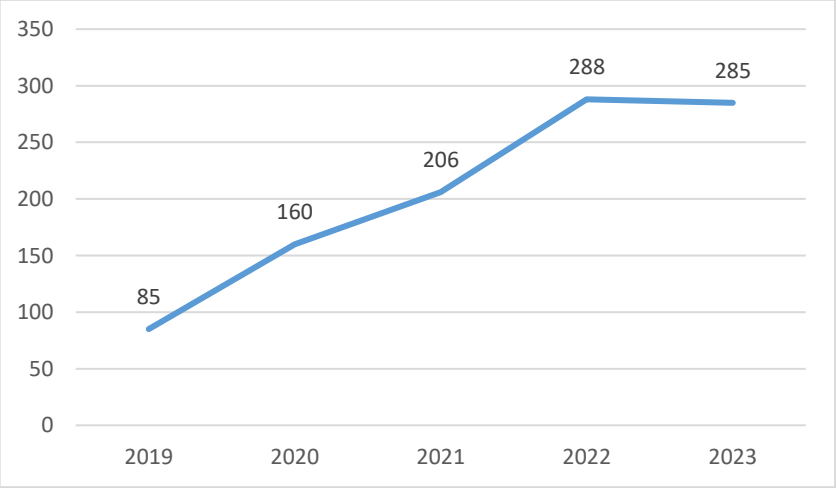
Tabela 6 - Critério de Inclusão e Exclusão

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 explícitos e especificamente dedicados ao tema pesquisado

Fonte: adaptado pelo autor de Liao, 2017

O critério de inclusão aplicado nos artigos resultantes o desenvolvimento de um modelo como resultado do trabalho ou utilizar as técnicas e os métodos propostos nesse trabalho no contexto de redes IoT. Ou, então, avaliar a rede de uma forma sistêmica, de modo que todos os componentes da rede estivessem envolvidos no modelo proposto.

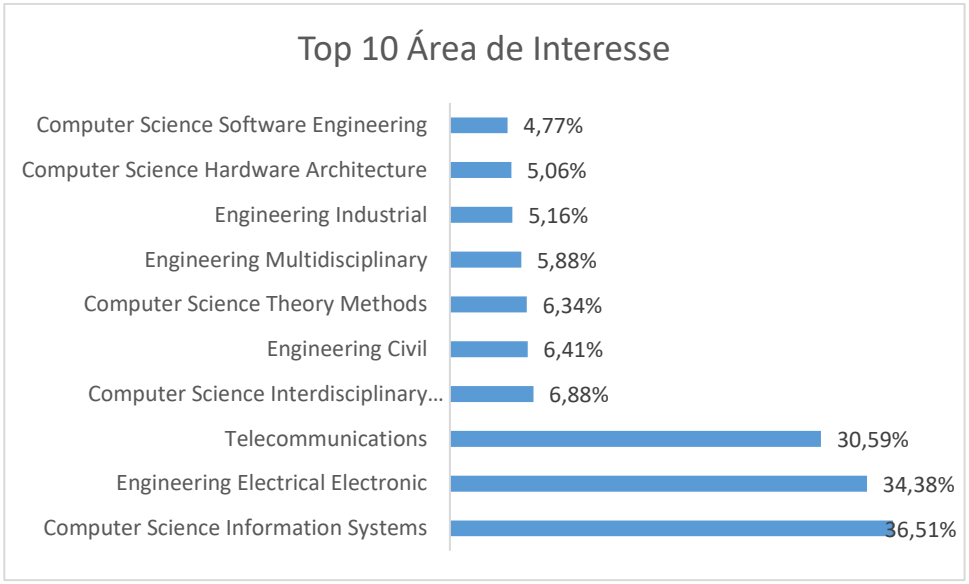
Figura 9 - Evolução das Publicações



Fonte: elaborado pelo autor

E, ainda, a ciência da computação, engenharia e telecomunicações estão entre as dez áreas de interesse do assunto, conforme destacado na Figura 10.

Figura 10- TOP 10 Áreas de Interesse de Publicação



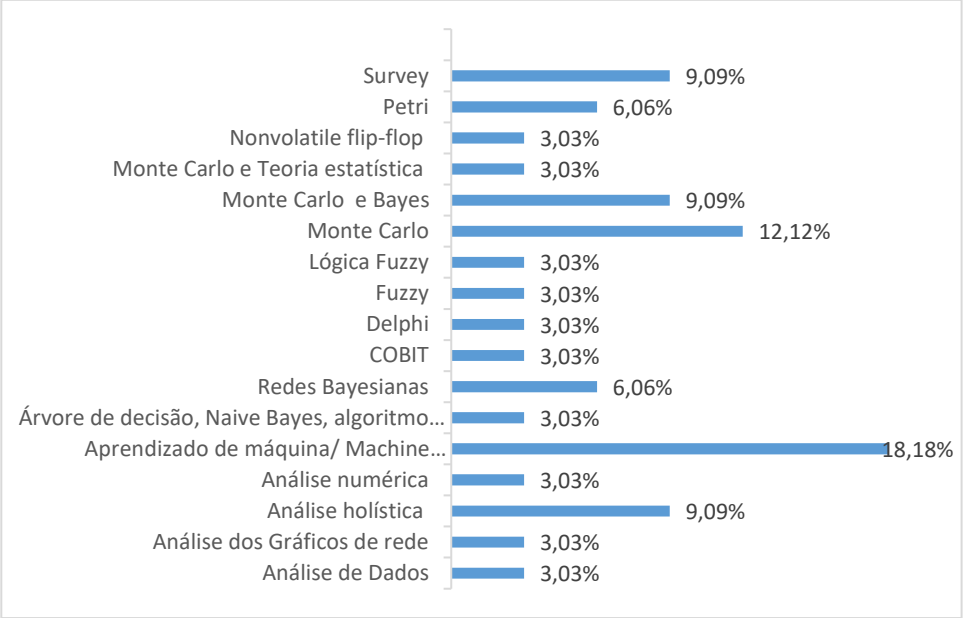
Fonte: elaborado pelo autor

Entre as 10 áreas de maior interesse notou-se que é ainda um tema estudado por áreas mais técnicas (engenharia, telecomunicações). E a área relacionada ao negócio/ cliente como, por exemplo: a área médica não teve destaque entre as 10 área de maiores de publicações.

Dentre os artigos que propunham um modelo, apenas 1 deles propôs analisar a rede de forma sistêmica. Os demais trabalhos propuseram modelos baseados em uma camada. No trabalho de Baranowski, J. (2022), por exemplo, o modelo proposto focou na camada física.

Entre as técnicas mais utilizadas, destacam-se Aprendizado de máquina/ Machine Learning/ Redes Neurais/ Inteligência Artificial, Survey e Análise holísticas, conforme representado na Figura 11.

Figura 11 - Técnicas Mais Aplicadas



Fonte: elaborado pelo autor

A Figura 11 apresenta a técnica de aprendizagem de máquina entre as mais utilizadas e Monte Carlo como a segunda mais utilizada nos trabalho, indicando que suas aplicações trouxeram resultados relevantes. No entanto, combinar Monte Carlo com Redes Bayesianas foi pouco explorada

3.1. TRABALHOS CORRELATOS

A revisão da literatura demostrou que trabalhos referentes ao tema abordam apenas um componente da rede ou um contexto/ problema específico, por exemplo, apenas para um problema da área (privacidade dos dados da área médica, ataque de cibersegurança em sistemas de carros inteligentes ou educação ou aumentar a produção no agronegócio). A tabela 7, relaciona combinação de técnicas, abordagem e o contexto proposto nestes trabalhos aos artigos selecionados na etapa anterior.

Tabela 7 – Trabalhos X Técnicas utilizadas

Autor	**Técnica / Método**	**Aborda sistemicamente os componentes da IoT**	**Contexto aplicado - problemática**
Anajemba (2020)	Análise numérica	Não	Privacidade dos dados
Pacheco (2018)	Aprendizado de máquina	Não	Privacidade dos dados
Pacheco (2018)	Análise de Dados	Não	Integridade dos dados
El-Gendy (2023)	Machine Learning	Sim	Privacidade dos dados
Pacheco (2020)	Redes Neurais	Não	Segurança dos Dados (Detecção de intrusão)
Junqi G. *et al* (2023)	Inteligência artificial	Não	Privacidade dos dados
Savazzi. (2020)	Aprendizagem de máquina	Não	Distribuição da carga operacional dos componentes da rede
Tahsien (2020)	Aprendizagem de máquina	Não	Segurança da informação
Valdivia (2020)	COBIT	Não	Mitigar riscos de ataques de cibersegurança
CHANG (2020)	Delphi	Não	Governança da Rede/Controle Interno
Sha (2020)	Survey	Não	Segurança
Karunarathne (2021)	Survey	Não	Privacidade e Segurança dos dados
Alwarafy (2021)	Survey	Não	Privacidade e Segurança dos dados
Sarwar (2023)	Survey	Não	Privacidade e Segurança dos dados
Kandasamy (2020)	Análise holística	Não	Segurança da rede

Byrnes (2019)	Markov Chain Monte Carlo e Bayes	Não	Desempenho dos sensores em cidades inteligentes
Choi (2020)	Nonvolatile flip-flop	Não	Otimizar custos de energia
Lomotey (2017)	Petri	Não	Rastreabilidade dos dados
Ghosh (2019)	Petri	Não	Integridade dos dados
Attaullah (2022)	Lógica Fuzzy	Não	Privacidade e Segurança dos dados
Campanile (2020)	Fuzzy	Sim	Sobrecarga energética na rede
George (2018)	Análise dos Gráficos de rede	Não	Segurança da rede IIoT
Qingping (2018)	Redes Bayesianas	Não	Segurança dos dados
Zhang (2018)	Redes Bayesianas	Não	Segurança dos dados
Gyamfi (2019)	Redes Bayesianas	Não	Custo de energia
Chen, Q. *et al* (2016)	Monte Carlo	Não	Otimizar a memória dos dispositivos
Sharma (2021)	Monte Carlo	Não	Integridade dos dados
Darabi (2023)	Monte Carlo	Não	Otimizar a memória dos dispositivos
Ntafloukas (2022)	Monte Carlo	Não	Segurança dos dados
Zhang (2023)	Monte Carlo e Teoria estatística	Não	Integridade dos dados e otimizar custos de energia
Baranowski (2022)	Monte Carlo e Bayes	Não	Falhas nos dispositivos
Coccia (2022)	Monte Carlo e Bayes	Não	Otimizar custos de energia de forma temporal
Satam (2022)	Árvore de decisão, Naive Bayes, algoritmo Ripper	Não	Segurança dos Dados (Detecção de intrusão)
Kinjo (2022)	Bayes	Sim	Identificar a probabilidade da rede falhar, no contexto da saúde
Sung (2023)	Análise holística	Não	Privacidade

Zhang (2023)	Análise holística dos trabalhos que utilizaram Deep Learning	Não	Privacidade

Fonte: elaborado pelo autor

Ao analisar os trabalhos correlatos nota-se que Lomotey (2017) aplicou a técnica de Petri e 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.

Ghosh (2019) também utilizou a rede de Petri nas camadas de Enlace, transporte e rede do modelo. E a problemática estudada foi a integridade dos dados. Nota-se que as camadas, cuja interação com o usuário é maior, não foram abordadas no trabalho.

A Lógica Fuzzy foi utilizada nos trabalhos de Campanile (2020); Ntafloukas (2022), nos contextos de sobrecarga energética da rede e na privacidade e segurança dos dados, respectivamente. No entanto, nos dois trabalhos, os dispositivos foram focos desses trabalhos.

O trabalho de Valdivia (2020), publicado em uma conferência, abordou o problema de segurança de dados e propôs a criação de uma agente inteligente, ou seja, uma entidade inteligente que permitisse avaliar o cenário e propusesse resposta atuais, baseando-se no Cobit e na ISO 27001.

O trabalho de Tahsien (2020) teve como tema a problemática da privacidade e segurança dos dados, destacando o aumento da quantidade de dispositivos conectados à rede. No entanto, o resultado do trabalho não desenvolveu um modelo, mas uma survey.

Outros autores, como Kandasamy (2020) estudaram o assunto sem desenvolver um modelo. O autor estudou o contexto de Privacidade e Segurança dos dados propondo uma análise holística.

El-Gendy (2023); Pacheco (2020); Tahsien (2020); Savazzi (2020) estudaram diferentes problemas na rede IoT e utilizaram técnicas diferentes de Aprendizagem de máquina, redes neurais. No entanto em nenhum desses abordaram todas os componentes da rede.

Chen (2016) propôs um modelo usando Monte Carlo, no qual abordou a otimização da memória de dispositivos e quantificando o efeito até a primeira falha ocorrer. Ntafloukas (2022) também utilizou a técnica de Monte Carlo para avaliação de ataques ciberfísicos no contexto dos motivos e impactos nos usuários da rede.

Kinjo (2022) estudou a privacidade e Segurança dos Dados e propôs a criação de um modelo que abrangeu todas as camadas da rede, inclusive a camada de aplicação. No entanto, apenas as redes bayesianas foram utilizadas no trabalho.

Os trabalhos de Coccia (2022); Byrnes (2019) e Baranowski (2022) discutiram a combinação de Bayes e Monte Carlo. No entanto, a abordagem da característica intrínseca das redes bayesianas que permite a análise sistêmica do problema para calcular a probabilidade de falha na rede não foi adotada por nenhum autor.

A maioria dos autores abordaram mais de uma camada da rede (física e rede, rede e aplicação, por exemplo), no entanto não foi identificado um modelo resultante desse trabalho que se estendesse até as camadas de aplicação conjuntamente

Além disso, nos trabalhos estudados, os autores se propuseram a abordar apenas um contexto – problemática – tais como: otimizar custo de energia, otimizar memória, integridade de dados, desempenho de sensores. E, na maioria dos trabalhos, a problemática era aplicada a um contexto específico, por exemplo, aumentar a produção.

Diante da análise desses artigos, não foram identificados trabalhos que atendessem a todos os itens que esse trabalho se desenvolveu, ou seja, um modelo que permeasse todas as camadas da rede e com capacidade de mensurar os riscos da rede falhar.

4. METODOLOGIA

Este capítulo apresenta os métodos e materiais adotados para a realização desta pesquisa, apresentando a natureza do estudo e o processo metodológico. O processo metodológico inclui o esquema de desenvolvimento para a coleta de dados e as técnicas utilizadas para a construção do modelo e análise dos dados.

4.1. MÉTODO DE PESQUISA

Este trabalho versa sobre uma pesquisa aplicada, pois todo o processo de coleta de dados, aplicação de técnicas e análise dos dados tiveram como propósito gerar conhecimento para uma aplicação prática (KUMAR, 2011).

O 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 & Clark, 2013).

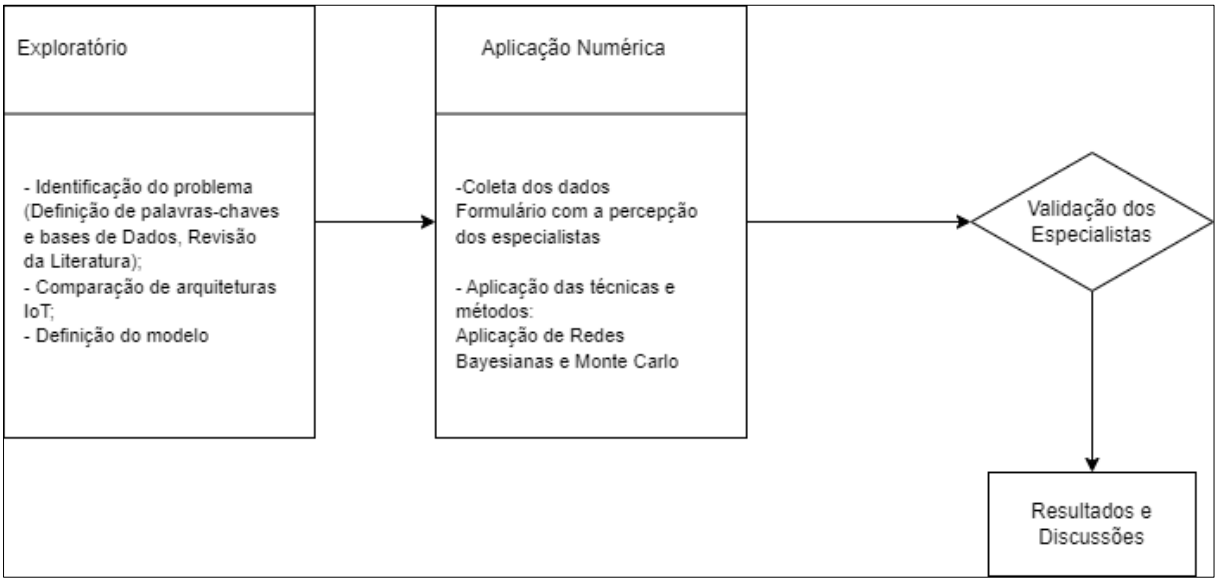
A utilização de uma abordagem qualitativa para a obtenção dessas informações diminuiu a quantidade de erros adversos. Cada uma das opções requer a conversão em valores numéricos e isso requer mais cuidado. Posteriormente, esses valores numéricos foram empregados em uma abordagem quantitativa, utilizando como parametrização inicial nas redes Bayesianas e no método Monte Carlo.

