



*Um Framework para Mensuração da  
Maturidade de Requisitos de Sistemas em IoT*  
**Luis Fernando dos Santos Pires**  
Setembro/ 2025

Dissertação de Mestrado em Ciência da  
Computação

# **Um *Framework* para Mensuração da Maturidade de Requisitos de Sistemas em IoT**

Esse documento corresponde a Dissertação apresentada a Banca Examinadora no curso de Mestrado Profissional em Ciências da Computação da UNIFACCAMP - Centro Universitário Campo Limpo Paulista

Campo Limpo Paulista, 09 de setembro de 2025.

Luis Fernando dos Santos Pires

Prof. Dr. Rodrigo Bonacin (Orientador)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

**Ficha catalográfica elaborada pela  
Biblioteca Central da Unifaccamp**

P744F

Pires, Luis Fernando dos Santos

Um *framework* para mensuração da maturidade de requisitos de sistemas em IoT / Luis Fernando dos Santos Pires. Campo Limpo Paulista, SP: Unifaccamp, 2025.  
155 f.

Orientador: Prof. Dr. Rodrigo Bonacin

Dissertação (Programa de Mestrado Profissional em Ciência da Computação) – Centro Universitário Campo Limpo Paulista – Unifaccamp.

1. Internet das coisas (IoT). 2. Engenharia de requisitos. 3. Maturidade dos requisitos. I. Bonacin, Rodrigo. II. Centro Universitário Campo Limpo Paulista. III. Título.

CDD – 005.75

## **AGRADECIMENTO**

Em primeiro lugar, agradeço a Deus, que me sustentou com força, sabedoria e fé durante toda essa caminhada. Sem Sua presença constante em minha vida, este momento não seria possível.

À minha esposa Letícia, meu amor e parceira de vida, agradeço por toda paciência, compreensão e apoio em cada etapa deste percurso. Sua presença foi essencial para que eu mantivesse o equilíbrio e a motivação.

Aos meus filhos, Antonio e Joaquim, que são meu maior orgulho e fonte diária de inspiração. Que esta conquista sirva como exemplo de que, com dedicação e esforço, somos capazes de realizar grandes sonhos.

À minha mãe, Auristela, e ao meu pai, George, agradeço profundamente pelo amor, educação e valores que sempre me transmitiram.

Um agradecimento muito especial à minha sogra, Aparecida (in memoriam), que foi minha maior incentivadora. Sua confiança em meu potencial, suas palavras de encorajamento e seu apoio incondicional me acompanharam em todos os momentos desta jornada. Sua ausência física não apagou a força da sua presença em minha vida e em cada conquista que alcanço.

Agradeço também à minha tia Cristina e ao meu tio Paulino pelo carinho, apoio e pelas palavras de incentivo que, em diferentes momentos, me fortaleceram e me motivaram a seguir em frente.

Ao meu orientador, Prof. Rodrigo Bonacin, expresso minha sincera gratidão pela orientação dedicada, pelas valiosas contribuições acadêmicas e pelo incentivo constante para o aprimoramento deste trabalho.

Agradeço também ao Centro Universitário Campo Limpo Paulista – UNIFACCAMP, por toda a formação recebida, pelo corpo docente qualificado e pela estrutura que me permitiu crescer intelectual e profissionalmente.

Por fim, aos amigos, colegas e a todos que, de alguma forma, fizeram parte desta trajetória, deixo meu muito obrigado. Cada palavra de incentivo e cada gesto de apoio tiveram um papel importante para que este sonho se tornasse realidade.

**Resumo:** A Internet das Coisas (IoT) transformou a interação com o mundo físico, conectando dispositivos e gerando grandes volumes de dados. No entanto, o desenvolvimento eficaz de sistemas IoT exige um rigoroso processo de engenharia de requisitos devido à crescente complexidade, heterogeneidade dos dispositivos e importância dos dados coletados. A ausência de frameworks para mensurar a maturidade dos requisitos em sistemas IoT é um desafio significativo, podendo resultar em sistemas falhos, altos custos e riscos à segurança. Este trabalho propõe um novo framework para avaliar a maturidade dos requisitos em sistemas IoT, ajudando desenvolvedores a criar soluções mais robustas e alinhadas às necessidades. A pesquisa inclui uma revisão da literatura, definição do framework, seleção de um caso de estudo e aplicação do framework para validação dos requisitos, apoiada por um software desenvolvido para executar seu funcionamento. O framework abrange etapas como identificação da necessidade, coleta de dados, levantamento e validação de requisitos, e determinação do nível de maturidade. Como contribuição, espera-se que a proposta melhore a qualidade dos sistemas IoT, reduza custos de desenvolvimento, aumente a segurança e a satisfação do usuário, além de orientar futuras pesquisas na área.

**Palavras-Chave:** Internet das Coisas (IoT); Engenharia de Requisitos; Maturidade dos Requisitos; Framework; Validação de Requisitos; Segurança.

**Abstract:** The Internet of Things (IoT) has transformed the interaction with the physical world by connecting devices and generating large volumes of data. However, the effective development of IoT systems requires a rigorous requirements engineering process due to the increasing complexity, device heterogeneity, and the importance of the collected data. The lack of frameworks to measure requirements maturity in IoT systems is a significant challenge, potentially leading to flawed systems, high costs, and security risks. This work proposes a new framework to assess requirements maturity in IoT systems, helping developers create more robust solutions aligned with real needs. The research includes a literature review, framework definition, selection of a case study, and application of the framework for requirements validation, supported by software developed to execute its functioning. The framework encompasses stages such as needs identification, data collection, requirements elicitation and validation, and determination of maturity level. As a contribution, the proposal is expected to improve IoT system quality, reduce development costs, increase security and user satisfaction, and guide future research in the area.

**Keywords:** Internet of Things (IoT); Requirements Engineering; Requirements Maturity; Framework; Requirements Validation; Security.

## Sumário

1. Introdução .....	1
1.1 Contexto, Motivação e Justificativa.....	2
1.2 Objetivos, Contribuições e Métodos.....	6
1.3 Estrutura da Proposta .....	8
1.4 Conclusão do Capítulo.....	11
2. Referencial Teórico e Metodológico .....	12
2.1 Internet das Coisas .....	12
2.2 Engenharia de Requisitos para IoT .....	15
2.3 Qualidade de Software para IoT .....	16
2.4 Técnicas de Avaliação e Mensuração de Requisitos para IoT.....	16
2.5 Conclusão do Capítulo.....	20
3. Revisão da Literatura e Trabalhos Relacionados.....	21
3.1 Metodologia de Revisão .....	21
3.2 Resultados e Análise dos Artigos .....	24
3.2.1 Análise sobre engenharia de requisito em IoT .....	24
3.2.2 Análise sobre Qualidade de Software em IoT .....	27
3.2.3 Discussão Sobre a Revisão da Literatura.....	29
3.3 Trabalhos Relacionados.....	33
3.3.1 Frameworks de Avaliação em IoT .....	33
3.3.2 Análise Crítica dos <i>Frameworks</i> em Relação ao <i>QualIoT</i> .....	35
3.4 Diferenciais de Pesquisa .....	37
3.5 Proposta Metodológica da Pesquisa .....	38
3.6 Conclusão do Capítulo.....	40
4. O <i>Framework QualIoT</i> : Proposta e Estrutura.....	41

4.1 Elaboração do <i>Framework QualIoT</i> .....	41
4.2 Estrutura Conceitual do <i>Framework QualIoT</i> .....	42
4.3. Estrutura Detalhada do <i>Framework QualIoT</i> .....	44
4.3.1 Fluxo Estruturado do <i>Framework</i> .....	47
4.3.2 Perguntas Norteadoras .....	49
4.3.3 Ranking baseados em Requisitos para IoT .....	53
4.3.4 Pontuação por Categoria .....	56
4.3.5 Cálculo do Índice de Maturidade.....	57
4.7 Conclusão do Capítulo.....	60
5. Software <i>QualIoT</i> .....	61
5.1 Arquitetura Técnica .....	62
5.2 Contexto de Software .....	64
5.3 Sitemap .....	65
5.4 Fluxograma Funcional .....	66
5.5 Fluxo BPMN.....	68
5.6 Arquitetura Funcional .....	69
5.7 Diagrama de Caso de Uso.....	70
5.8 Conclusão do Capítulo.....	84
6. Estudo de Caso .....	85
6.1 Critérios de Seleção .....	86
6.2 <i>Briefing</i> .....	87
6.2.1 Pré-avaliação e divisão do grupo de pesquisa. ....	87
6.2.2 Questionário de Pré-Avaliação .....	89
6.2.3 Atribuição de Pesos e Classificação .....	90
6.2.4 Divisão dos Grupos.....	91

6.3 Ambiente de Pesquisa.....	92
6.4 Coleta de Dados .....	93
6.5 <i>Debriefing</i> .....	97
6.6 Procedimentos Éticos na Coleta de Dados .....	99
6.7 Conclusão do Capítulo.....	100
7. Análise dos Resultados e Discussão .....	102
7.1 Análise Quantitativa dos Resultados .....	102
7.1.1 Análises de Discrepâncias .....	104
7.1.2 Coeficiente Kappa .....	106
7.1.3 Resultados por Categoria de IoT .....	108
7.2 Avaliação por Equipamento .....	110
7.2.1 IoT Básico.....	110
7.2.2 IoT Intermediários .....	112
7.2.3 IoTs Avançados .....	114
7.3 Síntese do Resultado Individual .....	117
7.4 Distribuição de Pontuações.....	118
7.4.1 Desvio Padrão .....	119
7.4.2 Intervalo de Confiança.....	119
7.4.3 Testes Estatísticos.....	121
7.5 Resultados do <i>Debriefing</i> .....	123
7.5.1 Experiência Geral e Desafios.....	123
7.5.2 Resultados Quantitativos .....	125
7.5.3 Recomendação para Projetos Futuros.....	126
7.5.4 Insights Qualitativos e Sugestões de Melhoria.....	127
7.6 Validação do <i>Framework</i> .....	127