Segundo KUMAR (2011), a pesquisa ainda pode ser classificada quanto ao seu propósito. Inicialmente, essa pesquisa teve caráter exploratório, uma vez que o foco inicial era fornecer contexto sobre o problema estudado. Em um segundo momento, o estudo se tornou preponderantemente descritivo, em que houve o aprofundamento sobre o tema. É nesta etapa que o conhecimento prévio obtido na exploração da situação-problema é considerado.

4.2. ETAPAS PARA O DESENVOLVIMENTO

O desenvolvimento deste trabalho foi dividido em 3 etapas para a obtenção de um resultado mais consistente: Definição dos parâmetros de entrada, desenvolvimento e validação do modelo. Conforme a Figura 12.

Figura 12 – Etapas do Desenvolvimento



Fonte: elaborado pelo autor

Nos tópicos seguintes essas etapas foram detalhadas.

4.2.1. EXPLORATÓRIO

4.2.1.1. IDENTIFICAÇÃO DO PROBLEMA

A exploração do tema através da revisão de literatura selecionou 391 artigos, cujos componentes da rede foram classificados em um modelo de camadas (o utilizado na literatura). Além disso, no processo de revisão da literatura, foram identificados a privacidade e segurança dos dados como a principal preocupação dos pesquisadores.

4.2.1.2. COMPARAÇÃO DE ARQUITETURA JÁ UTILIZADAS

Para compreender os modelos mais utilizados na representação de uma rede IoT, buscou-se nas bases de dados da Web of Science e Scopus o termo “IoT architecture” ou “Internet of Things Architecture”, ordenando-os pelos mais citados.

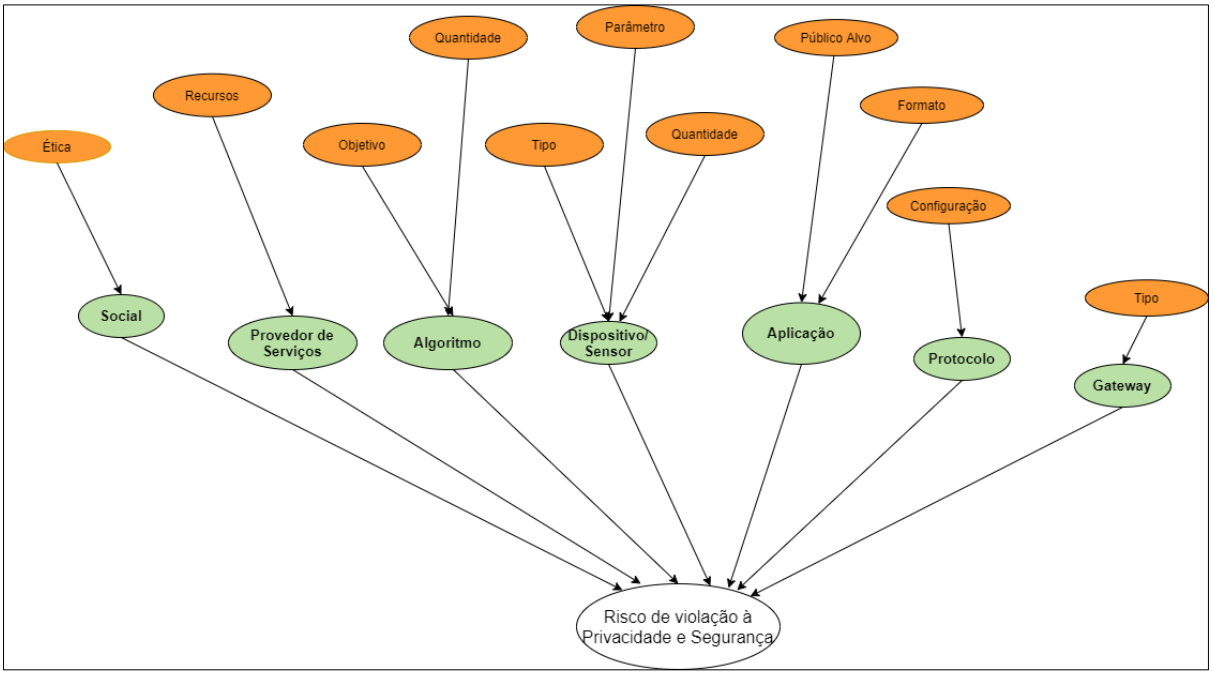
De modo geral, foi identificado que os trabalhos utilizavam a arquitetura em camadas, divergindo na quantidade de camadas. Uma arquitetura em camadas é entendida como a forma de organizar as responsabilidades de partes de um software,

normalmente criando um isolamento e dando um propósito bem definido a cada camada.

DEFINIÇÃO DO MODELO OSI*

Uma vez que na etapa anterior foi identificado que o modelo em camadas foi o mais utilizado nos trabalhos publicados, o modelo baseado nos componentes representado na Figura 13 foi adaptado para ser representado em camadas de modo que nenhum detalhe fosse perdido.

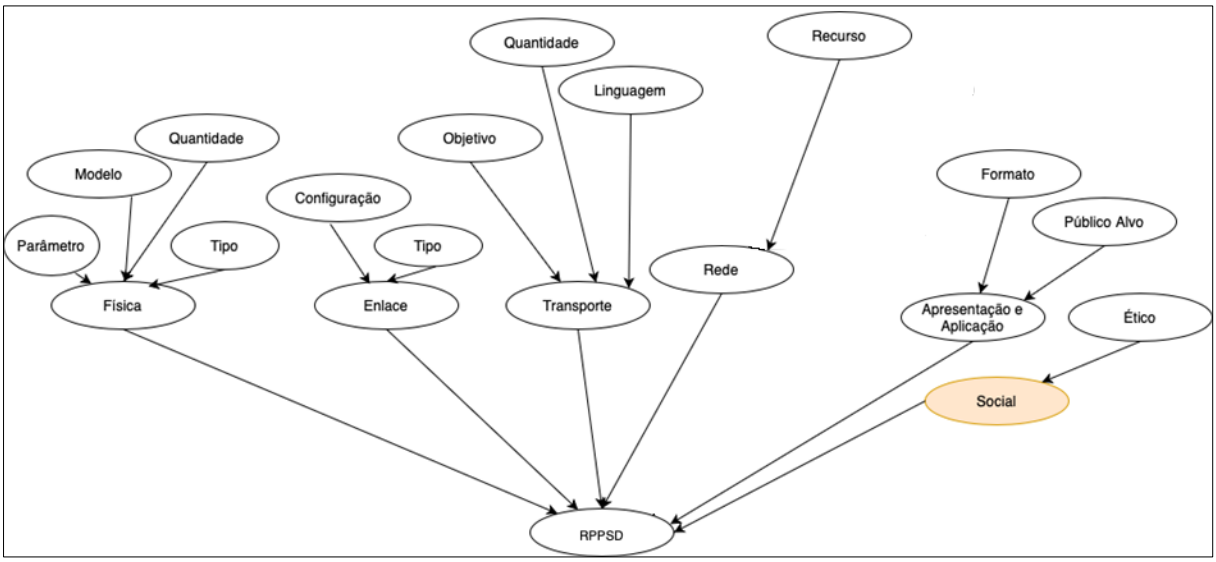
Figura 13 - Representação do Modelo Baseado em Componentes



Fonte: elaborado pelo autor

Após classificar os componentes em camadas, segundo o modelo OSI, desenvolveu-se o modelo OSI *, representado na figura 14.

Figura 14 - Modelo OSI*



O componente social não foi classificado em nenhuma camada do modelo OSI, por isso adotou-se o nome de OSI* para representar a diferença. Esse componente também não foi retirado do modelo, uma vez que foi destacado como um dos 3 componentes mais relevantes.

4.2.2. APLICAÇÃO NUMÉRICA

4.2.2.1. COLETA DOS DADOS

O ponto de partida para as probabilidades a priori foi a percepção atribuída pelos 12 especialistas, cujo perfil foi detalhado na Tabela 8. Existem vários cálculos métodos para agregação de opiniões de grupos, porém, a média 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, 2018).

Com isso, a consolidação das opiniões dos especialistas neste estudo foi realizada através 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:

$$P = \sqrt[n]{x_1 \times x_2 \times x_3 \times \ldots \times x_n} \qquad (4)$$

, no qual n é a quantidade de termos da multiplicação.

Tabela 8 - 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 do 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: elaborado pelo autor

A percepção dos 12 especialistas foi captada por meio da aplicação de um formulário (APÊNDICE A) e os resultados referentes à probabilidade de o subcomponente na rede falhar foram resumidas na tabela 9.

Tabela 9 - Percepção dos especialistas dos subcomponentes

	FÍSICA				ENLACE		TRANSPORTE			REDE	APLICAÇÃO	
	Quantidade	**Parâmetro**	**Modelo**	**Tipo**	**Configuração**	**Tipo**	**Quantidade**	**Objetivo**	**Linguagem**	**Provedor de Serviços**	**Formato**	**Público-alvo**
Esp. 1	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana	Mediana
Esp. 2	Alta	Muito alta	Muito baixa	Baixa	Alta	Alta	Baixa	Muito baixa	Baixa	Mediana	Mediana	Mediana
Esp. 3	Baixa	Alta	Mediana	Muito alta	Alta	Mediana	Mediana	Alta	Muito alta	Alta	Alta	Alta
Esp. 4	Baixa	Baixa	Baixa	Baixa	Baixa	Baixa	Mediana	Mediana	Baixa	Alta	Mediana	Alta
Esp. 5	Muito alta	Baixa	Muito alta	Muito alta	Mediana	Mediana	Mediana	Mediana	Mediana	Baixa	Muito alta	Muito alta
Esp. 6	Mediana	Mediana	Mediana	Mediana	Baixa	Baixa	Baixa	Baixa	Baixa	Baixa	Baixa	Baixa
Esp. 7	Alta	Baixa	Muito alta	Alta	Baixa	Baixa	Muito baixa	Muito baixa	Muito baixa	Muito alta	Baixa	Alta
Esp. 8	Muito baixa	Baixa	Baixa	Baixa	Baixa	Mediana	Baixa	Baixa	Baixa	Baixa	Baixa	Muito baixa
Esp. 9	Baixa	Baixa	Baixa	Baixa	Muito alta	Mediana	Muito baixa	Muito baixa	Muito baixa	Muito alta	Muito alta	Muito alta
Esp. 10	Alta	Mediana	Alta	Mediana	Alta	Mediana	Mediana	Baixa	Alta	Alta	Mediana	Alta
Esp. 11	Baixa	Baixa	Baixa	Baixa	Alta	Baixa	Alta	Mediana	Mediana	Alta	Alta	Alta
Esp. 12	Muito baixa	Muito baixa	Muito baixa	Muito baixa	Mediana	Mediana	Mediana	Baixa	Muito baixa	Alta	Baixa	Baixa

Fonte: elaborado pelo autor

Utilizamos a escala de conversão proposta por Namazian (2019) para a conversão de variáveis linguísticas em valores numéricos equivalentes, conforme a tabela 10.

Tabela 10 - Escala de conversão (falha)

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

Fonte: adaptado de Namazian (2019)

Após a conversão da probabilidade de falha percebida pelos especialistas em valores numéricos, foi possível a calcular a média e o desvio padrão para gerar a distribuição normal dos parâmetros de entrada. Essas etapas têm como objetivo reduzir a subjetividade da amostra aumentando a percepção dos especialistas.

Tabela 11 - Percepção dos especialistas sobre os subcomponentes, após a Aplicação da Escala de Conversão

	FÍSICA				ENLACE		TRANSPORTE			REDE	APLICAÇÃO	
	Quantidade	**Parâmetro**	**Modelo**	**Tipo**	**Configuração**	**Tipo**	**Quantidade**	**Objetivo**	**Linguagem**	**Provedor de Serviços**	**Formato**	**Público-alvo**
Esp. 1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
Esp. 2	0,7	0,9	0,1	0,3	0,7	0,7	0,3	0,1	0,3	0,5	0,5	0,5
Esp. 3	0,3	0,7	0,5	0,9	0,7	0,5	0,5	0,7	0,9	0,7	0,7	0,7
Esp. 4	0,3	0,3	0,3	0,3	0,3	0,3	0,5	0,5	0,3	0,7	0,5	0,7
Esp. 5	0,9	0,3	0,9	0,9	0,5	0,5	0,5	0,5	0,5	0,3	0,9	0,9
Esp. 6	0,5	0,5	0,5	0,5	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3
Esp. 7	0,7	0,3	0,9	0,7	0,3	0,3	0,1	0,1	0,1	0,9	0,3	0,7
Esp. 8	0,1	0,3	0,3	0,3	0,3	0,5	0,3	0,3	0,3	0,3	0,3	0,1
Esp. 9	0,3	0,3	0,3	0,3	0,9	0,5	0,1	0,1	0,1	0,9	0,9	0,9
Esp. 10	0,7	0,5	0,7	0,5	0,7	0,5	0,5	0,3	0,7	0,7	0,5	0,7
Esp. 11	0,3	0,3	0,3	0,3	0,7	0,3	0,7	0,5	0,5	0,7	0,7	0,7
Esp. 12	0,1	0,1	0,1	0,1	0,5	0,5	0,5	0,3	0,1	0,7	0,3	0,3

Fonte: elaborado pelo autor

Os valores apresentados na tabela 11 foram utilizados para avaliar a média e o desvio padrão para serem usados como parâmetro de entrada do modelo. E a percepção dos 12 especialistas sobre o nível de relevância, também captadas no formulário, foram resumidas na tabela 12.

Tabela 12 - Percepção dos especialistas dos componentes – relevância

	Dispositivo	**Gateway**	**Algoritmo**	**Protocolo**	**Provedor de Serviços**	**Social**	**Aplicação**
Esp. 1	Médio	Muito relevante	Médio	Médio	Muito relevante	Muito relevante	Muito relevante
Esp .2	Pouco relevante	Médio	Pouco relevante	Muito relevante	Muito relevante	Médio	Muito relevante
Esp .3	Pouco relevante	Muito relevante	Médio	Muito relevante	Muito relevante	Médio	Muito relevante
Esp .4	Pouco relevante	Pouco relevante	Médio	Médio	Muito relevante	Muito relevante	Muito relevante
Esp .5	Muito relevante	Médio	Pouco relevante	Pouco relevante	Pouco relevante	Médio	Muito relevante
Esp .6	Muito relevante	Muito relevante	Muito relevante	Muito relevante	Muito relevante	Muito relevante	Muito relevante
Esp . 7	Muito relevante	Pouco relevante	Médio	Pouco relevante	Muito relevante	Médio	Médio
Esp .8	Muito relevante	Muito relevante	Médio	Muito relevante	Médio	Muito relevante	Médio
Esp .9	Médio	Médio	Muito relevante	Pouco relevante	Médio	Muito relevante	Muito relevante
Esp .10	Pouco relevante	Médio	Médio	Médio	Muito relevante	Muito relevante	Muito relevante
Esp .11	Pouco relevante	Pouco relevante	Pouco relevante	Pouco relevante	Muito relevante	Muito relevante	Muito relevante
Esp. 12	Pouco relevante	Médio	Pouco relevante	Médio	Muito relevante	Médio	Pouco relevante

Fonte: elaborado pelo autor

4.2.2.2. REDES BAYESIANAS E MONTE CARLO

Após a conversão da percepção dos especialistas em relação à probabilidade do componente falhar, esta foi utilizada como ponto de partida inicial para definição das probabilidades a priori da rede bayesiana. Seguindo a distribuição normal com média e desvio padrão recebidos da avaliação da rede foi utilizada para representar a percepção de probabilidade de falha.

A distribuição normal é frequentemente empregada para modelar variáveis contínuas que seguem padrões de distribuição simétricos em torno de uma média específica. No contexto da probabilidade de falha em redes IoT, a distribuição normal pode ser utilizada para representar a incerteza associada a parâmetros críticos, como o tempo médio entre falhas de dispositivos, a taxa de erro de transmissão ou a capacidade de processamento de servidores na rede.

Ao aplicar a distribuição normal no cálculo da probabilidade de falha, podemos modelar a variabilidade e a dispersão dos dados em torno da média, permitindo uma análise mais abrangente dos riscos potenciais enfrentados pela rede IoT. Além disso, a distribuição normal oferece uma abordagem probabilística robusta para estimar a probabilidade de ocorrência de eventos de falha em diferentes cenários operacionais.

E para representar o impacto no modelo foram utilizadas as percepções dos especialistas em relação à relevância do componente. Essa percepção, segue uma distribuição uniforme, uma vez que atribui igual probabilidade a todos os valores dentro de um intervalo específico. Essa distribuição uniforme foi escolhida como uma simplificação inicial antes de introduzir distribuições mais complexas, conforme a Tabela 13.

Tabela 13 - Escalas de Conversão (Impacto)

Relevância	**Valor atribuído**
Pouco Relevante	1–3
Médio	3–6
Muito Relevante	6–9

Fonte: adaptada pelo autor de Bayraktar (2009)

Após definidas as distribuições a serem utilizadas, o Método Monte Carlo Clássico foi aplicado. Uma vez que se trata de um método flexível e que é possível ser aplicado a uma ampla gama de problemas complexos. Além de permitir a modelagem de sistemas e processos com múltiplas variáveis.

Para utilizar as percepções dos especialistas no modelo foi necessário realizar as conversões linguísticas aplicadas para a probabilidade de falha e o impacto, adaptadas de Namazian (2019) e Bayraktar (2009), respectivamente. Após a conversão a probabilidade de falha e o impacto foram multiplicados a cada iteração e foram realizadas 1000 iterações (CHRISTOPOULOS, 1998). E ao final das iterações, a média aritmética foi calculada para encontrar o risco de falha da rede.

Assim, constatou-se que o Método Monte Carlo permite a validação de modelos e a avaliação da robustez das conclusões em relação à variabilidade nos dados e nas suposições do modelo, conforme descrito nos tópicos seguintes.

4.2.3. SIMULAÇÃO: MODELAGEM COMPUTACIONAL DO MODELO

Para o desenvolvimento em Python (versão 3.10.12) foi utilizado a biblioteca PyAgrum no desenvolvimento de redes bayesianas. O PyAgrum (versão 1.1.0) é uma biblioteca cientifica dedicada para a construção de redes Bayesianas. E permite criar, modela, aprender, usar e calcular redes bayesianas e outros modelos.

Para o desenvolvimento foi utilizado o Google Colab, por se tratar de um ambiente prático e sem custos

4.2.3.1. 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, o que pode tornar a validação completa muito difícil. Segundo Librantz (2020), a utilização de dois axiomas é utilizada para a validação parcial do modelo.

4.2.3.2. AXIOMAS

Axioma da Probabilidade Condicional (Axioma 1)

Um ligeiro aumento/diminuição no nó pai no Axioma 1 resulta um aumento/diminuição no nó filho, ou seja, são diretamente proporcionais. Com isso, seja P(A|B) a probabilidade de um evento AA ocorrer dado que o evento BB ocorreu. O axioma da probabilidade condicional estabelece que:

Este axioma descreve como a probabilidade de um evento condicionado a outro evento é calculada com base na probabilidade conjunta dos dois eventos.

Regra da cadeia (Axioma 2)

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

A regra da cadeia é uma aplicação do axioma da probabilidade condicional. Ela descreve como calcular a probabilidade de múltiplos eventos ocorrerem em sequência.

Este axioma descreve como calcular a probabilidade conjunta de uma série de eventos, considerando as probabilidades condicionais de cada evento dado os eventos anteriores na sequência.

Esses axiomas formam a base para a construção de redes bayesianas e a atualização das probabilidades ao longo dos nós da rede.

4.2.3.3. EXEMPLOS DE APLICAÇÕES – CENÁRIOS

A eficácia do modelo proposto pode ser verificada a partir de outros 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 fatores pai, conforme os cenários abaixo (KINJO *et al*, 2022):

Cenário 1: Monitoramento de sala climatizada

- Seis parâmetros são configurados, onde cinco 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 no 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, armazenar 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 e transmitindo os dados 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 à 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 14.

Tabela 14 - Cenários de Aplicação

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

Fonte: Elaborado pelo autor

Os cenários acima citados foram também resumidos também em relação à relevância para a rede, conforme a Tabela 15.

Tabela 15 - Cenários de Aplicação

		Relevância		
		Cenário 1	**Cenário 2**	**Cenário 3**
Dispositivo/Sensor	Quantidade	POUCO RELEVANTE	MUITO RELEVANTE	MUITO RELEVANTE
	Parâmetro	POUCO RELEVANTE	MEDIO	MUITO RELEVANTE
	Tipo	MEDIO	MUITO RELEVANTE	MUITO RELEVANTE
Gateway	Tipo	MUITO RELEVANTE	MUITO RELEVANTE	MUITO RELEVANTE
Algoritmo	Quantidade	POUCO RELEVANTE	MEDIO	MEDIO
	Objetivo	MEDIO	MUITO RELEVANTE	MUITO RELEVANTE
Protocolo	Configuração	POUCO RELEVANTE	MUITO RELEVANTE	MUITO RELEVANTE
Provedor de Serviços	Recursos	POUCO RELEVANTE	MUITO RELEVANTE	MUITO RELEVANTE
Social	Ético	MUITO RELEVANTE	POUCO RELEVANTE	MUITO RELEVANTE
Aplicação	Formato (tipo)	MEDIO	MEDIO	MUITO RELEVANTE
	Público-alvo	MEDIO	MUITO RELEVANTE	MUITO RELEVANTE

Fonte: Elaborado pelo autor

5. RESULTADOS E DISCUSSÕES

Neste capítulo são apresentados os principais resultados do trabalho e suas respectivas discussões.

5.1. PADRONIZAÇÃO DE ARQUITETURA

A implantação e utilização de uma rede IoT é permeada de desafios técnicos, um dos mais citados é o gerenciamento da segurança. Para isso, entender a função de cada componentes da rede IoT e organizá-los de forma a extrair o máximo das suas potencialidades e benefícios se faz necessário. No entanto, dentre os trabalhos estudados notou-se a falta de padronização ao representar a rede e os respectivos componentes classificados em cada camada.

Portanto, a falta de padronização de uma representação de uma arquitetura IoT torna os modelos difíceis de comparação. Por exemplo, no modelo proposto por Ren (2017), a heterogeneidade dos dispositivos ainda é considerado um desafio, ou seja, inviável ao considerarmos redes IoT, cuja característica marcante é a possibilidade de conexão com diversos dispositivos.

Já na arquitetura de Chiang (2016), a Fog Computing, a heterogeneidade dos dispositivos conectados à rede não foi um problema. Trata-se de uma abordagem revolucionária para lidar com os desafios de processamento e distribuição de dados em sistemas de IoT. No entanto, essa arquitetura tem alto custo de manutenção e é suscetível a ataques. Com isso, ao abordar a privacidade e segurança dos dados, esta arquitetura ainda precisaria superar esse desafio.

E o modelo proposto pela IEC/ISO 30141/2018, apesar de adotar um padrão internacional e possivelmente garantirá a maior confiança dos clientes. Este modelo tem um custo inicial alto em: treinamento, ferramentas e recursos humanos especializados. Esse custo inicial alto é devido à complexidade para organizações, principalmente menores e menos experientes.

O modelo OSI foi utilizado neste trabalho como base para representar uma rede IoT, pois é um modelo consolidado para representar uma arquitetura de rede. Além disso, nenhum detalhe dos componentes da rede levantados e validados pelos especialistas são perdidos, além de promover padronização e interoperabilidade. E,

ainda, é um modelo bem estabelecido em redes, facilitando sua compreensão e análise.

A adoção do modelo OSI auxilia o entendimento e padronização da comunicação em tecnologias de redes, uma vez que seu uso em arquiteturas de redes já é consolidado. Além disso, o modelo divide a comunicação em camadas, permitindo que desenvolvedores e engenheiros se concentrem em problemas específicos sem se preocupar com a implementação de outras camadas. Isso facilita o design e a implementação de protocolos e aplicações IoT.

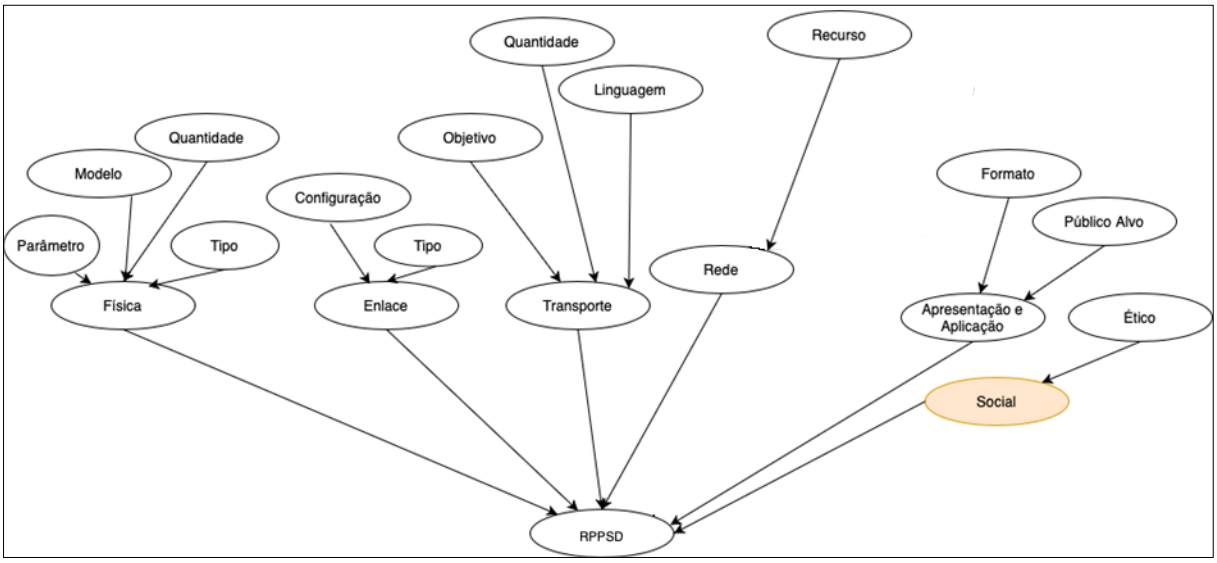
Com a divisão em camadas, torna-se mais fácil identificar e resolver problemas de comunicação. Ao adotar o modelo em camadas a inclusão de novas tecnologias não afeta outras camadas da rede, proporcionando maior flexibilidade (PALATTELLA, 2013).

5.2. MODELO OSI *

Como mencionado no tópico anterior, este trabalho utilizou o modelo de representação de uma rede baseado em camadas, uma vez que é o modo de representação mais utilizado na literatura. E utilizou-se do modelo em camadas OSI, uma vez que este apresentou mais vantagens ao utilizar a rede IoT no contexto de privacidade e segurança dos dados. A partir do modelo de OSI desenvolveu-se o modelo OSI*, de modo que os detalhes do componente X função na rede fossem completamente explorados. O levantamento dos componentes da rede foram, inclusive, validado por especialistas em KINJO (2022).

Por isso neste trabalho propomos o modelo OSI*, no qual os componentes foram classificados em camadas inclusive o componente Social, conforme a Figura 15.

Figura 15 - Representação do Modelo, com o Componente Social



Fonte: elaborado pelo autor

A princípio, o Componente social não se encaixava na classificação do modelo OSI. No entanto, de acordo com a pesquisa apresentada no capítulo de introdução, o fator humano foi considerado um elemento fundamental para o sucesso na implantação de redes IoT. A Tabela 1 desse trabalho apresenta o componente social diretamente relacionado ao fator humano, podendo indicar que esse é um fator que poderia impactar significativamente a rede.

Além da preocupação demonstrada na pesquisa de mercado, as questões sociais também são fonte de preocupação de outros autores. A partir disso, houve o surgimento, inclusive, de um novo termo: o Social Internet of Things (SIoT).

Como mencionado anteriormente a escolha pela adoção do modelo baseado nas camadas OSI proporciona a inclusão de novas tecnologias na rede nas camadas da rede sem comprometer o funcionamento da rede. Por isso, o modelo OSI* proporcionou melhor adaptação ao problema proposto, uma vez que questões sociais são fatores preocupantes na literatura e essas questões críticas foram destacadas pelos especialistas. E para incluir esse componente, considerado entre um dos três mais críticos do modelo (KINJO, *et al* 2022), o modelo OSI* proposto e desenvolvido neste trabalho.

5.3. DESENVOLVIMENTO DO MODELO

Em virtude da familiaridade com a linguagem, o modelo final foi desenvolvido em Python. Para isso, foi utilizada a biblioteca PyAgrum que foi escolhida pela sua simplicidade de gerar os gráficos e as tabelas para o modelo. A Figura 16, mostra o pseudo-código.