7.7 Comparação com <i>Frameworks</i> .....	129
7.8 Conclusão do Capítulo.....	131
8. Conclusão .....	133
8.1 Limitações da Pesquisa.....	133
8.2 Considerações Finais .....	134
Referências .....	136

## Glossário

1. Análise de Dados – Processo de examinar dados para obter informações relevantes.
2. API (Application Programming Interface) – Interface que permite a comunicação entre diferentes sistemas.
3. Arquitetura de Sistemas – Organização dos componentes estruturais de um sistema.
4. Arquitetura Orientada a Serviços (SOA) – Modelo que permite que sistemas forneçam serviços a outros.
5. Automação – Uso de tecnologia para executar tarefas com mínima intervenção humana.
6. Big Data – Análise de grandes volumes de dados com velocidade e variedade.
7. Cloud Computing – Armazenamento e processamento de dados em servidores remotos.
8. Conexão Machine-to-Machine (M2M) – Comunicação automática entre dispositivos sem interferência humana.
9. Confiabilidade – Capacidade de um sistema operar de forma consistente sem falhas.
10. Critérios de Avaliação – Parâmetros utilizados para medir desempenho ou qualidade.
11. Ciclo de Vida de Sistemas – Etapas de desenvolvimento, operação e manutenção de sistemas.
12. Dashboards – Interfaces visuais para apresentação e monitoramento de dados.
13. Desempenho do Sistema – Eficiência e velocidade com que um sistema executa suas funções.
14. Dimensionamento – Processo de organização dos dados ou critérios para facilitar a análise.
15. Dispositivos Embarcados – Componentes físicos com software integrado para funções específicas.
16. Edge Computing – Processamento de dados realizado próximo à fonte de geração.

17. Eficiência Energética – Capacidade de um dispositivo utilizar menos energia para realizar tarefas.
18. Engenharia de Requisitos – Processo de identificação, análise e gestão de requisitos de sistemas.
19. Escalabilidade – Capacidade do sistema de se adaptar a diferentes volumes de demanda.
20. Framework – Estrutura ou modelo conceitual para guiar processos técnicos.
21. Inteligência Artificial (IA) – Sistemas que simulam a inteligência humana para tomar decisões.
22. Interoperabilidade – Capacidade de diferentes sistemas operarem em conjunto.
23. Internet das Coisas (IoT) – Rede de objetos conectados capazes de coletar, processar e trocar dados.
24. Privacidade e Segurança – Proteção contra acessos não autorizados a informações sensíveis.
25. Rede 5G – Quinta geração de redes móveis com maior velocidade e baixa latência.
26. Redes de Comunicação – Infraestrutura que permite a troca de dados entre dispositivos.
27. Requisitos Funcionais – Descrevem o que um sistema deve fazer (funções esperadas).
28. Requisitos Não Funcionais – Características desejadas como desempenho, segurança e usabilidade.
29. Segurança Cibernética – Proteção de dados e sistemas contra ameaças digitais.
30. Sensores IoT – Dispositivos que coletam informações do ambiente físico.
31. Stakeholders – Partes interessadas no sistema, como usuários, desenvolvedores e investidores.
32. Transmissão de Dados – Envio e recepção de informações entre dispositivos.

## **Lista de Tabelas**

Tabela 1 – Resumo sobre as Motivações do Projeto .....	p. 04
Tabela 2 – Critérios de Inclusão e Exclusão de Artigos .....	p. 22
Tabela 3 – Dimensões da Engenharia de Requisitos para IoT .....	p. 23
Tabela 4 – Dimensões da Qualidade de Software para IoT .....	p. 27
Tabela 5 – Melhorias Baseadas em Eng. Requisitos e Qualidade de Software .....	p. 29
Tabela 6 – Síntese dos Trabalhos Relacionados .....	p. 31
Tabela 7 – Síntese dos Trabalhos Analisados .....	p. 32
Tabela 8 – Características dos Trabalhos Selecionados .....	p. 35
Tabela 9 – Síntese sobre os Diferenciais da Pesquisa .....	p. 38
Tabela 10 – Proposta de Metodologia de Pesquisa .....	p. 39
Tabela 11 – Disposição das Perguntas Norteadoras .....	p. 49
Tabela 12 – Ranking para Requisitos IoT .....	p. 56
Tabela 13 – Níveis de Maturidade em IoT .....	p. 59
Tabela 14 – Questionário de Pré-Avaliação .....	p. 90
Tabela 15 – Classificação de Pontuação .....	p. 91
Tabela 16 – Comparativo Geral por Dimensão e Categoria .....	p. 103
Tabela 17 – Matriz de Contingência .....	p. 107
Tabela 18 – Síntese dos Resultados .....	p. 109
Tabela 19 – Resultado Individual – Campainha Inteligente .....	p. 110
Tabela 20 – Resultado Individual – Relógio .....	p. 111
Tabela 21 – Resultado Individual – Câmera .....	p. 112
Tabela 22 – Resultado Individual – Robô Aspirador .....	p. 113
Tabela 23 – Resultado Individual – Assistente Virtual .....	p. 114
Tabela 24 – Resultado Individual – Drone .....	p. 115
Tabela 25 – Desempenho entre Grupos .....	p. 117
Tabela 26 – Testes Estatísticos .....	p. 121
Tabela 27 – Síntese sobre a Experiência Geral e Desafios .....	p. 124
Tabela 28 – Resultado Quantitativo .....	p. 124

## **Lista de Figuras**

Figura 1 – Expansão da IoT .....	p. 03
Figura 2 – Arquitetura para Validação de Requisitos IoT .....	p. 43
Figura 3 – Framework para Mensuração de Requisitos .....	p. 45
Figura 4 – Software <i>QualIoT</i> .....	p. 61
Figura 5 – Arquitetura Técnica .....	p. 62
Figura 6 – Diagrama de Contexto .....	p. 64
Figura 7 – Sitemap .....	p. 65
Figura 8 – Fluxograma Funcional .....	p. 66
Figura 9 – BPMN .....	p. 68
Figura 10 – Arquitetura Funcional .....	p. 69
Figura 11 – Diagrama de Caso de Uso .....	p. 72
Figura 12 – Visão Macro da Metodologia de Pesquisa .....	p. 86
Figura 13 – Gráfico - Mediana de Pontos na Pré-Avaliação .....	p. 91
Figura 14 – Registro Fotográfico – Participantes .....	p. 93
Figura 15 – Registro Fotográfico – Participantes utilizando Framework .....	p. 94
Figura 16 – Registro Fotográfico – Participantes sem o uso do Framework .....	p. 94
Figura 17 – Formulário Grupo 2 .....	p. 95
Figura 18 – Registro Fotográfico – Participantes sem o uso do Framework .....	p. 96
Figura 19 – Formulário Debriefing .....	p. 98
Figura 20 – Comparativo Geral por Dimensão e Categoria de IoT .....	p. 104
Figura 21 – Maior Discrepância entre os Grupos .....	p. 106
Figura 22 – Diferença Média por Categoria de IoT de Grupo .....	p. 108
Figura 23 – Gráfico de Comparaçāo sobre a Campainha Inteligente .....	p. 110
Figura 24 – Gráfico de Comparaçāo sobre o Relógio .....	p. 111
Figura 25 – Gráfico de Comparaçāo sobre a Câmera .....	p. 112
Figura 26 – Gráfico de Comparaçāo sobre o Robô Aspirador .....	p. 113

Figura 27 – Gráfico de Comparação sobre Assistente Virtual .....	p. 114
Figura 28 – Gráfico de Comparação sobre o Drone .....	p. 116
Figura 29 – Média e Mediana .....	p. 118
Figura 30 – Desvio Padrão .....	p. 118
Figura 31 – Resultados para ANOVA .....	p. 121
Figura 32 – Resultados para o Teste T .....	p. 122
Figura 33 – Aspectos Quantitativos Debriefing .....	p. 125
Figura 34 – Participação em Projetos Futuros .....	p. 125
Figura 35 – Comparação de Frameworks .....	p. 129
Figura 36 – Logotipo <i>QualloT</i> .....	p. 147
Figura 37 – Paleta de Cores .....	p. 147
Figura 38 – Consulta INPI .....	p. 148

## **Lista de Siglas**

5G – Quinta Geração de Redes Móveis

ABINC – Associação Brasileira de Internet das Coisas

ANOVA – Analysis of Variance (Análise de Variância)

API – Application Programming Interface

CEP – Comitê de Ética em Pesquisa

CoAP – Constrained Application Protocol

IA – Inteligência Artificial

IIC – Industrial Internet Consortium

IoT – Internet das Coisas

IoT-MM – Internet of Things Maturity Model

MQTT – Message Queuing Telemetry Transport

M2M – Machine-to-Machine

PLN – Processamento de Linguagem Natural

*QualIoT* – Quality Framework for Internet of Things (Framework proposto)

RETIoT – Requirements Engineering Technology for IoT

RMF – Risk & Maturity Framework

SOA – Service-Oriented Architecture

TCLE – Termo de Consentimento Livre e Esclarecido

UCM4IoT – Use Case Modeling for IoT

# 1. Introdução

A Internet das Coisas (IoT) alterou a maneira como interagimos com o mundo físico, conectando dispositivos e gerando grandes volumes de dados. Esses dispositivos estão integrados em diversos contextos, como cidades inteligentes, saúde e manufatura, ampliando as possibilidades de automação e inteligência.