Figura 16 - Pseudo-Código

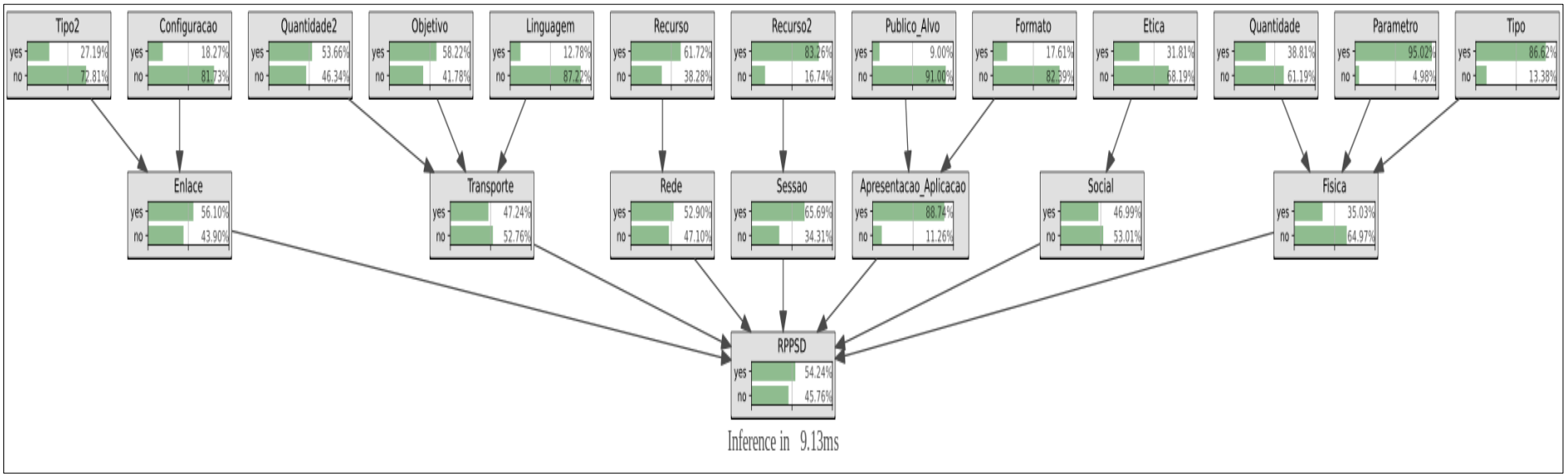
```
INICIO

  //DEFININDO AS ENTRADAS

  DEFINIR probabilidade_falha = distribuição normal
  DEFINIR impacto_falha = distribuição uniforme


  // DEFINIR ESTRUTURA DA REDE
  rede_modelo = ("Fisica{yes|no}->RPPSD{yes|no}<-Enlace{yes|no};\
                 Transporte{yes|no}->RPPSD{yes|no}<-Rede{yes|no};\
                 Sessao{yes|no}->RPPSD{yes|no}<-
Apresentacao_Aplicacao{yes|no};\
                 Social{yes|no}->RPPSD{yes|no};\
                 Quantidade{yes|no}->Fisica<-Parametro{yes|no};\
                 Fisica<-Tipo{yes|no};\
                 Tipo2{yes|no}->Enlace<-Configuracao{yes|no};\
                 Quantidade2{yes|no}->Transporte<-Objetivo{yes|no};\
                 Linguagem{yes|no}->Transporte;\
                 Recurso{yes|no}->Rede;\
                 Recurso2{yes|no}->Sessao;\
                 Etica{yes|no}->Social;\
                 Publico_Alvo{yes|no}->Apresentacao_Aplicacao<-
Formato{yes|no}")

  // DEFINIR AS TABELAS DE PROBABILIDADES CONDICIONAIS  (CPT)

      DEFINIR CPT_Falha: P(Falha) = probabilidade_falha
      DEFINIR CPT_Impacto: P(Impacto | Falha) = impacto


  // CALCULAR O RISCO DE FALHA
  FUNÇÃO calcular_risco()
      P(Risco) = P(Falha) * P(Impacto | Falha)
      RETORNAR P(Risco)
  FIM FUNÇÃO
```

```
  // FUNÇÃO MONTE CARLO
  FUNÇÃO calcular_risco_monte_carlo(N)
      DEFINIR soma_risco = 0

      // REALIZAR 1000 ITERAÇÕES
      PARA i DE 1000 ATÉ N FAÇA
          // Gerar uma amostra aleatória de falha
          falha_ocorre = gerar_aleatorio(0, 1) < probabilidade_falha

          // Calcular o impacto
          SE falha_ocorre ENTÃO
              impacto = impacto_falha // Se falha ocorre, impacto é
total
          SENÃO
              impacto = 0 // Se não há falha, impacto é zero
          FIM SE

          // Somar o risco
          soma_risco = soma_risco + impacto
      FIM PARA

      // Calcular a média do risco
      media_risco = soma_risco / N
      RETORNAR media_risco

FIM FUNÇÃO
```

Fonte: elaborado pelo autor

O resultado do modelo desenvolvido no PyAgrum foi representado na Figura 17.

Figura 17- Modelo Desenvolvido em Python, utilizando o PyAgrum

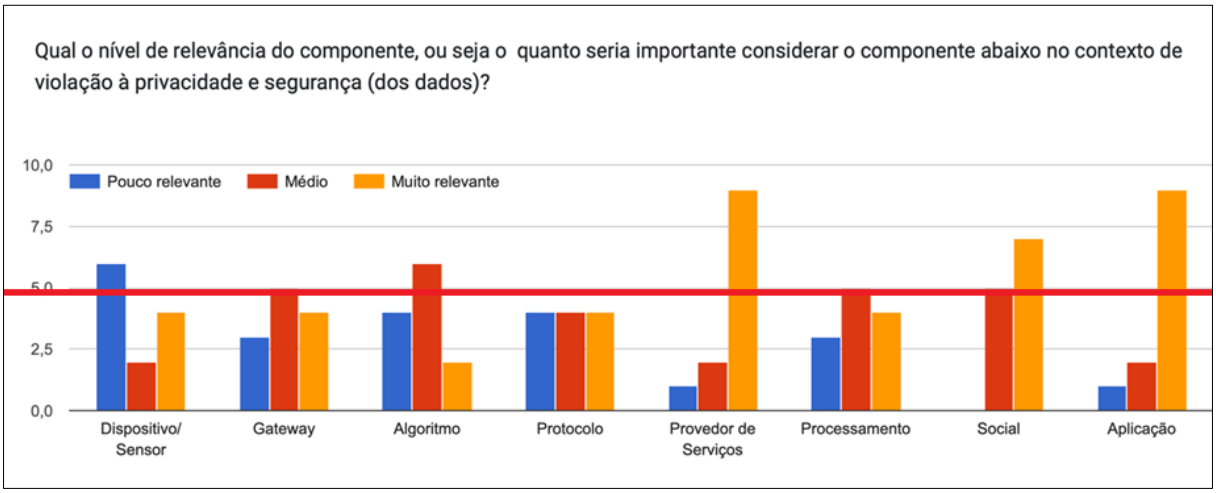


Fonte: elaborado pelo autor

5.4 CRITICIDADE

Na fundamentação teórica questões éticas/sociais foram levantadas como um dos pontos de preocupação dessas tecnologias. A criticidade desse componente foi corroborada também nas pela percepção dos especialistas. O resultado da pesquisa apresentou o componente Provedor de Serviço, Social e Aplicação entre os mais relevantes para o modelo, conforme destacado na Figura 18.

Figura 18 - Relevância do Componente



Fonte: elaborado pelo autor

Destaca-se ainda que o componente Social não foi considerado por nenhum dos especialistas com pouca relevância.

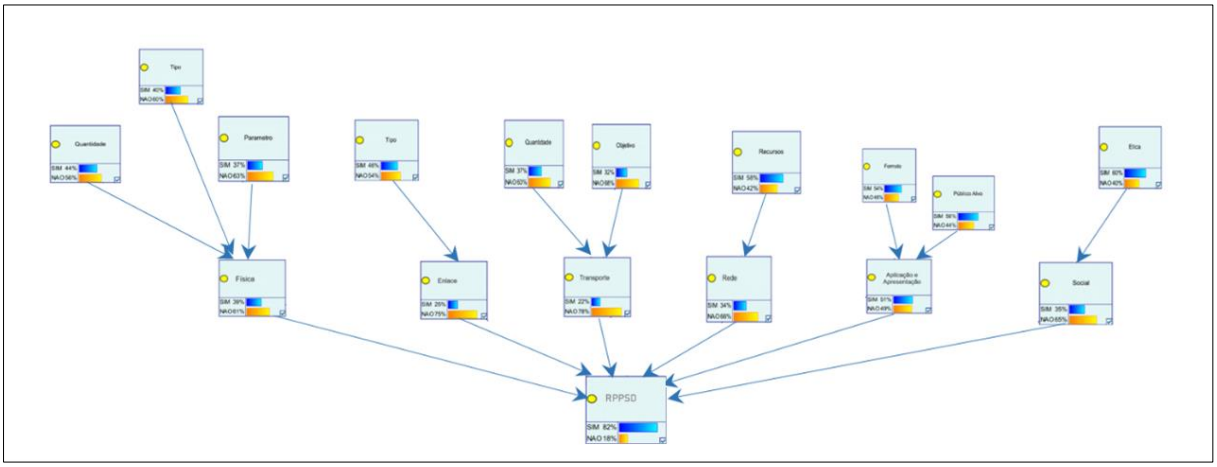
E ainda, possivelmente devido à dificuldade de estabelecer um padrão de representação na rede (conforme o item 5.1 Padronização da arquitetura) é devido ao Provedor de Serviços. Este componente diverge entre os autores estudados em relação à responsabilidade.

Sendo este o principal ponto de divergência de classificação na definição e quantidade de camadas ao representar uma rede, como, por exemplo: de que componente seriam os responsáveis por essa tarefa: os dispositivos móveis/ wereables ou os servidores.

5.5 VALIDAÇÃO: COMPARAÇÃO COM OUTROS SOFTWARES

O modelo desenvolvido em Python foi comparado com outras ferramentas já homologadas pela comunidade acadêmica, como o GENIE, conforme apresentado na Figura 19.

Figura 19 - Modelo Desenvolvido no Software GENIE



Fonte: elaborado pelo autor

No modelo desenvolvido no GENIE os componentes foram evidenciados e a probabilidade de falha correspondeu proporcionalmente à quantidade de componentes evidenciados, conforme demostrado na Tabela 16.

Tabela 16 - Modelo desenvolvido no GENIE

	Probabilidade de Falha	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: elaborado pelo autor

No modelo desenvolvido no Python os componentes foram evidenciados e a probabilidade de falha correspondeu proporcionalmente à quantidade de componentes evidenciados, conforme apresentado na Tabela 17.

Tabela 17 - Modelo desenvolvido no Python

	Probabilidade de Falha	Variação (%)
Prévia	0,80	0
Configuração (Protocolo)	0,81	1,3
Configuração (Protocolo): Parâmetros (Dispositivo)	0,82	3,2
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços)	0,84	4,6
Configuração (Protocolo): Parâmetros (Dispositivo):Recursos (Provedor de Serviços): Ética (Social)	0,86	5,01

Fonte: elaborado pelo autor

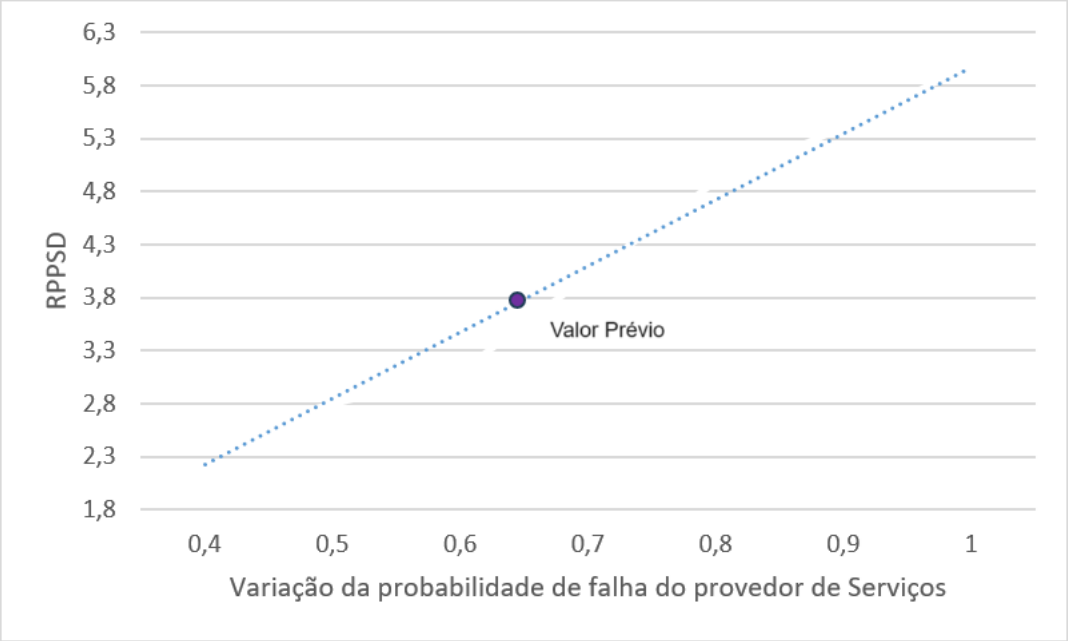
Nota-se que os dois modelos respondem ao axioma. E ao comparar a probabilidade de falha entre os modelos, a diferença foi de 2%.

5.6 VALIDAÇÃO: AXIOMAS

Conforme apresentado na Aplicação numérica, o modelo apresentado foi validado de acordo com 2 axiomas:

O gráfico mostrado na Figura 20 corrobora o Axioma 1, no qual o risco de violação à privacidade e segurança dos dados aumenta conforme o nó pai Recursos, referente ao Provedor de Serviços. Assim como diminuirá conforme o nó pai diminui.

Figura 20 - Variação da probabilidade de falha do Provedor de Serviços X Risco



Fonte: elaborado pelo autor

A Tabela 18 apresenta os resultados do segundo experimento para validação.

Essa tabela representa que quando a condição de Recursos (da camada Rede) é definida como 100%, o risco de violação à privacidade e segurança dos dados aumenta 1,3 %. Além disso, quando outro componente é adicionado, o risco é ainda maior que o anterior.

Tabela 18 - Validação do Modelo (axioma 2)

	Risco de Perda de Privac. e Seg. (dos dados)	Variação (%)
Prévia	0,80	0
Recurso (Rede)	0,83	1,3

Recurso (Rede): Parâmetros (Física)	0,84	3,4
Recurso (Rede) Parâmetros (Física):Recursos (Sessão)	0,84	5,2
Recurso (Rede) Parâmetros (Física):Recursos (Sessão): Público Alvo(Apresentação_Aplicação)	0,85	6,8

Fonte: elaborado pelo autor

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

5.7 VALIDAÇÃO: EXEMPLOS DE APLICAÇÃO

Conforme mencionado no tópico de aplicação numérica para avaliar a eficácia do modelo, com o auxílio de uma especialista, foram criados 03 (três) cenários que o modelo pode ser aplicado:

Uma vez calculado a probabilidade da rede falha no cenário 1, monitoramento de sala climatizada, cada componente foi multiplicado pelo impacto para obter o risco conforme a Tabela 19.

Tabela 19 - Risco no Cenário 1

		Falha	Impacto
FÍSICA	Quantidade	0,44	2
	Parâmetro	0,4	2
	Tipo	0,37	4
ENLACE	Tipo	0,4	7
TRANSPORTE	Quantidade	0,37	2
	Objetivo	0,32	4
REDE	Provedor de Serviços	0,58	2
APLICAÇÃO	Público	0,54	8
	Formato	0,59	4
SOCIAL	Ética	0,6	4

Fonte: elaborado pelo autor

Ao final, a probabilidade de falha do contexto de privacidade e segurança dos dados foi de 3,16.

No cenário 2, monitoramento de Polissonografia Home Care**,** o modelo foi implementado e a probabilidade de falha de cada componente foi multiplicado também pelo impacto para obter o risco. E para o cenário 2, obtivemos o risco de 7,89.

Por fim, para o cenário 3, monitoramento e controle de gotejamento de medicação, repetimos o mesmo procedimento para os cenários anteriores obtendo-se o risco de 8,91.

Após a implementação e definição do risco, dado por probabilidade de falha × impacto, e foi possível definir um ranking de risco para os cenários propostos. A Tabela 20 representa o ranking do risco desses cenários.

Tabela 20 - Ranking de Cenários

Sistema	Classificação	Risco
Cenário 3	1	8,91
Cenário 2	2	7,89
Cenário 1	3	3,16

Fonte: elaborado pelo autor

De acordo com o ranking, o cenário 3 é o mais crítico e com o maior risco associado. Possivelmente, isso ocorreu devido às consequências graves que uma falha nessa rede pode acarretar, colocando em risco a vida do paciente. A falha da rede no cenário 3 também pode ocasionar:

- Administração incorreta de medicação: uma falha na rede pode resultar em erros na administração da medicação, como subdosagem ou superdosagem. E comprometer a eficácia do tratamento do paciente
- Complicações médicas: uma dosagem inadequada do medicamento pode não tratar adequadamente a condição do paciente e uma superdosagem pode causar efeitos colaterais adversos. E em ambas as situações a vida do paciente estará em risco, afetando o tratamento da enfermidade.

No cenário 2, a falha na rede pode não acarretar diretamente na vida do paciente. No entanto, entre as possíveis consequências estão:

- Perda de dados do monitoramento: ausência de dados cruciais durante o monitoramento da polissonografia do paciente. Com isso, a precisão para identificação de problemas de saúde fica comprometida

- Diagnósticos comprometidos: a imprecisão dos dados pode comprometer o diagnóstico e, consequentemente, atrasar/interromper o início de um tratamento eficaz
- Segurança e confiança comprometidos: geralmente, o monitoramento do paciente envolve a coleta de dados do paciente durante vários dias ou semanas. A falha na rede pode interromper essa coleta contínua de dados, prejudicando a capacidade de acompanhar a evolução do paciente e, até mesmo, provocar vazamento de dados sensíveis.
- Custos de saúde: uma falha na rede pode acarretar custos adicionais de saúde, tais como repetição de exames de polissonografia, consultas médicas (devido à imprecisão dos dados). E, em casos mais graves, possíveis hospitalizações do paciente em razão da demora no diagnóstico correto.