Costa *et al.* (2016), a Internet das Coisas (IoT) tem como principais objetivos aprimorar a qualidade de vida e tornar os processos industriais mais eficientes, por meio da automação de atividades que antes dependiam da intervenção humana. Médini *et al.* (2017) reforçam essa visão, descrevendo a IoT como uma tecnologia que impacta profundamente todos os aspectos da vida diária. Sua expansão redefine as interações com o mundo, abrindo novas perspectivas para um futuro digital. No entanto, como em qualquer grande transformação tecnológica, surgem desafios significativos, sendo um dos maiores a garantia da qualidade nas soluções de IoT, um aspecto vital para manter a funcionalidade e o valor dessas tecnologias (Ray *et al.* 2018).

O desenvolvimento de sistemas IoT eficazes e com alta qualidade requer um rigoroso processo de engenharia de requisitos. Noorzadeh *et al.* (2024) ressaltam que as características intrínsecas dos sistemas IoT, como redes, software, hardware, percepção de contexto e interoperabilidade, tornam a engenharia de requisitos uma tarefa altamente complexa. A qualidade nos requisitos IoT é essencial para garantir a confiabilidade e a utilidade dos dados coletados. Plageras *et al.* (2018) afirmam que, sem qualidade, os dados gerados pelos dispositivos IoT perdem seu valor, comprometendo a eficácia das soluções e limitando o potencial da tecnologia.

Este estudo propõe um *framework*, para mensurar a maturidade dos requisitos em sistemas IoT, com foco na garantia da qualidade, confiabilidade e segurança dessas soluções. Ao abordar a crescente complexidade dos sistemas IoT e a necessidade de validação rigorosa dos requisitos, a pesquisa visa contribuir significativamente para a evolução da engenharia de software nessa área emergente.

O *framework*, denominado *QualIoT*, é uma ferramenta voltada à avaliação da qualidade de software em sistemas IoT, com foco específico na análise dos requisitos. Sua aplicação também permite mensurar o nível de maturidade desses requisitos, fornecendo uma base sólida para decisões de melhoria contínua. O *QualIoT* é

estruturado em três processos principais: *(i)* Mensuração, que compreende a coleta e análise de dados relacionados a aspectos fundamentais da qualidade dos requisitos, como interoperabilidade, segurança, privacidade, usabilidade e confiabilidade; *(ii)* Classificação, que organiza os resultados obtidos em níveis de maturidade previamente definidos, permitindo uma visualização clara do estágio atual dos requisitos dentro de um contexto de desenvolvimento; *(iii)* Avaliação, que consolida os dados analisados, identifica deficiências e oferece recomendações práticas para aprimoramento dos sistemas IoT.

O *framework* proposto considera a heterogeneidade dos dispositivos, a diversidade de protocolos de comunicação, a importância dos dados gerados, bem como aspectos relacionados à usabilidade da solução. O diferencial deste trabalho está na proposição de um conjunto específico de métricas e indicadores para avaliar a maturidade dos requisitos, permitindo uma análise precisa e detalhada dos sistemas IoT. O estabelecimento de métricas e indicadores precisos mitiga a subjetividade na avaliação e fornece uma base objetiva para a validação dos requisitos em sistemas IoT. A metodologia adotada inclui uma revisão abrangente da literatura, a definição do framework e a aplicação do framework para validar os requisitos.

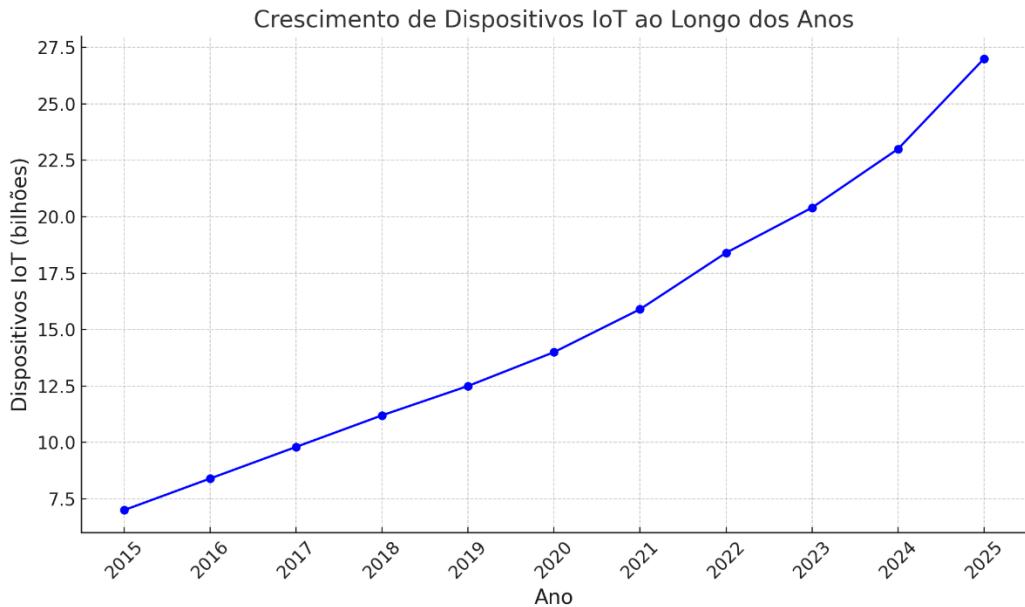
Com isso, os resultados esperados incluem a melhoria da qualidade dos requisitos para sistemas IoT por meio da mensuração dos requisitos organizados por dimensões. Este trabalho, portanto, visa contribuir para o avanço da engenharia de requisitos, oferecendo um *framework* diferenciado para a avaliação da maturidade em sistemas IoT, ao mesmo tempo em que orienta futuras pesquisas e práticas nesse campo.

## 1.1 Contexto, Motivação e Justificativa.

Nos últimos anos, os avanços tecnológicos têm transformado vários aspectos da vida cotidiana, com a IoT desempenhando um papel central nessa mudança. Dispositivos IoT estão se tornando cada vez mais presentes em residências, locais de trabalho e ambientes urbanos. Esses dispositivos conectados não apenas facilitam tarefas diárias, mas também ampliam a capacidade de gerar, coletar e gerenciar grandes volumes de dados em tempo real.

A IoT está impactando significativamente tanto indivíduos quanto mercados, ao possibilitar novas formas de criação e gerenciamento de informações. A Associação

Brasileira de Internet das Coisas (ABINC) reporta que, em 2015, existiam cerca de 7 bilhões de dispositivos IoT conectados globalmente. Esse número cresceu exponencialmente, atingindo 14 bilhões em 2020 e 20,4 bilhões em 2023. Conforme ilustra a Figura 1, as projeções indicam que, este ano (2025), o número de dispositivos conectados chegará a 27 bilhões.



**Figura1.** Expansão da IoT. **Fonte:** ABINC (Adaptado pelo autor)

A expansão da IoT é impulsionada pela convergência de tecnologias como a Inteligência Artificial (IA) e o 5G, que permitem uma comunicação mais rápida e eficiente entre dispositivos. Essas inovações não apenas aprimoram o desempenho dos sistemas IoT, mas também criam oportunidades de automação e análise de dados em tempo real.

O avanço tecnológico contínuo, impulsionado por dispositivos móveis, redes sociais e a Internet das Coisas, tem revolucionado os modos de vida e trazido novos desafios para indivíduos e organizações. Para contextualizar as motivações deste estudo, destacam-se três elementos-chaves, descritos a seguir:

(i) *Complexidade crescente dos sistemas IoT*: Com a proliferação de dispositivos IoT e a interconexão de sistemas heterogêneos, a complexidade dos requisitos aumenta, tornando importante a validação para garantir a qualidade e a confiabilidade. Noorzadeh *et al.* (2024) também apontam que a complexidade da engenharia de requisito em

sistemas IoT se deve à diversidade de componentes como redes, software, hardware, percepção de contexto e interoperabilidade.

(ii) *Custos elevados de falhas:* Erros nos requisitos podem resultar em retrabalho, atrasos no desenvolvimento e falhas em sistemas em produção, gerando custos significativos. Kaleem *et al.* (2019) afirmam que, ao identificar claramente os requisitos desde o início do projeto, é possível evitar falhas de *design*, erros de implementação e retrabalho desnecessário, reduzindo custos e otimizando o tempo de desenvolvimento.

(iii) *Riscos à segurança e privacidade:* A natureza dos dados coletados pelos sistemas IoT exige um alto nível de segurança e privacidade. A validação dos requisitos ajuda a garantir que esses aspectos sejam considerados desde o início do desenvolvimento. Alaba *et al.* (2018) afirmam que a segurança dos dispositivos IoT é uma preocupação central para garantir a operação confiável dos sistemas e a proteção dos dados coletados. Em um cenário cada vez mais conectado, dispositivos IoT estão sujeitos às ameaças cibernéticas, como ataques hackers e violações de privacidade. Portanto, requisitos fundamentados de segurança são importantes para mitigar esses riscos e proteger dados sensíveis. Para resumir as motivações do projeto, a Tabela 1 apresenta uma visão geral dos principais fatores que impulsionam este estudo.

**Tabela 1** - Resumo sobre as motivações do projeto.

Motivação	Descrição	Fontes
<i>Complexidade crescente dos sistemas IoT</i>	A proliferação de dispositivos IoT e a interconexão de sistemas heterogêneos aumentam a complexidade dos requisitos, tornando a validação essencial para garantir a qualidade e a confiabilidade.	(Aaqib <i>et al.</i> 2023). (Noorzadeh <i>et al.</i> , 2024).
<i>Custos elevados de falhas</i>	Erros nos requisitos podem levar a retrabalho, atrasos no desenvolvimento e falhas no sistema em produção, gerando custos significativos.	(Kaleem <i>et al.</i> , 2019).
<i>Riscos à segurança e privacidade</i>	A natureza dos dados coletados em sistemas IoT exige um alto nível de segurança e privacidade. A validação dos requisitos ajuda a garantir que esses aspectos sejam considerados desde o início do desenvolvimento.	(Alaba <i>et al.</i> , 2018).

**Fonte:** Autoria própria

Projetar um modelo para mensuração da maturidade dos requisitos em sistemas IoT é uma tarefa complexa, dada a diversidade de critérios de qualidade envolvidos. Sistemas IoT demandam uma abordagem que conte com aspectos como desempenho,

escalabilidade, adaptabilidade e confiabilidade, cada um possuindo diferentes níveis de prioridade conforme o contexto de aplicação. Segundo Dijkman *et al.* (2015), frameworks de qualidade para IoT precisam integrar dimensões como eficiência no uso de recursos, flexibilidade para acomodar novas funcionalidades e a capacidade de lidar com falhas em tempo real. Essas variáveis são complexas de mensurar e padronizar, pois cada aplicação IoT pode apresentar requisitos de qualidade bastante específicos.

Além disso, a dificuldade também está na natureza distribuída e dinâmica dos sistemas IoT, que exige uma avaliação contínua da qualidade ao longo do ciclo de vida dos dispositivos e sistemas. Frameworks de qualidade para IoT devem ser capazes de acomodar a evolução contínua de tecnologias e padrões, assegurando a manutenção da qualidade dos sistemas (Perera *et al.*, 2014).

A criação de um *framework* para mensurar a maturidade dos requisitos de IoT apresenta vários desafios do ponto de vista computacional. Primeiramente, a diversidade de dispositivos e plataformas IoT torna a padronização um desafio, uma vez que cada dispositivo pode ter diferentes capacidades de processamento, armazenamento e comunicação, dificultando a criação de métricas universais de qualidade. Além disso, a natureza distribuída dos sistemas IoT implica que a coleta e análise de dados de desempenho e qualidade devem ser realizadas de forma descentralizada e em tempo real, aumentando a complexidade do *framework*.

Para justificar este estudo, identificaram-se três necessidades principais que fundamentam a abordagem e o aprofundamento propostos neste campo da computação:

(i) *Falta de metodologias específicas*: Embora existam diversas metodologias para engenharia de requisitos, ainda há uma lacuna em relação a metodologias específicas para a validação de requisitos em sistemas IoT. Noorzadeh & Amini (2024) afirmam que métodos tradicionais de engenharia de requisitos não são suficientes para abordar os desafios específicos apresentados pela IoT.

(ii) *Necessidade de garantir a qualidade*: A validação dos requisitos é um passo essencial para garantir a qualidade do software, especialmente em sistemas complexos como os de IoT. Kaleem *et al.* (2019) destacam que, como as aplicações IoT estão emergindo rapidamente, é necessário focar no ciclo de vida de desenvolvimento de software para assegurar os níveis adequados de qualidade.

*(iii) Contribuição para o avanço da área:* O desenvolvimento de um validador de requisitos para IoT pode promover avanços significativos na pesquisa em engenharia de requisitos e qualidade de software.

Apesar dos avanços, ainda existem lacunas significativas na literatura. Muitos estudos focam em aspectos isolados da qualidade em sistemas IoT, como segurança ou desempenho, mas poucos abordam uma visão holística que integre múltiplas dimensões de qualidade. Além disso, a maioria dos *frameworks* existentes não considera a evolução contínua das tecnologias IoT e a necessidade de adaptação constante. O Capítulo 3 apresenta uma revisão sobre o tema, detalhando essas e outras lacunas existentes na literatura. Portanto, há uma necessidade clara de *frameworks* que sejam abrangentes, mas também flexíveis e adaptáveis. A abordagem proposta neste estudo visa preencher essas lacunas ao desenvolver um *framework* de maturidade que integre múltiplas dimensões de qualidade e se adapte às mudanças tecnológicas. O uso de técnicas de mensuração específicas permitirá uma avaliação mais precisa e contínua da qualidade dos sistemas IoT, garantindo que eles possam evoluir sem comprometer os requisitos de qualidade.

## 1.2 Objetivos, Contribuições e Métodos

Esta pesquisa aborda uma lacuna crítica no desenvolvimento de sistemas IoT: a ausência de ferramentas padronizadas que possibilitem avaliar a qualidade dos requisitos de forma sistemática e comparável. Considerando que requisitos de alta qualidade são essenciais para sistemas robustos, seguros e eficientes, propõe-se a criação de um *framework* que, além de avaliar a qualidade, também permita inferir o nível de maturidade desses requisitos com base em critérios objetivos. Assim, a questão central desta pesquisa é: *Como avaliar a qualidade dos requisitos em sistemas IoT de forma estruturada, permitindo também estimar seu nível de maturidade?* Para responder a essa pergunta, a pesquisa explorará diversas subquestões, como:

- (i) Quais são os critérios e indicadores mais relevantes para avaliar a maturidade dos requisitos?*
- (ii) Como a maturidade dos requisitos influencia a qualidade final do sistema?*
- (iii) Como o *framework* pode ser adaptado a diferentes contextos de desenvolvimento?*

A relevância desta pesquisa reside na necessidade de garantir a qualidade, a segurança e a eficiência dos sistemas IoT. O objetivo geral desta pesquisa é desenvolver um *framework* para mensuração e classificação de requisitos em sistemas IoT, com o objetivo de garantir a qualidade dos requisitos. Este *framework* deve incluir metodologias e ferramentas que permitam a identificação, análise e verificação de requisitos, visando assegurar que os sistemas IoT atendam às expectativas dos stakeholders e operem de maneira eficiente e segura em diversos ambientes e condições.

Além disso, o *framework* deve ser capaz de se adaptar às constantes evoluções tecnológicas, proporcionando uma base sólida para o desenvolvimento de soluções de IoT. Assim, como objetivos específicos, destacam-se:

- (i) Identificar e classificar os principais atributos de qualidade aplicáveis aos requisitos em sistemas IoT;
- (ii) Desenvolver métricas, critérios e instrumentos de avaliação que permitam medir a qualidade dos requisitos;
- (iii) Estruturar uma metodologia de classificação da maturidade dos requisitos com base nas avaliações realizadas;
- (iv) Aplicar e validar o framework em um estudo de caso com diferentes tipos de dispositivos IoT, analisando sua eficácia e aplicabilidade prática.

A hipótese desta pesquisa é que a implementação de um *framework* dedicado à avaliação da qualidade dos requisitos pode contribuir para a melhoria contínua dos sistemas IoT, tornando o processo de engenharia de requisitos mais estruturado, seguro e alinhado com boas práticas.

A arquitetura proposta inclui componentes principais, fluxos de dados e mecanismos de validação. Serão utilizadas técnicas de engenharia de requisitos específicas para IoT, como análise de necessidades e categorização de requisitos por critérios objetivos, garantindo um fluxo estruturado para organização e análise.

Para cada aspecto avaliado, serão utilizadas perguntas norteadoras que guiarão a validação dos requisitos, abrangendo elementos como identificação única, capacidade de atualização, consumo de energia, sensores, protocolos de comunicação, segurança, privacidade, processamento de dados e experiência do usuário. Com base nessas análises, será aplicada uma pontuação que permitirá mensurar a qualidade e estimar a maturidade dos requisitos.

As contribuições esperadas abrangem as dimensões científica, tecnológica e prática. No campo científico, espera-se fortalecer a base teórica da engenharia de requisitos para IoT. Do ponto de vista tecnológico, o *framework* poderá melhorar a precisão dos processos de validação e apoiar o desenvolvimento de produtos mais confiáveis. Na prática, espera-se reduzir falhas, retrabalho e aumentar a satisfação dos usuários finais.

Embora a aplicação em larga escala não seja escopo deste trabalho, acredita-se que o *framework* tenha potencial para gerar impacto significativo na qualidade de sistemas IoT, além de fomentar novas pesquisas na área.

### 1.3 Estrutura da Proposta

O primeiro capítulo introduz o conceito da Internet das Coisas (IoT) e seu impacto significativo em diversos setores, destacando o crescimento exponencial do número de dispositivos conectados e a revolução que isso traz para a coleta e análise de dados. A engenharia de requisitos para sistemas IoT é apresentada como uma área crítica, devido à sua complexidade intrínseca, que envolve não apenas o desenvolvimento de software, mas também a integração de hardware, redes de comunicação, e questões de segurança e privacidade. Este capítulo também discute a relevância de garantir a qualidade, segurança e eficiência dos requisitos de sistemas IoT, propondo a criação de um *framework* específico para mensurar a maturidade dos requisitos. Esta seção detalha como o *framework* proposto estrutura a avaliação da maturidade dos requisitos em sistemas IoT, abordando elementos essenciais como interoperabilidade, usabilidade e segurança.

O segundo capítulo oferece uma revisão aprofundada da literatura relacionada ao tema, começando com uma definição clara de IoT e explorando sua evolução histórica, o estado atual da tecnologia e as principais tendências futuras. A seguir, são discutidos os desafios específicos da engenharia de requisitos para IoT, destacando a complexidade envolvida na especificação de requisitos devido à natureza distribuída e dinâmica desses sistemas. O capítulo também aborda diferentes *frameworks* e modelos existentes para a validação de requisitos em sistemas de software tradicionais, comparando-os com as necessidades particulares dos sistemas IoT. Além disso, são identificadas lacunas na literatura atual, especialmente no que diz respeito à falta de metodologias padronizadas para a validação de requisitos IoT, o que justifica a necessidade do desenvolvimento do

*framework*. Este capítulo ainda inclui uma análise crítica de estudos relevantes, que aborda a aplicação de técnicas de engenharia de requisitos específicas para IoT e suas limitações.