Considerando o cenário 1, a falha na rede tem consequências em escalas um pouco menores, não colocando, diretamente, a vida de uma pessoa/produto/equipamento em perigo. Entre as possíveis consequências podemos citar:

- Controle ambiental desregulado: perda do controle ambiental da sala climatizada, podendo ocasionar variações indesejadas na temperatura, umidade ou outros parâmetros. Essa variação afeta o conforto das pessoas no ambiente e, em casos extremos, pode comprometer a qualidade de produtos ou equipamentos sensíveis.
- Eficiência operacional: uma sala com climatização desregulada pode ocasionar uso excessivo e desnecessário de energia para manter as condições ambientais estáveis.
- Não conformidade com as normas: em alguns setores como saúde e alimentício, principalmente, o monitoramento do ambiente é crucial para cumprir normas de segurança. Em alguns casos, uma falha na rede pode ocasionar violações regulatórias e implicações legais consequentes.

Em todos os cenários a falha na rede IoT pode afetar pessoas/ produtos/ equipamentos em maior ou menor escala. No entanto, em todos a segurança e confiança na rede ficam comprometidas. Quando se trata de dados relacionados a

uma pessoa, no qual envolve a coleta de dados do paciente ao longo do tempo. A falha na rede pode interromper essa coleta contínua de dados, prejudicando a capacidade de acompanhar a evolução do paciente e até mesmo vazamento de dados sensíveis. E as leis de proteção de dados aplicam multas rigorosas nesses casos e mais do que isso a imagem da instituição que não possui esse cuidado fica prejudicada.

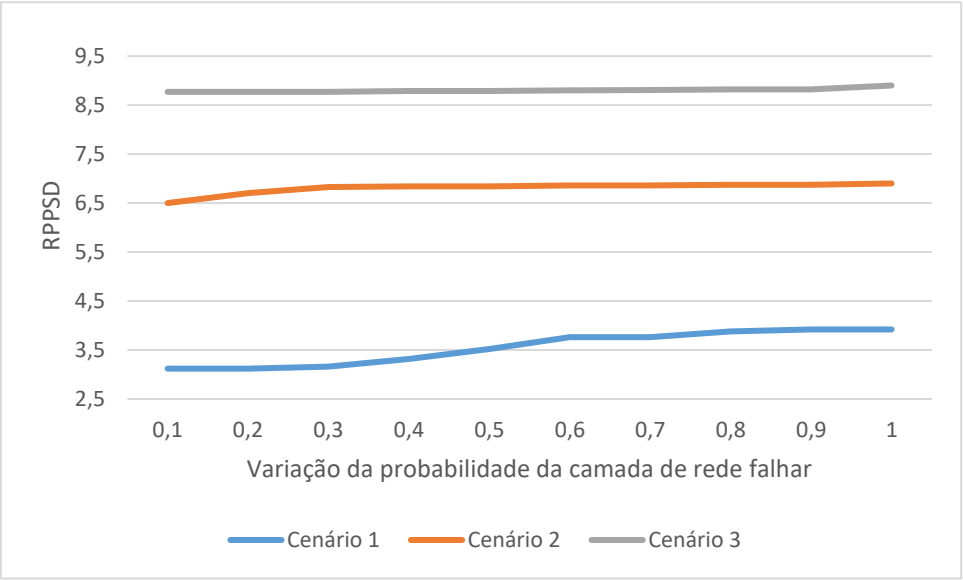
Em todos os cenários, falhas na rede IoT podem afetar pessoas/produtos/equipamentos em maior ou menor escala. Portanto, em todos os cenários, segurança e confiança na rede ficam comprometidas quando se trata de dados relacionados a indivíduos, que envolva a coleta de dados de pacientes ao longo do tempo. Assim sendo, falhas na rede podem interromper a coleta contínua de dados, prejudicando o acompanhamento da evolução do paciente e, até mesmo, podendo acarretar o vazamento de dados sensíveis. Nesses casos, as leis de proteção de dados aplicam multas rigorosas. Além disso, a imagem da instituição que não adota esses cuidados fica muito prejudicada.

Por isso é importante implementar estratégias de redundância, monitoramento de sistemas críticos, manutenção preventiva, backup de dados, planos de contingência, protocolos de segurança robustos, E principalmente da conscientização das pessoas que utilizam a rede, evitando assim vazamento de dados devido a questões éticas/sociais.

Por essa razão, é importante implementar estratégias de redundância, monitoramento de sistemas críticos, manutenção preventiva, backup de dados, planos de contingência e protocolos de segurança robustos para evitar que falhas na rede não ocorram. E, principalmente, investir na conscientização das pessoas que utilizam a rede para prevenir um possível vazamento de dados devido a questões éticas/sociais.

O mesmo modelo foi aplicado também variando de 0 a 100% a probabilidade de falha no componente camada de rede, simulando o efeito da variação deste componente na classificação do risco dos sistemas, representado na Figura 21.

Figura 21 – Efeito do componente de “*camada da rede*” na classificação do risco dos sistemas



Fonte: elaborado pelo autor

A partir dos resultados verifica-se que a classificação dos sistemas não se altera, permanecendo o mesmo ranking Cenário 3, Cenário2, Cenário 1. O Cenário 3, o monitoramento e controle de gotejamento de medicação representam um aspecto crítico dos cuidados de saúde modernos. A precisão na administração de medicamentos e fluidos, a segurança dos dados e a proteção contra falhas técnicas e cibernéticas são fundamentais para garantir a eficácia e a segurança do tratamento. Portanto, é essencial que instituições de saúde implementem práticas rigorosas de monitoramento, manutenção e segurança para proteger esses dispositivos e assegurar que o tratamento seja realizado de forma segura e eficaz.

6. CONCLUSÕES

A análise os riscos em redes Internet das Coisas (IoT) são essenciais para garantir a confiabilidade e a segurança desses sistemas complexos e interconectados. Este trabalho explorou a aplicação das redes bayesianas e do método de Monte Carlo como ferramentas eficazes para mensurar os riscos associados a redes IoT. A integração dessas técnicas oferece uma abordagem robusta para a modelagem e avaliação de incertezas.

Ao utilizar Monte Carlo para aumentar a quantidade de percepções dos especialistas permitiu a redução da subjetividade e, com isso, mensurar o risco de privacidade e segurança dos dados. As redes bayesianas proporcionam uma estrutura gráfica poderosa para representar e analisar as relações de dependência entre os diversos componentes de uma rede IoT. Elas facilitam a compreensão das interações entre os elementos da rede e permitem a incorporação de informações incertas, o que é crucial para a avaliação de riscos em sistemas dinâmicos e complexos. Por outro lado, o método de Monte Carlo complementa essa análise ao permitir simulações estocásticas que ajudam a quantificar a probabilidade de diferentes cenários de falha e suas consequências.

Assim sendo, para a teoria, este trabalho propôs uma representação de uma rede IoT, o modelo OSI*. O modelo OSI*, é uma evolução de um modelo já aceito ao representar redes de computadores e ao aplicar no contexto de redes Internet das Coisas esta representação proporcionou esclarecer os componentes que foram classificados em cada camada.

A classificação dos componentes nas camadas da rede sofre divergências entre os trabalhos já existente. E este trabalho classificou os componentes já levantados na literatura e validados por especialistas, de modo que a inclusão ou exclusão de um componente na rede é facilmente classificado. Além disso o modelo OSI *, inclui componentes externos para modelagem e simulação no risco de privacidade e segurança dos dados em redes IoT.

O componente externo, questões sociais, foram elencadas como críticas pelos especialistas e corroborada pelos autores estudos. Portanto não poderiam ser retiradas do modelo OSI*.

A aplicação prática deste trabalho, o modelo pode ser utilizado como uma ferramenta na implantação de projetos de IoT e possivelmente, aumentar o sucesso na construção e manutenção de projetos de IoT, conforme destacado na introdução.

Inicialmente, optou-se por estudar o risco de violação à privacidade e segurança dos dados, pois o tema foi identificado como um dos mais abordados nos trabalhos estudados e pesquisas de mercado. No entanto, posteriormente, outros riscos como integridade de dados e rastreabilidade poderão ser estudados ou até mesmo testados, utilizando o modelo proposto nesse trabalho.

7. REFERÊNCIAS

ABROON Qazi, ABDULRAHIM Shamayleh, SAMEH El-Sayegh, STEVEN Formaneck, Prioritizing risks in sustainable construction projects using a risk matrix-based Monte Carlo Simulation approach, **Sustainable Cities and Society**, v. 65, 2021, doi: https://doi.org/10.1016/j.scs.2020.102576

AHMED, Fizar, An Internet of Things (IoT) Application for Predicting the Quantity of Future Heart Attack Patients, **International Journal of Computer Applications** , v.164, ed.6, p.36-40, 2017, doi:10.5120/ijca2017913773

ALMUSAYLIM, Zahrah A., ALHUMAM, Abdulaziz, JHANJHI, Noor Zaman, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review, **Ad Hoc Networks**, v. 101, ed. 6, 2020, doi:10.1016/j.adhoc.2020.102096

AL-FUQAHA, A., GUIZANI, Mohsen. MOHAMMADI, Mehdi; ALEDHARI, Mohammed; AYYASH, Moussa. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. **IEEE Communications Surveys & Tutorials**, v. 17, n. 4, p. 2347-2376, 2015, doi: 10.1109/COMST.2015.2444095

ALANEZI, Mohammed Ateeq. Vulnerabilities, Threats and Challenges on Cyber Security and the Artificial Intelligence based Internet of Things: A Comprehensive Study; **INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY**, vol.22, ed.2, p.153-158. 2022

ALWARAFY, Alwarafy; Al-Thelaya, Khaled ; Abdallah, Mohamed; Schneider, Jens; Hamdi, Mounir, A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things, **IEEE INTERNET OF THINGS JOURNAL**, v.8, 2021, doi: 10.1109/JIOT.2020.3015432

AL-SARAWI, Shadi, Anbar, Mohammed, Abdullah, Rosni, Al Hawari, Ahmad, Internet of Things Market Analysis Forecasts, 2020–2030. **2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)**, IEEE, 2020.doi: 10.1109/WorldS450073.2020.9210375

ALSHOHOUMI, Fatma, Sarrab, Mohammed, AlHamadani, Abdulla, Al-Abri, Dawood, Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns. **INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS**, v.10, ed. 7, p.232-251, 2019. doi: 10.14569/IJACSA.2019.0100733

ANAJEMBA, Joseph Henry, TANG,YUE, Iwendi, CELESTINE, Ohwoekevwo, AKPESIRI Srivastava, Gautam, JO, Ohyun, Realizing Efficient Security and Privacy in IoT Networks, **SENSORS**, vol. 20, 2020, doi: 10.3390/s20092609

Associação Brasileira de Internet das Coisas[1]. Segurança em IoT: desafios e estratégias de proteção no mundo conectado. Disponível: < https://abinc.org.br/seguranca-em-iot-desafios-e-estrategias-de-protecao-no-mundo-conectado/>, acessado em: 16.mai.2023

Associação Brasileira de Internet das Coisas [2]. Aplicações de IoT que se tornaram viáveis com o 5G. Disponível: <https://abinc.org.br/aplicacoes-de-iot-que-se-tornaram-viaveis-com-o-5g/ >, acessado em: 16.mai.2023

ATTAULLAH, Hasina, KANWAL, Tehsin, ANJUM, Adeel, AHMED, Ghufran, KHAN, Suleman, RAWAT, Danda B. , KHAN, Rizwan, **Fuzzy-Logic-Based Privacy-Aware Dynamic Release of IoT-Enabled Healthcare Data**, IEEE INTERNET OF THINGS JOURNAL, v.9, 2022, doi: 10.1109/JIOT.2021.3103939

ATZORI, Luigi, IERA, Antonio, MORABITO, Giacomo, The Internet of Things: A Survey, **Computer Networks**, v. 54, p. 2787–2805. 2010, doi: https://doi.org/10.1016/j.comnet.2010.05.010

ATZORI, Luigi, IERA, Antonio, MORABITO, Giacomo, NITTI, Michele, The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization, **COMPUTER NETWORKS**, v.56, ed. 16, p. 3594-3608, 2012, doi: 10.1016/j.comnet.2012.07.2012

AYDOS, Murat, VURAL, Yilmaz, Tekerek, Adem, Assessing risks and threats with layered approach to Internet of Things security, **MEASUREMENT & CONTROL**, v. 52, ed. 5-6, p. 338- 353, 2019, doi: 10.1177/0020294019837991

BARANOWSKI, Jerzy, Predicting IoT failures with Bayesian workflow. **Eksploatacja i Niezawodność – Maintenance and Reliability**, v. 24, ed.2, p.248–259, 2022.

BARMISH, Ross, LAGOA, Costantino, The uniform distribution: A rigorous justification for its use in robustness analysis. **Math. Control Signal Systems** ,v. ed. 10, 203–222, 1997, doi: https://doi.org/10.1007/BF01211503

BAYRAKTAR, Mehmet Emre, HASTAK , Makarand, A decision support system for selecting the optimal contracting strategy in highway work zone projects . **Automation in Construction**. v.18, p-834-843, 2009.

BYRNES, J.M.; Lin, YJ; Tsai, TR; Lio, YL. Bayesian Inference of delta = P(X < Y) for Burr Type XII Distribution Based on Progressively First Failure-Censored Samples. **MATHEMATICS**. vol.7. ed. 9. 2019

BINMORE, Kenneth, Imaginary Philosophical Dialogues between Sages down the Ages, **Editora Springer**. 2020

BORGIA, Eleonora, The Internet of Things Vision: Key Features, Applications and Open Issues, **Computer Communications**, v.54, p1–31, 2014, doi: http://dx.doi.org/10.1016/j.comcom.2014.09.008

BRINGHENTI, Daniele, MARCHETTO, Guido, SISTO, Riccardo, VALENZA, Fulvio, Automation for Network Security Configuration: State of the Art and Research Trends, **ACM COMPUTING SURVEYS**, v.56, ed. 3, 2023, doi: 10.1145/3616401

CAMPANILE, Lelio; IACONO, Mauro, MARULLI, Fiammentta, MASTROIANNI, Michele, MAZZOCCA, Nicola, Toward a Fuzzy-based Approach for Computational Load Offloading of IoT Devices, **JOURNAL OF UNIVERSAL COMPUTER SCIENCE**, v. 26, ed. 11, p. 1455-1474, 2020, doi: 10.3897/jucs.2020.077

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, doi: https://doi.org/10.1016/j.im.2020.103335

CHEN, Qingyu, CHEN, Li, WANG, Haibin, WU, Longsheng, LI, Yuanqing, ZHAO, Xing, CHEN, Mo, Instruction-Vulnerability-Factor-Based Reliability Analysis Model for Program Memory**. Journal of Electronic Testing: Theory and Applications (JETTA)**. v. 32, p. 695-703, 2016, doi: 10.1007/s10836-016-5624-y

CHETTRI, Lalit, BERA, Rabindranath, A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems, **IEEE INTERNET OF THINGS JOURNAL**, v. 7, ed.1, p-16-32, 2020, doi: 10.1109/JIOT.2019.2948888

CHIANG, Mung, ZHANG, Tao, Fog and IoT: An Overview of Research Opportunities, **IEEE INTERNET OF THINGS JOURNAL,** v.3, p. 854-864, 2016, doi: 10.1109/JIOT.2016.2584538

CHICK, Stephen; Bayesian Analysis For Simulation Input And Output. **Winter Simulation Conference Proceedings**. 1997.

CHOI, Gwang Hui, NA, Taehui, Analysis of State-of-the-Art Spin-Transfer-Torque Nonvolatile Flip-Flops Considering Restore Yield in the Near/Sub-Threshold Voltage Region, **Electronics**, v. 9, ed. 12, 2020, doi: 10.3390/electronics9122118

CHWIF, Leonardo, 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

CIECHANOWICZ, Zbigniew, Risk analysis: requirements, conflicts and problems. **Computers & Security**, v. 16, ed.3, p.223–232, 1997, doi:10.1016/s0167-4048(97)00004-7

CISCO, Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing, Disponível em < https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2017/m05/cisco-survey-reveals-close-to-three-fourths-of-iot-projects-are-failing.html>, acessado em: 16/05/2023

CHUNG-LEE, Lai, WEI, Whei-Jane. Action Research on Collaborative Design: A case study. **12th International Conference on Computer Supported Cooperative Work in Design**, 2008.