O terceiro capítulo apresenta a base teórica e metodológica que sustenta esta pesquisa, combinando uma revisão sistemática da literatura com a análise crítica de trabalhos relacionados. Inicialmente, foram mapeados os principais desafios e práticas atuais na engenharia de requisitos e na avaliação da qualidade em sistemas IoT, identificando lacunas recorrentes como a ausência de critérios padronizados e métodos adaptáveis às particularidades desses sistemas. Em seguida, são discutidos *frameworks* existentes voltados à avaliação de requisitos, segurança e maturidade em IoT. Embora cada abordagem contribua em áreas específicas, observou-se que a maioria carece de uma visão integrada, especialmente no que diz respeito à qualidade dos requisitos e sua evolução ao longo do tempo. A análise comparativa dos trabalhos consultados reforça a necessidade de uma solução que combine critérios de qualidade, métodos de avaliação estruturada e suporte à adaptação contínua dos requisitos. Com base nesses fundamentos, foi concebido o *framework QualIoT*, cuja proposta é preencher essas lacunas e oferecer uma abordagem prática e abrangente para a avaliação da qualidade dos requisitos em sistemas IoT.

O quarto capítulo apresenta o detalhamento do *framework QualIoT*, abordando sua concepção, estrutura conceitual, critérios de avaliação e o processo de cálculo do índice de maturidade. São descritas as dimensões consideradas no modelo, as perguntas norteadoras utilizadas para orientar a avaliação dos requisitos e o método de pontuação empregado para classificar a maturidade das soluções IoT analisadas. Ao final do capítulo, também é discutida a lógica de classificação dos níveis de maturidade, com base nas pontuações obtidas.

O quinto capítulo introduz o *Software QualIoT*, ferramenta desenvolvida para operacionalizar a aplicação prática do *framework*. São apresentados os principais aspectos do sistema, incluindo a arquitetura técnica, os fluxos funcionais, os módulos implementados e o modo como a ferramenta apoia a avaliação de requisitos em diferentes contextos de IoT. A utilização do software permite aplicar os conceitos do modelo proposto de forma sistematizada, tornando viável sua adoção em estudos e projetos reais.

O sexto capítulo explora o estudo de caso realizado para validar o *framework QualIoT*, abordando os métodos e resultados obtidos na aplicação prática. Inicialmente, a metodologia foi estruturada em grupos para comparar o impacto do uso completo do *framework* em relação à aplicação apenas de suas dimensões isoladas. Foram realizadas etapas rigorosas, incluindo pré-avaliações, a aplicação do *framework* em dispositivos IoT de diferentes níveis de maturidade e análises qualitativas e quantitativas dos dados coletados. Esse capítulo revelou que o uso do *framework* contribuiu para avaliações mais consistentes, rigorosas e completas, principalmente em dimensões críticas como privacidade, segurança e transmissão de dados. Também se destacou que a abordagem estruturada ajudou os avaliadores a identificarem lacunas e propor melhorias, enquanto a abordagem menos sistemática teve resultados mais dispersos e subjetivos.

O sétimo capítulo apresenta a análise dos resultados obtidos. Estes resultados são amplamente discutidos e analisados em diferentes perspectivas, com destaque para as diferenças entre os dois grupos de participantes. São apresentados gráficos e tabelas que demonstram como o *framework QualIoT* influenciou positivamente a precisão e a consistência das avaliações. Os dispositivos foram analisados por nível de complexidade (básico, intermediário e avançado), evidenciando como o uso do *framework* ajudou na identificação de limitações técnicas e funcionais que poderiam ser negligenciadas. Além disso, foram realizados testes estatísticos, como ANOVA e Teste T, para validar a significância das diferenças observadas. O capítulo conclui ressaltando a robustez do *framework* em guiar avaliações técnicas e sua aplicabilidade em sistemas IoT complexos, como assistentes virtuais e dispositivos com inteligência artificial.

Por fim, o último capítulo sintetiza as contribuições da pesquisa, reforçando a relevância de um método estruturado para avaliação de requisitos em sistemas IoT. É demonstrado que o *framework* se mostrou eficaz ao fornecer ferramentas para avaliar a maturidade de sistemas, ajudando a identificar falhas e potenciais de melhoria. As conclusões destacam que o uso de abordagens sistemáticas como essa é essencial para lidar com os desafios da IoT, especialmente em relação à segurança e à privacidade.

Para fins de transparência, comprovação e aprofundamento das informações utilizadas nesta pesquisa, foram organizados apêndices e anexos ao final desta

dissertação. Nos apêndices, encontram-se: o artigo de revisão de literatura publicado no XX Workshop de Computação da UNIFACCAMP (Apêndice I); o artigo estendido, oriundo da mesma revisão, publicado na Revista FT – Qualis B2 (Apêndice II); a autorização para realização da pesquisa nas Faculdades Integradas Rio Branco (Apêndice III); o Termo de Consentimento Livre e Esclarecido (TCLE), devidamente submetido e aprovado pelo Comitê de Ética em Pesquisa (CEP) da Universidade Santo Amaro – UNISA (Apêndice IV); a representação da identidade visual do projeto, contendo o logotipo e a paleta de cores adotada (Apêndice V); e, por fim, a documentação do nome e identidade do *framework* proposto, *QualIoT*, incluindo a consulta de disponibilidade no Instituto Nacional da Propriedade Industrial – INPI (Apêndice VI).

Complementarmente, nos anexos, são apresentados: o certificado de premiação de melhor artigo no XX Workshop de Computação (Anexo I); o certificado da publicação do artigo na revista (Anexo II); a folha de rosto aprovada para a realização de pesquisa com seres humanos (Anexo III); e o certificado de registro de software junto ao INPI (Anexo IV).

## 1.4 Conclusão do Capítulo

A introdução deste estudo destaca a importância da Internet das Coisas (IoT) como uma força motriz na transformação tecnológica contemporânea, conectando dispositivos e promovendo automação em diversos contextos. Reconhecendo a complexidade da engenharia de requisitos em sistemas IoT, esta pesquisa propõe um *framework* que apoia a evolução contínua da engenharia de requisitos para sistemas IoT, promovendo soluções mais completas, seguras e alinhadas às demandas de um cenário tecnológico em constante transformação.

A proposta, fundamentada em uma revisão abrangente da literatura e na definição de métricas específicas, visa oferecer um *framework* que apoie a validação dos requisitos e contribua para o aprimoramento das práticas de engenharia de software em sistemas IoT, promovendo soluções mais fundamentadas e adaptáveis em um cenário de constante evolução tecnológica.

## **2. Referencial Teórico e Metodológico**

Este capítulo tem como objetivo apresentar de maneira concisa e clara os principais elementos e dimensões deste estudo. Será apresentada a Internet das Coisas (IoT) e sua adoção como tecnologia relevante (Seção 2.1). Além disso, será destacada a engenharia de requisitos como um aspecto fundamental na busca pela qualidade de software (Seção 2.2). Na sequência são apresentados conceitos de qualidade de software (Seção 2.3) e o referencial adotado em mensuração, ranking e avaliações (Seção 2.4), que compõe as técnicas necessárias para a criação do *framework* proposto.

### **2.1 Internet das Coisas**

A Internet das Coisas (IoT) representa uma revolução tecnológica que interconecta dispositivos físicos à rede digital, possibilitando a comunicação e troca de dados entre eles. De acordo com Gubbi *et al.* (2013), a IoT é caracterizada pela interconexão de sensores, dispositivos, redes e sistemas, facilitando a automação e o monitoramento de processos em tempo real. A conectividade entre esses dispositivos "inteligentes" permite interações tanto entre os próprios dispositivos quanto com os usuários, criando um ecossistema dinâmico e contínuo de informações.

Avanços em tecnologias de comunicação, como o 5G, têm impulsionado o crescimento da IoT ao aumentar a capacidade de conexão e reduzir a latência (Li, Xu e Zhao, 2015). Esses avanços permitem a implementação de sistemas IoT em grande escala, abrangendo áreas como cidades inteligentes, saúde, agricultura e automação industrial. Contudo, a complexidade inerente a esses sistemas traz desafios significativos de integração e segurança, os quais precisam ser superados para garantir a eficácia e a confiabilidade das soluções IoT.

Para alcançar o pleno potencial da IoT, o desenvolvimento de padrões e *frameworks* é essencial, orientando a implementação e a gestão dos dispositivos conectados. Segundo Atzori, Iera e Morabito (2010), a padronização é importante para assegurar a interoperabilidade entre dispositivos de diferentes fabricantes e facilitar a escalabilidade dos sistemas. *Frameworks* de referência são igualmente importantes para mitigar os desafios de segurança e privacidade inerentes à conectividade de múltiplos dispositivos em redes heterogêneas. A adoção da IoT também tem implicações econômicas e sociais

significativas. Li, Xu e Zhao (2015) destacam que a IoT pode transformar indústrias inteiras, modificando a forma como produtos são projetados, fabricados e mantidos. A capacidade de coletar e analisar grandes volumes de dados em tempo real pode aprimorar a tomada de decisões em diversas áreas, desde o gerenciamento de recursos naturais até a prestação de serviços de saúde. Nesse contexto, é possível organizar os componentes essenciais da IoT em dois grupos: infraestrutura técnica e aspectos de qualidade e uso.

A infraestrutura técnica envolve sensores, transmissão de dados e plataformas de processamento. A coleta de dados ocorre por meio de sensores, dispositivos embarcados e outras entidades conectadas. Esses sensores são projetados para operar em tempo real e capturar variáveis como temperatura, umidade ou movimento, sendo sua precisão um fator determinante para a confiabilidade das decisões (Miorandi *et al.*, 2012). A frequência de amostragem também impacta a eficácia dos sistemas, especialmente em aplicações com alta resolução temporal. Além disso, a capacidade de armazenamento deve ser dimensionada para lidar com grandes volumes de dados, sendo comum o uso de técnicas de compressão e agregação para evitar perdas e otimizar o tráfego (Zhang *et al.*, 2017).