COCCIA, Rossana, TONTI, Veronica, GERMANO, Chiara, PALONE, Francesco, PAPI, Lorenzo, CELSI, Lorenzo Ricciardi. A Multi-Variable DTR Algorithm for the Estimation of Conductor Temperature and Ampacity on HV Overhead Lines by IoT Data Sensors. **ENERGIES**. v.15, ed. 7. 2022, doi: https://doi.org/10.3390/en15072581

CRESWELL, John W, CLARK, Vicki, Pesquisa de Métodos Mistos. Editora Penso, 2a ed, 2013

DARABI, Abdolreza; SALEHI, Mohammad Reza; ABIRI, Ebahim, Single-sided gate-wrap-around CNTFET SRAM cell for utilization in reliable IoT-based platforms. **AEU - International Journal of Electronics and Communications**. v. 163, 2023, doi: https://doi.org/10.1016/j.aeue.2023.154605

DONG Hu, TONG Sun, LIJIAN Yao, ZIDONG Yang, AICHEN Wang, Yibin Ying, Monte Carlo: A flexible and accurate technique for modeling light transport in food and agricultural products, **Trends in Food Science & Technology**, v. 102, 2020, doi: https://doi.org/10.1016/j.tifs.2020.05.006

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

ECARDT, Martina; KERBER, Wolfgang, Property rights theory, bundles of rights on IoT data, and the EU Data Act, **EUROPEAN JOURNAL OF LAW AND ECONOMICS**, v. 57, p.113-143, 2024, doi: 10.1007/s10657-023-09791-8

EL-GENDY, Sherif, ELSAYED, Mahmound Said, JURCUT, Anca, AZER, Marianne A, Privacy Preservation Using Machine Learning in the Internet of Things, **MATHEMATICS**, v.11, ed.16, 2023, doi:10.3390/math11163477

ELSAADANY, Amr; SOLIMAN, Mohamed, Experimental Evaluation of Internet of Things in the Educational Environment**. International Journal of Engineering Pedagogy**, v. 7 ed.3, p. 50-60, 2017 , doi:10.3991/ijep.v7i3.7187

ERAZO-GARZÓN, Lenin, CEDILLO,Priscila, ROSSI, Gustavo, MOYANO,Jose, A Domain-Specific Language for Modeling IoT System Architectures That Support

Monitoring, **IEEE Access**, v.10, p. 61639-61665, 2022, doi: 10.1109/ACCESS.2022.3181166

FAROOQ, Muhammad Shoaib, RIAZ, Shamyla, ABID, Adnan, ABID, Kamran, NAEEM, Muhammad Azhar, A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming, **IEEE Access**, v. 7, p. 156237-156271, 2019, doi: 10.1109/ACCESS.2019.2949703

FROSDICK, Steve, The techniques of risk analysis are insufficient in themselves. Disaster Prevention and Management: **An International Journal**. v. 6, ed. 3. p. 165 – 177, 1997.

FRUSTACI, Mario, PACE, Pasquale, ALOI, Gianluca, FORTINO, Giancarlo, Evaluating Critical Security Issues of the IoT World: Present and Future Challenges, **IEEE INTERNET OF THINGS JOURNAL**, v.5, p. 2483-2495, 2018, doi: 10.1109/JIOT.2017.2767291

FURFARO, Angelo ; ARGENTO, Luciano, PARISE, A ; Piccolo, A, Using virtual environments for the assessment of cyberseturity issues in IoT scenarios, **SIMULATION MODELLING PRACTICE AND THEORY**, v. 73, p. 43-54, 2017, doi: 10.1016/j.simpat.2016.09.007

CHRISTOPOULOS, Arthur, Assessing the distribution of parameters in models of ligand–receptor interaction: to log or not to log, **Trends in Pharmacological Sciences**, v. 19, ed 9, p. 351-357, 1998, doi: https://doi.org/10.1016/S0165-6147(98)01240-1

GEORGE, Gemini, THAMPI, Sabu M., A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations, **IEEE ACCESS**, v. 6, 2018, doi: 10.1109/ACCESS.2018.2863244

GREENGARD, S. The Internet of Things. **The MIT Press**, ISBN: 9780262527736, 2015

GYAMFI, Kojo Sarfo, BRUSEY James, GAURA Elena, WILKINS, Ross, Heartbeat design for energy-aware IoT: Are your sensors alive?, Expert Systems with Applications, v. 128, p. 124-139, 2019, doi: https://doi.org/10.1016/j.eswa.2019.03.022

HAMZA, R.; ZHENG Yan, MUHAMMAD, Khan, BELLAVISTA,Paolo, TITOUNA, Faiza, A privacy-preserving cryptosystem for IoT E-healthcare. **Information Sciences**, v. 527, p. 493-510, 2020, doi: 10.1016/j.ins.2019.01.070

HASAN, Mohammed Zaki, AL-TURJMAN, Fadi, SWARM-based data delivery in Social Internet of Things, **Future Generation Computer Systems-The International Journal Of Escience**, v. 92, p. 821-836, 2019, doi: 10.1016/j.future.2017.10.032

HASSOUN, Abdo, GARCIA-GARCIA,Guillermo, TROLLMAN, Hanna, JAGTAP, Sandeep, PARRA-LÓPEZ, Carlos, CROPOTOVA, Janna, BHAT, Zuhaib, CENTOBELLI, Piera, AÏT-KADDOUR, Abderrahmane, Birth of dairy 4.0: Opportunities and challenges in adoption of fourth industrial revolution technologies in the production of milk and its derivatives, **Current Research In Food Science** , v.7, 2023, doi: 10.1016/j.crfs.2023.100535

HECKERMAN, David, MAMDANI, Abe, WELLMAN, Michael P., Real-World Applications of Bayesian Networks. **Communications of the ACM**, 1995

HUANG, Mingeng; LIU, Anfeng; XIONG, Neal N., WANG, Tian, VASILAKOS, Athanasios V., An effective service-oriented networking management architecture for 5G-enabled internet of things. **Computer Networks**, v. 173, 2020, doi: 10.1016/j.comnet.2020.107208, doi: https://doi.org/10.1016/j.comnet.2020.107208

HUSEYIN, Yildirim; ALI-ELDIN, Amr M.T. A model for predicting user intention to use wearable IoT devices at the workplace. **Journal of King Saud University - Computer and Information Sciences**. v.31, ed. 4, p. 497-505, 2018, doi: https://doi.org/10.1016/j.jksuci.2018.03.001

IoT Analytics. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. disponível em < https://iot-analytics.com/number-connected-iot-devices/ >, acessado em: 05/12/2023

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

JAFRI, Syed Talib Abbas, AHMED, Irfan, ALI, Sundus, YAHAYA, Jamaiah, QAMAR, Faizan, ABDULLAH, Zuriani Hayati, Split Hop Penalty for Transmission Quality Metrics in a Better Approach to Mobile Ad Hoc Networking (BATMAN) for IoT-Based MANET, **SYMMETRY-BASEL**, v. 15, ed. 5, 2023, doi: https://doi.org/10.3390/sym15050969

KAKKAVAS, Anastasios, CASTAÑEDA GARCÍA, Mario, SECO-GRANADOS, Gonzalo, WYMEERSCH, Henk, STIRLING-GALLACHER, Richard, NOSSEK, Josef, Position Information From Reflecting Surfaces, **IEEE Wireless Communications Letters**, v. 10, ed. 6, p. 1300-1304, 2021, doi: 10.1109/LWC.2021.3064915

KANDASAMY, Kamalanathan, SRINIVAS, Srinivas, ACHUTHAN, Krishnashree, Rangan, Venkat P., IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process, **EURASIP JOURNAL ON INFORMATION SECURITY**, 2020, doi: 10.1186/s13635-020-00111-0

KARABACAK, Bilge, SOGUKPINAR, Ibrahim, ISRAM: information security risk analysis method, **Computers & Security**, v. 24, ed. 2, 2005, doi: https://doi.org/10.1016/j.cose.2004.07.004

KARUNARATHNE, Sivanarayani M., SAXENA, Neetesh, KHAN, Muhammad Khan, Security and Privacy in IoT Smart Healthcare, **IEEE INTERNET COMPUTING**, v.25, ed. 4, 2021, doi:10.1109/MIC.2021.3051675

KEMMERER, Richard A., Cybersecurity. **25th International Conference on Software Engineering, 2003**., 2003

KERZNER, Harold *et al*. **Gerenciamento de Projetos:** Uma abordagem sistêmica para planejamento, programação e controle. São Paulo. Editora Blucher, 2011.

KIRCHHOF, Jorg Christian, RUMPE, Bernhard, SCHMALZING, David, WORTMANN, Andreas, MontiThings: Model-Driven Development and Deployment of Reliable IoT Applications. **JOURNAL OF SYSTEMS AND SOFTWARE**, v.183, 2022, doi: 10.1016/j.jss.2021.111087

KITCHENHAM, Barbara, CHARTERS, Stuart M., Guidelines for performing systematic literature reviews in software engineering. **Technical Report – Department of Computer Science**. University of Durham, Durham, 2007

KINJO, Erika Midori, LIBRANTZ, André Felipe Henriques Librantz, SOUZA, Edson Melo, SANTOS, Fábio Cosme Rodrigues dos Santos, Modelagem Bayesiana aplicada para cálculo da probabilidade de falha em Sistemas de Saúde IoT. **RISTI**, Portugal, 2022, doi: 10.17013/risti.47.87–108

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

KÜHNER, Daniel, Internet der dinge telekommunikationsinfrastruktur. **Seminarband: Mobile und Verteilte Systeme-Ubiquitous Computing Teil IV**. Universität Karlsruhe-Fakultät für Informatik, p. 1–15, 2007.

KREJCÍ, J., STOKLASA, Jan, 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

LAHLOU, Saadi, Identity, social status, privacy and face-keeping in digital society, **Social Science Information Sur Les Sciences Sociales**, v. 47, ed.3. 2008, doi: 10.1177/0539018408092575

LI, Xang, PAK, Chanil, BI, Kexin, Analysis of the development trends and innovation characteristics of Internet of Things technology – based on patentometrics and bibliometrics. **Technology Analysis & Strategic Management**, v. 32, ed.1, 2019, doi:10.1080/09537325.2019.1636960

LIAO, Yongxin, DESCHAMPS, Fernando, ROCHA LOURES, Eduardo, RAMOS, Luiz Felipe Pierin, Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal. **International Journal of Production Research**, v. 55, ed. 12, p. 3609-3629, 2017, doi: 10.1080/00207543.2017.1308576

LIAO, Weixian, SALINAS, Sergio, LI, Ming, LI, Pan, LOPARO, Kenneth A., Cascading Failure Attacks in the Power System: A Stochastic Game Perspective, **IEEE**

INTERNET OF THINGS JOURNAL, v. 4, ed. 6, 2017, doi: 10.1109/JIOT.2017.2761353

LIBERATI Alessandro *et al*. **The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration**, Journal of Clinical Epidemiology, 2009

LIBRANTZ, André Felipe Henriques Librantz, COSTA, Ivanir, SPINOLA, Mauro de Mesquita, OLIVEIRA NETO, Geraldo Cardoso, ZERBINATTI, Leandro, Risk assessment in software supply chains using the Bayesian method. **International Journal of Production Research**, v. 59, ed. 22, p.6758-6775, 2021, doi: 10.1080/00207543.2020.1825860

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**, v. 19, ed. 21, 2019 , doi: 10.3390/s19214788

LIU, JianHua, TONG, Weiqin, Device service networks maintenance scheme in the internet of things, **PRZEGLAD ELEKTROTECHNICZNY**, v. 88, ed.9, p. 222-225, 2012

LOMOTEY Richard K., PRY Joseph, SRIRAMOJU, Sumanth, Wearable IoT data stream traceability in a distributed health information system. **Pervasive and Mobile Computing**, v. 40. p. 692-707, 2017, doi: 10.1016/j.pmcj.2017.06.020

LUO, Shiliang, CHENG, Lianglun, REN, Bin, Practical Swarm Optimization based Fault-Tolerance Algorithm for the Internet of Things**, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS**, v. 8, ed.4, p. 1178-1191, 2014, doi:10.3837/tiis.2014.04.001

MARTINS, Alaíde Barbosa, SANTOS, Celso Alberto Saibel, Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **Revista de Gestão e Tecnologia e Sistema de Informação**. v. 2, ed. 2, 2005

MEJJAOULI, Sobhi, Internet of Things based Decision Support System for Green Logistics. **Sustainability**. v. 14. ed. 22. 2022, doi: 10.3390/su142214756

MICROSOFT. IoT Signals, Disponível em < https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT-Signals-Microsoft-072019.pdf>, Acessado em: 16/05/2023

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

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

MIGLIORE, Marco Donald, World Beneath the Physical Layer: An Introduction to the Deep Physical Layer. **IEEE Access**, v.9, p. 77106 -77126, 2021

MUHAMMED, Thaha, MEHMOOD, Rashid, ALBESHRI, Aiiad, KATIB, Iyad, UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities, **IEEE ACCESS**, v.6, 2018

MURPHY, Kevin, A Brief Introduction to Graphical Models and Bayesian Networks. disponível em < https://www.cs.ubc.ca/~murphyk/Bayes/bnintro.html >, acessado em 18/03/2024, 1998

NAMAZIAN, Ali, YAKHCHALI, Siamak Haji, YOUSEFI, Vahidreza, TAMOŠAITIENE, Jolanta,Combining Monte Carlo Simulation and Bayesian Networks Methods for Ass essing Completion Time of Projects under Risk, **INTERNATIONAL JOURNAL OF ENVIRONMENTAL RESEARCH AND PUBLIC HEALTH**, v. 16, ed. 24, 2019, doi: 10.3390/ijerph16245024

NAYAK , Padmalaya, RAY, Niranjan, RAVICHANDRAN, P. **IoT Applications, Security Threats, and Countermeasures**. Editora CRC Press, 2022

NTAFLOUKAS, Konstantinos, McCrum, D.P. ; Pasquale, L., A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure, **APPLIED SCIENCES-BASEL**, v. 12, ed. 18, 2022, doi:10.3390/app12189241

NIETO-MOROTE, Ana, RUZ-VILA, Francisco De Asís, A fuzzy approach to construction project risk assessment. **International Journal of Project Management.** v. 29. ed.2. p.220- 231, 2011, doi: 10.1016/j.ijproman.2010.02.002

NIKOUI, Tina Samizadeh, RAHMANI, Amir Masoud, BALADOR Ali, JAVADI, Hamid Haj Seyyed, Internet of Things architecture challenges: A systematic review. **INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS**, v. 34, ed.4. 2021. doi: https://doi.org/10.1002/dac.4678

NIŽETIĆ, Sandro, ŠOLIĆ, Petar, LÓPEZ-DE-IPIÑA GONZÁLEZ-DE-ARTAZA, Diego, PATRONO, Luigi, Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future**. *Journal of Cleaner Production***, v. 274, 2020, doi: 10.1016/j.jclepro.2020.122877

PACHECO, Luis Alberto Belem, ALCHIERI, Eduardo Adilio Pelinson Alchieri, BARRETO, Priscila América Solis Mendez, Device-Based Security to Improve User Privacy in the Internet of Things, **SENSORS**, v.18, ed. 8, 2018, doi:10.3390/s18082664

PACHECO, Jesus, BENITEZ BALTAZAR, Victor Hugo, FÉLIX-HERRÁN, Luis Carlos, SATAM, Pratik, Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes, **IEEE ACCESS**, v. 8, 2020, doi:10.1109/ACCESS.2020.2988055

PACHECO, Jesus, HARIRI, Salim, Anomaly behavior analysis for IoT sensors, **TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES**, v.29, ed. 4, 2018, doi:10.1002/ett.3188

PALATTELLA, Maria Rita, ACCETTURA, Nicola, VILAJOSANA, Xavier, WATTEYNE, Thomas, GRIECO, Luigi Alfredo, BOGGIA, Gennaro, DOHLER, Mischa, Standardized Protocol Stack for the Internet of (Important) Things, **IEEE Communications Surveys & Tutorials**, v. 15, ed. 3, p. 1389-1406, 2013, doi: 10.1109/SURV.2012.111412.00158

PATTERSON, Randolph E., HOROWITZ, Steven, 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**, 1984.