Dispositivos embarcados, como microcontroladores e *single-board computers*, também atuam nesse processo, realizando análises locais antes de enviar dados para a nuvem. Essa abordagem, conhecida como *edge computing*, permite filtrar informações irrelevantes e reduzir a carga de dados, aumentando a eficiência (Shi *et al.*, 2016). Câmeras de vigilância, *smartphones* e outros dispositivos também participam do ecossistema como nós de captura e retransmissão de dados (Atzori, Iera e Morabito, 2010).

A transmissão de dados, por sua vez, deve equilibrar confiabilidade, latência e eficiência energética. Tecnologias como *Wi-Fi*, *Bluetooth*, *Zigbee* ou redes celulares (3G, 4G, 5G) são escolhidas conforme as demandas de largura de banda, alcance e consumo. O uso de protocolos como MQTT (*Message Queuing Telemetry Transport*) e CoAP (*Constrained Application Protocol*) é comum em aplicações com restrições de processamento, pois são leves e seguros. Segundo Quincozes *et al.* (2024), a escolha adequada do protocolo é essencial para assegurar segurança e desempenho em diferentes contextos de IoT.

O processamento e armazenamento de dados são viabilizados principalmente pela *cloud computing*, que oferece elasticidade, escalabilidade e capacidades avançadas para aplicações como *machine learning* e análise preditiva (Armbrust *et al.*, 2010). Modelos como *IaaS*, *PaaS* e *SaaS* permitem ajustar o nível de controle conforme a necessidade da aplicação (Mell e Grance, 2011). Em paralelo, o *edge computing* continua sendo importante em sistemas que exigem baixa latência e respostas em tempo real, como na indústria ou em veículos autônomos (Shi *et al.*, 2016).

Além dos aspectos técnicos, a IoT demanda atenção especial à qualidade dos dados, à segurança e à experiência do usuário. A segurança é um dos pontos mais relevantes, dada a quantidade de dados sensíveis e a exposição dos dispositivos a redes públicas. Segundo Roman, Najera e Lopez (2011), proteger dispositivos com recursos limitados e garantir a privacidade em ambientes distribuídos exige soluções como criptografia de ponta a ponta, autenticação robusta e segmentação de rede (*security by design*). A atualização contínua dos dispositivos também é necessária para corrigir vulnerabilidades, embora a ausência de padrões globais dificulte a adoção universal dessas práticas (Weber, 2010). Uma abordagem de "defesa em profundidade" se mostra eficaz para mitigar riscos (Li *et al.*, 2015).

A análise de dados desempenha papel estratégico na geração de valor em sistemas IoT. Segundo Fortino et al. (2018), a capacidade de transformar dados em informações relevantes permite antecipar problemas, otimizar recursos e apoiar decisões automatizadas ou humanas. Técnicas como *machine learning*, *redes neurais* e *clustering* são utilizadas para identificar padrões e detectar anomalias (Zhang *et al.*, 2017). Em ambientes sensíveis, como saúde ou segurança pública, a geração de alertas rápidos e precisos é essencial (Kreković *et al.*, 2024)

Finalmente, a usabilidade é um fator determinante para o sucesso das soluções. Hassan *et al.* (2020) destacam cinco atributos principais: facilidade de aprendizado, eficiência, memorização, prevenção de erros e satisfação do usuário. Interfaces simples, acessíveis e adaptáveis garantem uma melhor experiência, especialmente para usuários com diferentes níveis de familiaridade com tecnologia. A inclusão de recursos como comandos de voz, legendas em tempo real e *feedback* tátil promove acessibilidade e inclusão digital (Lazar *et al.*, 2015; W3C, 2018).

## 2.2 Engenharia de Requisitos para IoT

A Engenharia de Requisitos é um processo fundamental no desenvolvimento de sistemas de software, pois envolve a identificação, documentação e gerenciamento das necessidades e expectativas dos *stakeholders*. Sommerville (2011) argumenta que uma engenharia de requisitos eficaz é essencial para assegurar que o sistema final atenda às necessidades dos usuários e seja entregue dentro dos prazos e orçamentos estabelecidos. Uma engenharia de requisitos bem conduzida contribui para a redução de alterações no projeto e para a melhoria da comunicação entre a equipe de desenvolvimento e os stakeholders.

No contexto da IoT, a engenharia de requisitos apresenta desafios específicos devido à natureza distribuída e dinâmica desses sistemas. Esses desafios incluem a necessidade de lidar com uma vasta quantidade de dispositivos heterogêneos, que geram dados de diferentes fontes, em tempos e formatos variados (Perera et al., 2014). A definição clara das funcionalidades e restrições torna-se essencial para garantir a interoperabilidade entre dispositivos e a consistência dos dados processados.

Além dos requisitos funcionais, os requisitos não funcionais, como segurança, privacidade e desempenho, assumem um papel central em sistemas IoT. Devido à sua exposição contínua a redes externas, esses sistemas estão vulneráveis a ameaças cibernéticas, tornando fundamental a consideração desses requisitos desde o início do processo de engenharia (Roman, Najera & Lopez, 2011). Práticas de segurança por design são essenciais para proteger dados sensíveis e manter a integridade do sistema.

Estudos como os Quincozes *et al.* (2024) e Saeed *et al.* (2021) destacam que a elicitação de requisitos para sistemas IoT deve ser um processo iterativo, com envolvimento ativo dos stakeholders, incluindo usuários finais, desenvolvedores e especialistas em segurança. Quincozes *et al.* (2024) recomenda métodos como workshops e entrevistas, enquanto Saeed *et al.* (2021) acrescentam a importância da prototipagem rápida para adaptar as necessidades em um ambiente dinâmico, permitindo ajustes constantes conforme novas tecnologias surgem e as expectativas dos usuários evoluem.

A priorização dos requisitos também desempenha um papel chave na engenharia de requisitos para IoT. Karlsson, Wohlin e Regnell (1998) destacam a importância de equilibrar as necessidades dos diferentes stakeholders e de garantir que os requisitos

mais críticos sejam abordados primeiro. Em sistemas IoT, isso frequentemente significa priorizar requisitos de segurança e interoperabilidade, que são essenciais para garantir uma operação segura e contínua dos dispositivos e da infraestrutura.

## 2.3 Qualidade de Software para IoT

A qualidade de software é um aspecto importante em projetos de desenvolvimento, especialmente em sistemas complexos como os de IoT. Segundo Pressman (2014), qualidade de software envolve a conformidade do produto com os requisitos funcionais e não funcionais, além de sua capacidade de atender às expectativas dos usuários.

Em sistemas IoT, a qualidade é avaliada por fatores como confiabilidade, segurança, usabilidade e desempenho, que são essenciais para garantir a operação contínua e segura dos dispositivos conectados. Para assegurar a qualidade em sistemas IoT, é fundamental implementar processos rigorosos de teste e validação ao longo do ciclo de vida do desenvolvimento do software. Basili e Boehm (2001) destacam a importância de incluir testes de integração, que garantem a comunicação segura entre dispositivos, e testes de carga, que avaliam o desempenho do sistema sob diferentes condições de uso. Esses testes permitem identificar e corrigir problemas antes da implantação, reduzindo o risco de falhas em ambientes reais.

A avaliação contínua da qualidade em IoT também exige o monitoramento de métricas-chave, como tempo de resposta, taxa de falhas e disponibilidade do sistema (Fenton & Pfleeger, 1998). O uso de ferramentas de monitoramento automatizado ajuda a detectar problemas em tempo real, possibilitando intervenções rápidas para minimizar impactos no usuário final. Além disso, a qualidade de software em IoT está fortemente ligada à capacidade do sistema de se adaptar a mudanças no ambiente operacional, um conceito descrito por Lehman e Belady (1985) em sua análise sobre a evolução dos sistemas de software.

## 2.4 Técnicas de Avaliação e Mensuração de Requisitos para IoT

A avaliação e mensuração de sistemas IoT é decisivo para determinar a eficácia, eficiência e maturidade das soluções implementadas. Diferentes técnicas de mensuração são aplicadas na literatura para avaliar os sistemas IoT em termos de qualidade,

desempenho, segurança, usabilidade e outros critérios importantes. A seguir, são apresentadas as técnicas de avaliação e mensuração identificadas na literatura e adotadas como base teórica para este estudo. Essas técnicas compõem o estado da arte e servem de referência para o desenvolvimento do *framework* proposto, que será detalhado no Capítulo 4.

Perguntas norteadoras são uma técnica amplamente utilizada para a avaliação qualitativa de sistemas complexos, como os de IoT. Segundo Lincoln e Guba (1985), essas perguntas são eficazes para orientar a coleta de informações de maneira estruturada, permitindo que os pesquisadores se aprofundem em aspectos específicos do sistema, como desempenho e satisfação dos usuários. Isso ajuda a garantir que todas as dimensões importantes do sistema sejam exploradas e consideradas durante a avaliação.

Além de facilitar o levantamento de dados, as perguntas norteadoras promovem uma análise reflexiva, essencial para compreender as interações entre os componentes do sistema e os usuários. Essa técnica é particularmente útil em contextos de IoT, onde a diversidade de dispositivos e a heterogeneidade dos dados exigem uma abordagem mais flexível e adaptativa (Patton, 2002). Ao fazer perguntas que se relacionam diretamente com os objetivos do sistema, é possível identificar áreas de melhoria e ajustar as estratégias de desenvolvimento.

As perguntas norteadoras também servem para envolver os *stakeholders* de maneira ativa no processo de avaliação. A inclusão de diferentes perspectivas, como de usuários finais e desenvolvedores, ajuda a criar uma visão mais holística do sistema. De acordo com Stake (1995), essa abordagem participativa é importante para assegurar que as avaliações reflitam as necessidades reais dos usuários, promovendo uma maior aderência dos requisitos. Por fim, as perguntas norteadoras contribuem para a triangulação de dados, um conceito central em pesquisas qualitativas que visa aumentar a credibilidade dos achados (Denzin, 2012). Ao combinar diferentes fontes de informação e perspectivas, a triangulação ajuda a validar as conclusões, garantindo que a avaliação do sistema IoT seja fundamentada e baseada em uma compreensão abrangente dos fenômenos estudados.

Já a utilização de rankings é uma técnica que permite a comparação estruturada entre diferentes soluções ou componentes de um sistema IoT. Segundo Saaty (1980), essa abordagem facilita a tomada de decisões ao ordenar elementos de acordo com

critérios predefinidos, como eficiência e custo-benefício. Em um ambiente de IoT, rankings podem ser usados para avaliar a qualidade de dispositivos de sensores, desempenho de protocolos de comunicação, ou a segurança de diferentes soluções.

Os rankings são especialmente úteis quando há a necessidade de priorizar melhorias em sistemas que apresentam limitações de recursos, como energia e largura de banda. Por exemplo, em um estudo de IoT aplicado a cidades inteligentes, classificações podem ajudar a identificar quais sensores de monitoramento são mais eficazes em termos de custo e precisão (Zanella *et al.*, 2014). Esse tipo de análise comparativa permite que os tomadores de decisão aloquem recursos de maneira mais eficiente.

Além disso, a utilização de rankings facilita a comunicação de resultados para os *stakeholders*. Apresentar dados de forma ordenada e clara torna mais fácil para os envolvidos entenderem as diferenças entre as alternativas avaliadas. Isso é importante em contextos empresariais, onde decisões sobre a adoção de tecnologias IoT precisam ser fundamentadas em critérios objetivos (Ali *et al.*, 2018).

Rankings também permitem uma avaliação dinâmica dos componentes do sistema IoT, adaptando-se à medida que novas tecnologias ou atualizações são introduzidas. Segundo Hwang e Yoon (1981), técnicas de análise multicritério, como o Método de Análise Hierárquica (AHP), são eficazes para ajustar os rankings conforme as condições do ambiente mudam, garantindo que a avaliação permaneça relevante ao longo do tempo.

A atribuição de notas e o uso de escalas são técnicas quantitativas amplamente utilizadas para mensurar atributos específicos de sistemas IoT. Likert (1932) introduziu o conceito de escalas de classificação ordinalizadas, que são amplamente utilizadas para avaliar a percepção dos usuários em relação a critérios como usabilidade, segurança e confiabilidade. Em sistemas IoT, essas escalas são aplicadas para coletar feedbacks que auxiliam na identificação de pontos fortes e fracos dos dispositivos e aplicativos.

Essas escalas permitem que *feedbacks* subjetivos sejam transformados em dados quantitativos, facilitando a análise estatística. Isso é especialmente útil em avaliações que requerem a comparação entre diferentes versões de um software ou dispositivo. Segundo Trochim (2006), o uso de notas permite realizar análises descritivas e

inferenciais, contribuindo para uma compreensão mais detalhada do desempenho dos sistemas IoT.

A análise das respostas em escalas também possibilita a identificação de padrões de satisfação ou insatisfação dos usuários. Estudos demonstram que a mensuração por meio de escalas é eficaz para avaliar o impacto das funcionalidades de um sistema IoT na experiência do usuário (Marin *et al.*, 2015). Essas métricas podem ser usadas para guiar ajustes que aumentem a aceitação do sistema.

Além disso, o uso de escalas contribui para o processo de melhoria contínua em sistemas IoT. A coleta regular de avaliações permite que os desenvolvedores identifiquem rapidamente as áreas que necessitam de ajustes e implementem melhorias iterativas. Segundo Nielsen (2012), essa prática de avaliação contínua é necessária para manter a qualidade do software ao longo de seu ciclo de vida.

Ainda sobre a avaliação contínua, podemos considerá-la um elemento central na garantia da qualidade e adaptabilidade dos sistemas IoT. Segundo Basili e Boehm (2001), a avaliação contínua durante o desenvolvimento de um sistema permite identificar problemas em tempo real, possibilitando correções rápidas antes que o sistema seja implementado em ambientes reais. Isso é particularmente importante em aplicações de IoT, onde a estabilidade e a segurança são essenciais para operações críticas. O monitoramento de métricas-chave, como tempo de resposta, taxa de falhas e disponibilidade do sistema, ajuda a manter a eficiência operacional e a segurança do sistema IoT (Fenton & Pfleeger, 1998). Ferramentas de monitoramento automatizado permitem detectar anomalias rapidamente, o que reduz o tempo de resposta para a resolução de problemas, evitando impactos negativos na experiência dos usuários finais.

Além disso, a avaliação contínua facilita a adaptação dos sistemas IoT a novos cenários operacionais e requisitos de mercado. Lehman e Belady (1985) destacam a importância da adaptabilidade dos sistemas de software, afirmando que a evolução contínua é necessária para que as soluções permaneçam relevantes. Em sistemas IoT, isso inclui a capacidade de incorporar novos dispositivos e tecnologias, ajustando-se conforme as necessidades dos usuários mudam.

A integração de processos de avaliação contínua ao ciclo de vida do software ajuda a criar um sistema mais completo e preparado para enfrentar desafios futuros. A análise de métricas de desempenho em tempo real permite que ajustes sejam feitos de

forma proativa, garantindo que o sistema opere de maneira eficiente e segura mesmo em ambientes complexos e dinâmicos (Miorandi *et al.*, 2012).

## 2.5 Conclusão do Capítulo

Este capítulo enfatizou a complexidade e importância da IoT e a necessidade de uma abordagem sistemática para lidar com seus desafios. A engenharia de requisitos é fundamental para definir as necessidades específicas de cada aplicação, garantindo que os sistemas atendam aos objetivos esperados. A qualidade de software, por sua vez, assegura a confiabilidade, segurança e eficiência, essenciais para a operação de dispositivos interconectados. As métricas de mensuração proporcionam uma base para avaliar e melhorar continuamente o desempenho e a maturidade dos sistemas IoT, permitindo adaptações em um ambiente em constante evolução.

A criação e adoção de *frameworks* padronizados são vitais para a interoperabilidade, possibilitando que diferentes dispositivos e tecnologias se integrem de forma eficiente. Isso é decisivo em um cenário de crescimento contínuo, onde novas soluções e dispositivos são introduzidos regularmente. A segurança, sempre um ponto decisivo, deve ser tratada desde o design, considerando a natureza distribuída e as vulnerabilidades dos sistemas IoT. Adicionalmente, a mensuração detalhada e contínua, utilizando técnicas como perguntas norteadoras, rankings, e avaliações quantitativas, contribui para uma visão completa das soluções IoT, garantindo que os sistemas sejam otimizados não apenas em termos de desempenho, mas também quanto à usabilidade e satisfação do usuário. A necessidade de uma abordagem proativa é evidente, especialmente para antecipar e mitigar problemas antes que afetem negativamente os usuários e a infraestrutura.

Portanto, o capítulo conclui que, para que a IoT realize seu pleno potencial e impacte positivamente as sociedades e economias globais, é imprescindível um equilíbrio entre inovação e rigor técnico, considerando as necessidades de adaptabilidade, segurança e eficiência dos sistemas. Ao abordar essas questões de maneira estruturada e orientada por métricas, é possível criar soluções IoT mais resilientes, alinhadas com os desafios e oportunidades do futuro.

### **3. Revisão da Literatura e Trabalhos Relacionados**

Este capítulo apresenta a base teórica, metodológica e conceitual que sustenta esta pesquisa, bem como o processo de construção do *framework QualIoT* proposto. O capítulo foi estruturado em três eixos complementares:

Primeiramente, conduzimos uma revisão sistemática da literatura sobre engenharia de requisitos e qualidade de software em sistemas IoT (Seção 3.2), com o objetivo de mapear os principais desafios, práticas e lacunas no estado da arte.

Em seguida, apresentamos uma análise crítica dos trabalhos relacionados e *frameworks* existentes (Seção 3.3), identificando suas contribuições e limitações, de modo a situar o *QualIoT* no contexto atual das abordagens para avaliação de requisitos em sistemas IoT.

Com base nessas análises, na Seção 3.5 descrevemos o processo de elaboração do *framework QualIoT*, detalhando a metodologia empregada, as decisões de projeto e os princípios adotados para o desenvolvimento de uma abordagem holística, flexível e orientada à prática.

Dessa forma, este capítulo consolida os fundamentos teóricos e metodológicos que nortearam o desenvolvimento do *QualIoT*, oferecendo uma visão integrada do contexto em que o *framework* foi concebido. A Seção 3.6 apresenta a conclusão do capítulo e destaca as contribuições que sustentam a proposta do *framework*, preparando o terreno para a descrição detalhada de sua estrutura e aplicação no capítulo seguinte.

#### **3.1 Metodologia de Revisão**

A revisão da literatura apresentada neste capítulo foi conduzida com base no guia metodológico proposto por Kitchenham (2004), que recomenda um processo sistemático e transparente para garantir a qualidade das revisões em Engenharia de Software e áreas correlatas. O objetivo principal desta revisão é responder à seguinte questão de pesquisa: “*Como garantir a qualidade de requisitos em sistemas IoT através da mensuração de seus requisitos?*”

Com essa finalidade, foi realizada uma pesquisa exploratória preliminar, que permitiu definir os parâmetros da revisão, o escopo de análise e a estratégia de busca. Foram estabelecidos o período de abrangência, as bases científicas a serem consultadas,

as palavras-chave, e a delimitação das áreas de busca. O período de análise foi delimitado entre janeiro de 2014 e julho de 2024, em razão do caráter emergente do tema e da expectativa de evolução significativa nos últimos dez anos. As buscas foram realizadas nas seguintes bases científicas: *Springer Link*, *IEEE Xplore*, *Science Direct* e *ACM Digital Library*. A base *Google Scholar* foi excluída do processo, por ser uma indexadora ampla e dificultar o controle de duplicatas e da qualidade dos resultados. A string de busca utilizada foi: (*IoT OR "Internet of Things"*) AND *"Requirement Engineering"* AND *"Framework"* AND (*"Quality"* OR *"Software Quality"*), sendo ajustada conforme a sintaxe de cada base.