PRAKASAM, Periasamy, MADHESWARAN M., SUJITH K.P., SAYEED , MD Shohel. An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices, **ICT Express**, v. 7, ed. 4, p. 487-492, 2021, doi: 10.1016/j.icte.2021.03.007

RADANLIEV, Petar, DE ROURE, David, Epistemological and Bibliometric Analysis of Ethics and Shared Responsibility-Health Policy and IoT Systems; **SUSTAINABILITY**; v. 13, ed.15, 2021, doi: 10.3390/su13158355

REN, Ju, GUO, Hui, XU, Chugui, ZHANG, Yaoxue, Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing, **IEEE NETWORK**, v. 31, ed.5, p.96-105, 2017, doi: 10.1109/MNET.2017.1700030

ROBERT, Christian, CASELLA, George, Monte Carlo Statistical Method, 2nd Edition. Springer, 2004

ROBINSON, Stewart, Conceptual modelling for simulation Part I: definition and requirements. **Journal Of The Operational Research Society**. v. 59, ed. 3. p. 278 – 290, 2008, doi: 10.1057/palgrave.jors.2602368

SAHI, Muneeb Ahmed, ABBAS, Haider, SALEEM, Kashif, YANG, Xiaodong, DERHAB, Abdelouahid, ORGUN, Mehmet A. ; IQBAL, Waseem, RASHID, Imran, Yaseen, Asif, Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions, **IEEE ACCESS**, v.6, p. 464-478, 2018, doi: 10.1109/ACCESS.2017.2767561

SALAGARE, Smita, PRASAD, Ramjee, An Overview of Internet of Dental Things: New Frontier in Advanced Dentistry. Wireless Personal Communications , v. 110, p. 1345-1371, 2020, doi: 10.1007/s11277-019-06790-4

SANTOS, Lidiane, SILVA, Eduardo, BATISTA, Thais, CAVALCANTE, Everton, LEITE, Jair, An Architectural Style for Internet of Things Systems, Proceedings of the 35th Annual ACM Symposium on Applied Computing, p. 1488–1497, 2020, doi: 10.1145/3341105.3374030

SATAM, Shalaka, SATAM, Pratik, PACHECO, Jesus, HARIRI, Salim, Security framework for smart cyber infrastructure, **CLUSTER COMPUTING-THE JOURNAL**

OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS, v.25, p. 2767-2778, 2022, doi:10.1007/s10586-021-03482-2

SARWAR, Kinza, YONGCHAREON, Sira, YU, Jian, REHMAN, Saeed Ur, A Survey on Privacy Preservation in Fog-Enabled Internet of Things, **ACM COMPUTING SURVEYS**, v.55, ed.1, 2023, doi:10.1145/3474554

SCHOENBERGER, Chana, UPBIN, Bruce, The Internet of Things, **Forbes Magazine**, v.169, p. 155–160, 2002

SHA, Kewei, YANG, T.Andrew, WEI, Wei, DAVARI, Sadegh, A survey of edge computing-based designs for IoT security, **DIGITAL COMMUNICATIONS AND NETWORKS**, v.6, ed.2, p. 195-202, 2020, doi:10.1016/j.dcan.2019.08.006

SHARMA, Shachi, BHATT, Prakash Datt, Performance Analysis of Gamma/M/1 Model for IoT-Based Sensor Data Traffic. **IEEE WIRELESS COMMUNICATIONS LETTERS**. v.10 ed. 11, 2021, doi: 10.1109/LWC.2021.3102322

SHARMA, Sagar, CHEN Keke, SHETH Amit, Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. **IEEE Internet Computing**, v. 22, ed. 2, p.42-51, 2018, doi; 10.1109/MIC.2018.112102519

SNOPKOWSKI, Ryszard, SUKIENNIK, Marta, NAPIERAJ, Aneta, Stochastic Simulation of Production Processes - Selected Issues, **INZYNIERIA MINERALNA-JOURNAL OF THE POLISH MINERAL ENGINEERING SOCIETY**, v.1, ed.1, p.137-146, 2021, doi: 10.29227/IM-2021-01-18

SOLAIMAN, Ellis, RANJAN, Rajic, JAYARAMAN, Prem Prakash, Mitra, Karan, Monitoring Internet of Things Application Ecosystems for Failure, **IT PROFESSIONAL**, v. 18, ed.5, p. 8-11, 2016, doi:10.1109/MITP.2016.90

SOKOLOWSKI, John A., BANKS, Catherine M., Principles of Modeling and Simulation, **John Wiley & Sons**, 2009, doi:10.1002/9780470403563

SOOD, Sandeep K., MAHAJAN Isha, Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus, **Computers in Industry**, v.91, p.33-44, 2017, doi: 10.1016/j.compind.2017.05.006

SUNG, Chun-Hsien, LU, Ming-Chin, Protection of personal privacy under the development of the Internet of Things, **WIRELESS NETWORKS**, 2023, doi: 10.1007/s11276-023-03569-1

TAHSIEN, Syeda Manjia, KARIMIPOUR, Hadis, SPACHOS, Petros, Machine learning based solutions for security of Internet of Things (IoT): A survey, **Journal of Network and Computer Applications**, v.161, 2020, doi:10.1016/j.jnca.2020.102630

TAO, Ming, ZUO, Jinglong, LIU, Zhusong, CASTIGLIONE, Aniello, PALMIERI, Francesco, Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. **FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE**, v. 78, p. 1040-1051, 2018

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

TRAN-DANG, Hoa, KROMMENACKER, Nicolas, CHARPENTIER, Patrick, KIM, Dong-Seong, Toward the Internet of Things for Physical Internet: Perspectives and Challenges. **IEEE Internet of Things Journal**, v.7, ed.6, p. 4711-4736, jun. 2020. DOI: 10.1109/JIOT.2020.2971736.

QINGPING Shi, JIAN Kang, RONG Wang, HANG Yi, YUN Lin, JIE Wang, A Framework of Intrusion Detection System based on Bayesian Network in IoT, **International Journal of Performability Engineering**, v.14, ed.10, 2018, doi: 10.23940/ijpe.18.10.p4.22802288

LIU, Qinming, DONG, Ming, PENG, Ying, A novel method for online health prognosis of equipment based on hidden semi-Markov model using sequential Monte Carlo methods, **Mechanical Systems and Signal Processing**, v. 32, p. 331-348, 2012, doi: 10.1016/j.ymssp.2012.05.004

QIU, Robin, ZHANG, Zhang, Design of Enterprise Web Servers in Support of Instant Information Retrievals, **Proceedings of the IEEE International Conference on Systems, Man and Cybernetics**, p. 2661–2666, 2003, doi: 10.1109/ICSMC.2003.1244286

VALDIVIA, Einar Jhordany Serna, MIRANDA, Jezreel Mejiá, Proposal of a Intelligent Agent for Management and Mitigation in Cibersecurity Risk for IoT Environments**.**,**2020 9TH INTERNATIONAL CONFERENCE ON SOFTWARE PROCESS IMPROVEMENT (CIMPS)**, p-148-154.2020, doi:10.1109/CIMPS52057.2020.9390114

VIBHUTE, Deepa S., GUNDALE, Ajit S. Early, Detection of Sensors Failure using IoT **International Research Journal of Engineering and Technology (IRJET)** . v. 6, ed. 5, 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, Ling, Environment supervision system for chemical industry park based on IOT. **Chemical Engineering Transactions**, v. 67, 2018, doi: 10.3303/CET1867081

WEBER, Philippe, MEDINA-OLIVA, Gabriela, SIMON, Christophe, IUNG, Benoît, Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. **Engineering Applications of Artificial Intelligence**, v.25, ed. 4, p 671-682, 2012 , doi: 10.1016/j.engappai.2010.06.002

WILLERS, Oliver, HUTH, Christopher, GUAJARDO, Jorge, SEIDEL, Helmut, MEMS Gyroscopes as Physical Unclonable Functions. **CCS'16: PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY**. 2016, doi: 10.1145/2976749.2978295

WINSTON, Wayne L., Decision making under uncertainty with RISK Optimizer: a step-by-step with Microsoft Excel and Palisade's RISK Optimizer software. **Palisade Corporation**, 2000

XAVIER, Carlos Magno *et al*. **Metodologia de Gerenciamento de Projetos**: Methodware: Abordagem prática de como iniciar, planejar, executar, controlar e fechar projetos. 2ª edição. Rio de Janeiro. Editora Brasport, 2009.

YAQOOB, Ibrar, AHMED, Ejaz, HASHEM, Ibrahim Abaker, AHMED, Abdelmuttlib Ibrahim Abdalla, GANI, Abdullah,IMRAN, Muhammad, GUIZAN, Mohsen, Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. **IEEE Wireless Communications**, v. 24, ed. 3, 2017, doi: 10.1109/MWC.2017.1600421

ZAGORECKI, Adam, DRUZDZEL, Marek J., Knowledge Engineering for Bayesian Networks: How Common Are Noisy-MAX Distributions in Practice?. **IEEE TRANSACTIONS ON SYSTEMS MAN CYBERNETICS-SYSTEMS**, v.43, ed. 1, p.186-195, 2013 , doi: 10.1109/TSMCA.2012.2189880

ZHANG, Haibin, ZHANG, Qian, LIU, Jiajia, GUO, Hongzhi. Fault Detection and Repairing for Intelligent Connected Vehicles Based on Dynamic Bayesian Network Model. **IEEE INTERNET OF THINGS JOURNAL**.v 5. ed 4, 2018, doi: 10.1109/JIOT.2018.2844287

ZHANG, Ningbo, ZHU, Xuzhen, A Hybrid Grant NOMA Random Access for Massive MTC Service. **IEEE INTERNET OF THINGS JOURNAL**, v.10, ed.6, 2023, doi: 10.1109/JIOT.2022.3222622

ZHANG, Qi, Artistic expression and data protection: Balancing aesthetics with data privacy in IoT, **HELIYON**, v.9, ed. 9, 2023, doi:10.1016/j.heliyon.2023.e19380

ZIO, Enrico, Challenges in the vulnerability and risk analysis of critical infrastructures. **RELIABILITY ENGINEERING & SYSTEM SAFETY**. v. 152, p.137-150, 2016 , doi: 10.1016/j.ress.2016.02.009

APÊNDICES

APÊNDICE A: FORMULÁRIO

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.

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)? *

Fator	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
	Interação social através da distância geográfica,	

	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/ S...	○	○	○	○	○
Gateway	○	○	○	○	○
Algoritmo	○	○	○	○	○
Protocolo	○	○	○	○	○
Provedor de S...	○	○	○	○	○
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/ S...	○	○	○	○	○
Gateway	○	○	○	○	○
Algoritmo	○	○	○	○	○
Protocolo	○	○	○	○	○
Provedor de S...	○	○	○	○	○
Processamento	○	○	○	○	○
Social	○	○	○	○	○
Aplicação	○	○	○	○	○

Há sugestão de outros componentes

Texto de resposta longa

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)? *

Fator	Subfator	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	

	Pouco relevante	Médio	Muito relevante
Quantidade (Dispositiv...	○	○	○
Parâmetro (Dispositivo...	○	○	○
Tipo (Dispositivos/ Sen...	○	○	○
Modelo (Dispositivos/ ...	○	○	○
Tipo (Gateway)	○	○	○
Quantidade (Algoritmo)	○	○	○
Objetivo (Algoritmo)	○	○	○
Linguagem (Algoritmo)	○	○	○
Configuração (Protocolo)	○	○	○

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 (Di...	○	○	○	○	○
Parâmetro (Di...	○	○	○	○	○
Tipo (Dispositi...	○	○	○	○	○
Modelo (Dispo...	○	○	○	○	○
Tipo (Gateway)	○	○	○	○	○
Quantidade (Al...	○	○	○	○	○
Objetivo (Algor...	○	○	○	○	○
Linguagem (Al...	○	○	○	○	○

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 (Di...	○	○	○	○	○
Parâmetro (Di...	○	○	○	○	○
Tipo (Dispositi...	○	○	○	○	○
Modelo (Dispo...	○	○	○	○	○
Tipo (Gateway)	○	○	○	○	○
Quantidade (Al...	○	○	○	○	○
Objetivo (Algor...	○	○	○	○	○
Linguagem (Al...	○	○	○	○	○
Configuração (...	○	○	○	○	○

Há sugestão de outros subcomponentes?

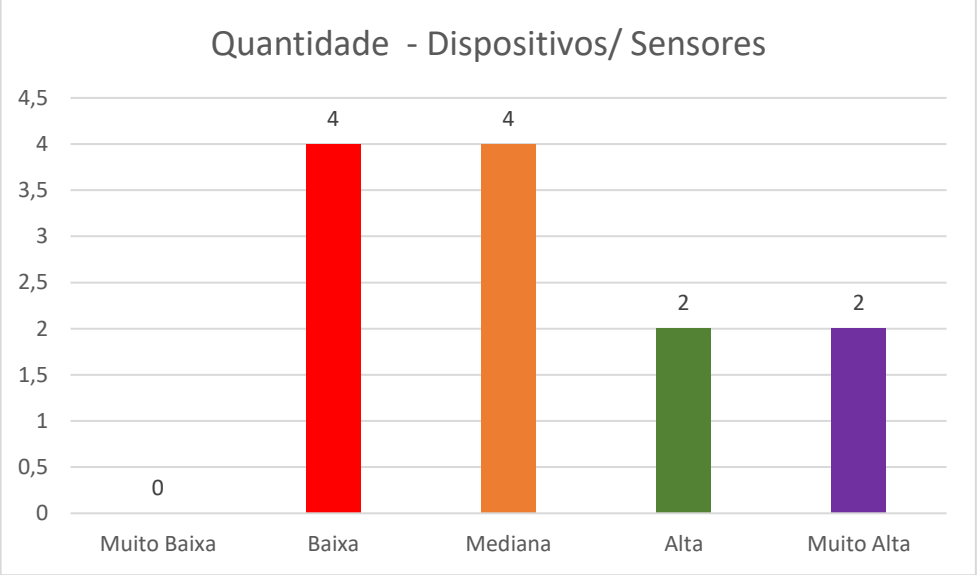
Texto de resposta longa

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

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

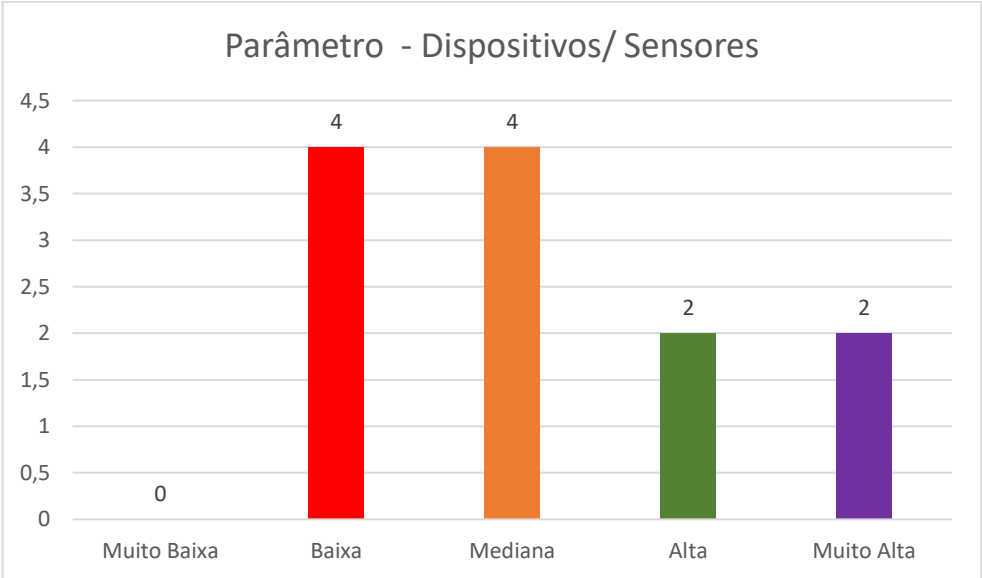
APÊNDICE B: PROBABILIDADE DE FALHAR

Figura B-1 - Probabilidade de Falha – Subcomponente Quantidade (do Dispositivo/ Sensor)



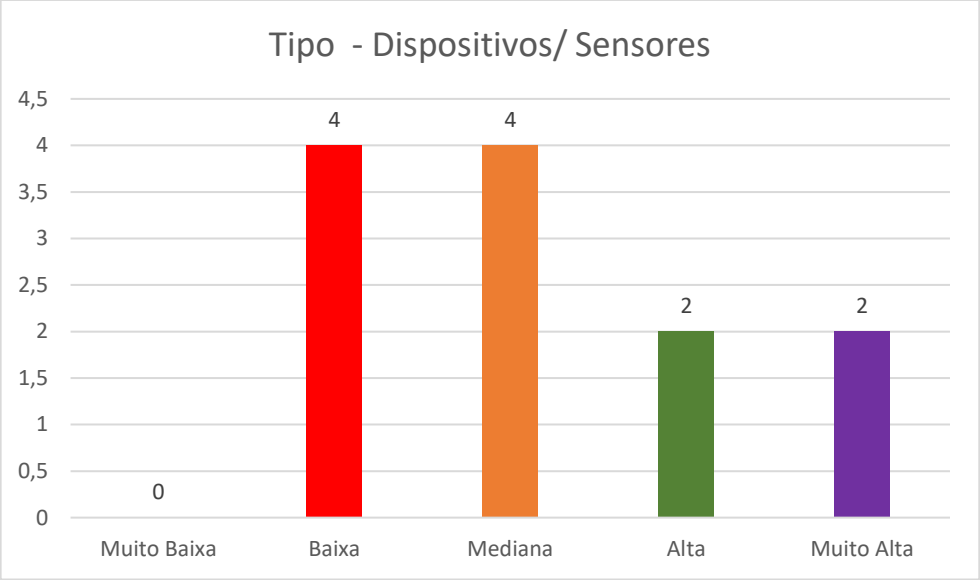
Fonte: adaptado pelo autor

Figura B-2 - Probabilidade de Falha – Subcomponente Parâmetro (do Dispositivo/ Sensor)



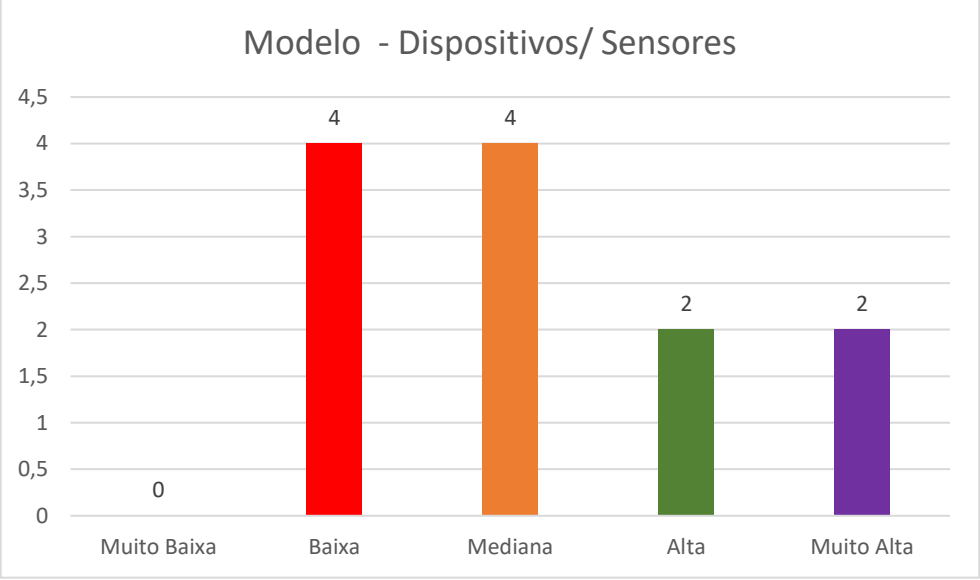
Fonte: Adaptado pelo autor

Figura D-3 - Probabilidade de Falha – Subcomponente Tipo (do Dispositivo/ Sensor)



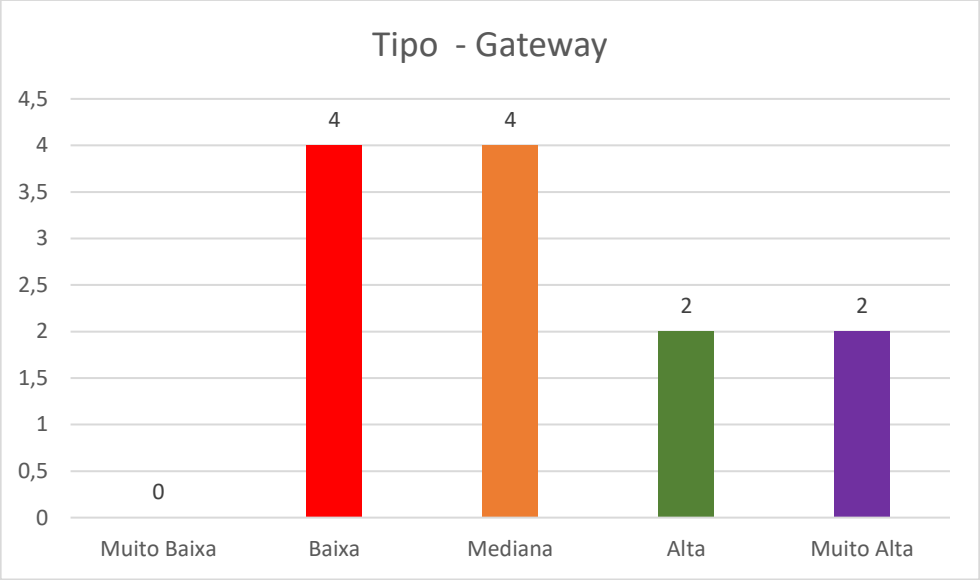
Fonte: Adaptado pelo autor

Figura B-4 - Probabilidade de Falha – Subcomponente Modelo (do Dispositivo/ Sensor)



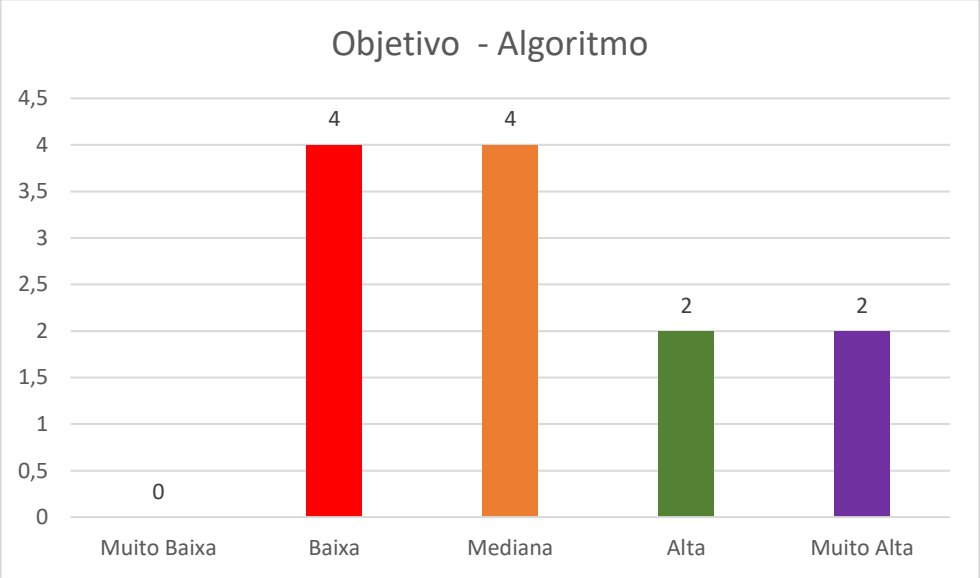
Fonte: Adaptado pelo autor

Figura B-5 - Probabilidade de Falha – Subcomponente Tipo (do Gateway)



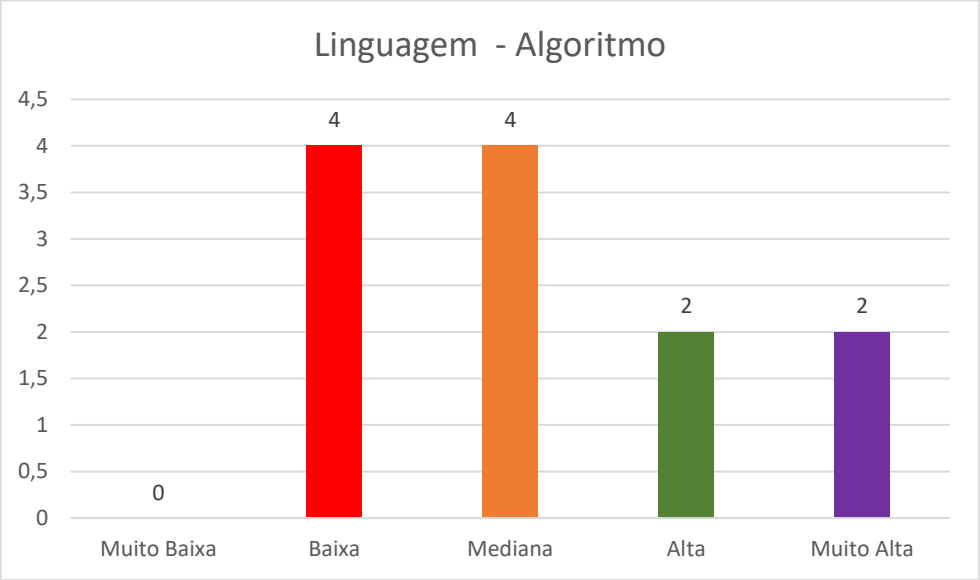
Fonte: Adaptado pelo autor

Figura B-6 - Probabilidade de Falha – Subcomponente Quantidade (do Algoritmo)



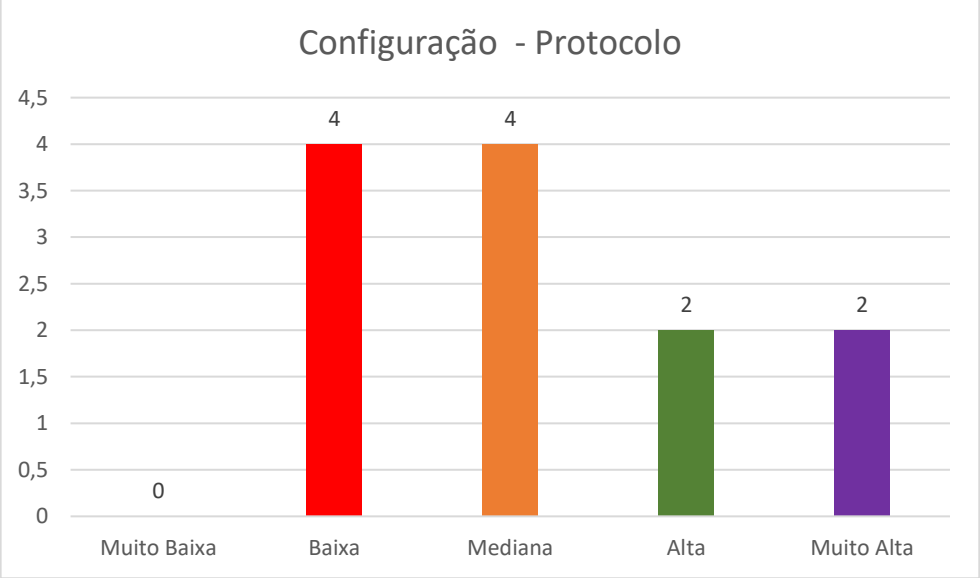
Fonte: Adaptado pelo autor

Figura B-7 - Probabilidade de Falha – Subcomponente Linguagem (do Algoritmo)



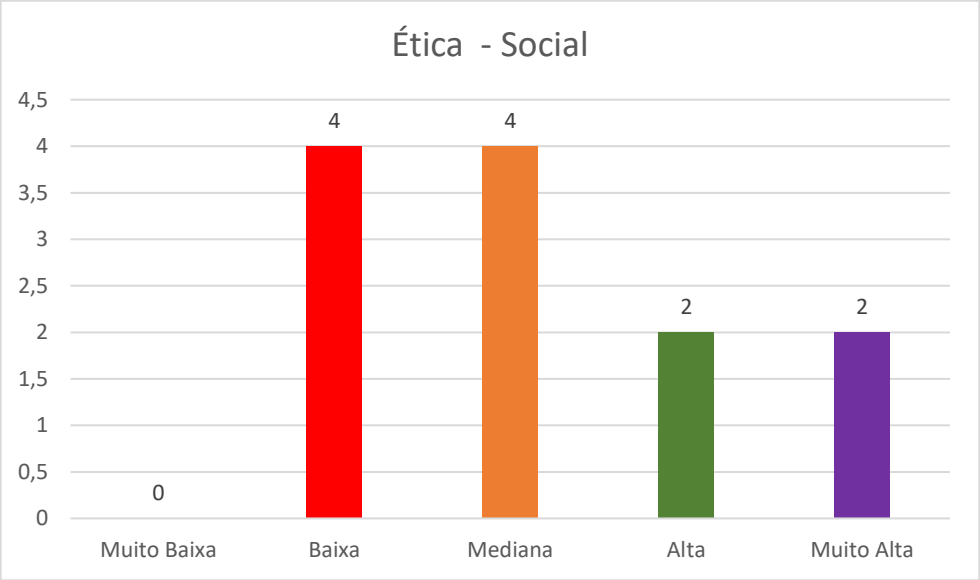
Fonte: Adaptado pelo autor

Figura B-8 - Probabilidade de Falha – Subcomponente Configuração (do Protocolo)



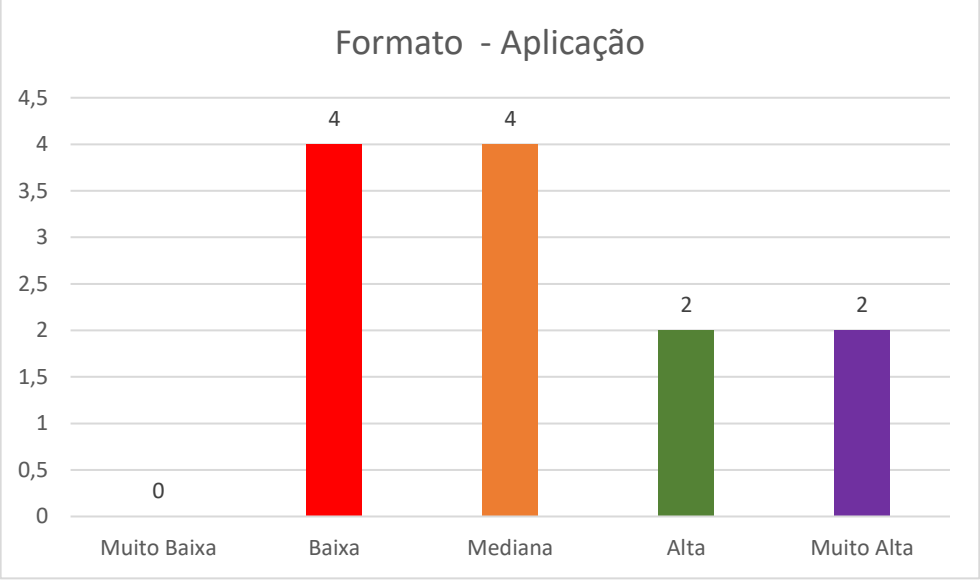
Fonte: Adaptado pelo autor

Figura B-9 - Probabilidade de Falha – Subcomponente Ética (do Social)



Fonte: Adaptado pelo autor

Figura B-10 - Probabilidade de Falha – Subcomponente Formato (da Aplicação)



Fonte: Adaptado pelo autor