A busca inicial resultou em 662 artigos: 91 provenientes da *Springer Link*, 159 da *IEEE Xplore*, 342 da *Science Direct* e 70 da *ACM Digital Library*. Após a remoção de 95 artigos duplicados, o conjunto de artigos passou por uma triagem com base em critérios de inclusão e exclusão previamente definidos. A Tabela 2 apresenta os critérios aplicados.

**Tabela 2 – Critérios de Inclusão e Exclusão**

Tipo	Código	Descrição
Inclusão	I1	Estudos que abordem qualidade em sistemas IoT.
	I2	Pesquisas sobre engenharia de requisitos aplicadas a IoT.
	I3	Trabalhos que considerem usuários e stakeholders.
	I4	Estudos que tratem de segurança, testes ou validação em IoT.
Exclusão	E1	Artigos em idiomas diferentes do inglês ou português.
	E2	Trabalhos não relacionados à qualidade ou requisitos em IoT.
	E3	Estudos fora da área de computação (ou sem relação multidisciplinar com computação).
	E4	Textos que não sejam publicações científicas (ex.: resumos, editoriais, notícias).

**Fonte:** Autoria própria

Na primeira etapa de seleção, foi realizada uma análise dos títulos, resumos e palavras-chave dos artigos. Os estudos que atendiam aos critérios de inclusão foram, então, analisados em profundidade em relação ao texto completo. Ao final do processo,

foram selecionados 49 artigos aderentes ao tema da pesquisa. Desses 49 artigos, 22 estudos apresentaram discussões relevantes para os temas de engenharia de requisitos e qualidade em sistemas IoT. Dentro desse conjunto, 17 artigos corresponderam a revisões de literatura, oferecendo uma visão consolidada sobre o estado da arte. Complementarmente, 5 artigos apresentaram *frameworks* estruturados, os quais foram identificados como adequados para a comparação com o *framework* proposto neste trabalho.

O processo metodológico seguido nesta revisão compreendeu um conjunto estruturado de etapas, que serão detalhadas na Tabela 3 a seguir. Essas etapas envolveram: definição da questão de pesquisa; definição da *string* de busca e seleção das bases de dados; execução das buscas e coleta inicial de artigos; remoção de duplicatas; aplicação dos critérios de inclusão e exclusão (triagem inicial de títulos, resumos e palavras-chave); análise completa dos artigos aderentes; e seleção final dos estudos para análise e comparação com o *framework* proposto. Como resultado, esta revisão sistemática permitiu mapear de maneira consistente o estado da arte sobre qualidade de requisitos em sistemas IoT, oferecendo uma base teórica sólida para o desenvolvimento do *framework QualIoT*. A síntese dessas etapas está apresentada na Tabela 3.

**Tabela 3 – Processo Metodológico**

<i>Etapa</i>	<i>Descrição</i>
1	Definição da questão de pesquisa.
2	Definição da <i>string</i> de busca e escolha das bases científicas.
3	Execução das buscas e coleta inicial de artigos.
4	Remoção de duplicatas.
5	Aplicação dos critérios de inclusão e exclusão (títulos, resumos e palavras-chave).
6	Análise completa dos artigos selecionados.
7	Seleção final dos estudos para comparação e fundamentação do <i>framework</i> proposto.

**Fonte:** Autoria própria

Cabe destacar que a revisão priorizou artigos publicados em periódicos e conferências com revisão por pares. Teses e dissertações foram consultadas apenas

como material complementar, quando relevantes para a contextualização teórica, mas não compuseram o núcleo de análise da revisão sistemática. Essa escolha visou assegurar maior rigor metodológico e comparabilidade entre os estudos selecionados

## 3.2 Resultados e Análise dos Artigos

A partir da metodologia descrita na Seção 3.1, foi conduzida uma revisão sistemática com o objetivo de identificar os principais desafios, práticas e lacunas no campo da avaliação da qualidade dos requisitos em sistemas IoT. A análise dos estudos selecionados permitiu mapear tanto as abordagens voltadas à engenharia de requisitos quanto aquelas relacionadas à qualidade de software, elementos que são fundamentais para a construção de soluções seguras em ambientes IoT.

Os resultados da revisão foram organizados em duas categorias complementares. A Seção 3.2.1 aborda as principais contribuições e desafios identificados na engenharia de requisitos para sistemas IoT, enquanto a Seção 3.2.2 analisa os critérios que definem a qualidade de software nesse contexto; e a Seção 3.2.3 discute de forma integrada os achados da revisão, evidenciando como a engenharia de requisitos e a qualidade de software se relacionam e impactam o desenvolvimento de soluções IoT. A partir dessa análise, buscou-se não apenas consolidar o estado da arte, mas também identificar as lacunas que justificam a proposta de um *framework* específico que será apresentado nos capítulos subsequentes.

### 3.2.1 Análise sobre engenharia de requisito em IoT

A engenharia de requisitos desempenha um papel central no desenvolvimento de soluções IoT, sendo responsável por garantir que os sistemas atendam de forma adequada às necessidades dos *stakeholders* e aos desafios tecnológicos próprios desse domínio. A revisão da literatura evidenciou que a especificação de requisitos em IoT é particularmente complexa devido à heterogeneidade dos dispositivos, à distribuição geográfica e à natureza dinâmica dos sistemas, fatores que demandam abordagens específicas e adaptativas. Diversos estudos analisados exploram essas particularidades sob diferentes dimensões. Costa *et al.* (2017), Kaleem *et al.* (2019), Almeida, Peres e L’Erario (2022), Nakajima & Komiyama (2019), Lindquist *et al.* (2022), Ge *et al.* (2018), Shital *et al.* (2023), Stergiou *et al.* (2018), Paul *et al.* (2017), Perez-Castillo *et*

*al.* (2018) e Banerjee & Sheth (2017) destacam que aspectos como funcionalidade, segurança, experiência do usuário, conflitos entre camadas, estruturas de qualidade e impacto dos requisitos na confiabilidade dos dispositivos são fundamentais no contexto IoT. Um primeiro conjunto de estudos enfatiza a necessidade de alinhar requisitos de funcionalidade, segurança e experiência do usuário. Kaleem *et al.* (2019) e Perez-Castillo *et al.* (2018) apontam que a definição de requisitos claros para funções básicas dos dispositivos — desde a coleta de dados até a interação com sistemas externos — deve ser complementada por requisitos de segurança e usabilidade. Esses autores destacam que falhas em requisitos de segurança podem comprometer não apenas a integridade dos dados, mas também a confiabilidade e a aceitação das soluções por parte dos usuários.

Em termos de elicitação e especificação, Costa *et al.* (2016) propõem um modelo estruturado que considera diferentes níveis de granularidade e abstração, facilitando a identificação de requisitos conflitantes e a priorização de aspectos críticos. Kaleem *et al.* (2019) reforçam a importância de um processo de elicitação participativo, envolvendo todas as partes interessadas desde as fases iniciais do projeto, de forma a reduzir ambiguidades e alinhar expectativas. Outro aspecto recorrente na literatura diz respeito à necessidade de gerenciar conflitos e influências em diferentes camadas dos sistemas IoT. Paul *et al.* (2017) alertam que requisitos de eficiência energética, latência e segurança podem entrar em conflito entre as diversas camadas (infraestrutura, rede, aplicação). Nakajima & Komiyama (2019) propõem um método baseado em abordagem multiobjetiva para mitigar esses conflitos, permitindo equilibrar requisitos de camadas distintas de maneira eficiente. Os desafios inerentes à engenharia de requisitos em IoT são amplamente reconhecidos. Banerjee & Sheth (2017) ressaltam que a heterogeneidade dos dispositivos, a distribuição física e a constante evolução tecnológica dificultam a aplicação de métodos tradicionais. Almeida, Peres & L'Erario (2022), em resposta a esses desafios, propõem um *framework* específico que utiliza técnicas como entrevistas, *workshops* e análise documental, visando adaptar as práticas de elicitação ao contexto dinâmico e distribuído da IoT.

Além disso, a importância de adotar estruturas de requisitos de qualidade é destacada. Nakajima & Komiyama (2019) demonstram como normas como a ISO/IEC 25030 podem ser aplicadas para avaliar a usabilidade, segurança, confiabilidade e desempenho

de dispositivos IoT, servindo como referência para garantir padrões consistentes de qualidade. Por fim, a relação entre requisitos e a qualidade final dos dispositivos IoT é amplamente discutida. Shital *et al.* (2023) e Lindquist *et al.* (2022) demonstram que requisitos bem definidos impactam diretamente a segurança, privacidade, confiabilidade e precisão das soluções. Em contrapartida, Stergiou *et al.* (2018) e Ge *et al.* (2018) ilustram como a negligência de requisitos críticos pode levar a falhas significativas, desde ataques cibernéticos até interrupções de serviço e comprometimento da integridade dos dados. A síntese das dimensões identificadas na engenharia de requisitos para sistemas IoT é apresentada na Tabela 4, que resume as categorias abordadas na literatura e as respectivas contribuições dos autores.

**Tabela 4 - Dimensões da Engenharia de Requisitos para IoT**

Categoria	Abordagens	Descrição
<i>Funcionalidade, Segurança e Experiência do Usuário</i>	<i>Requisitos para o Sucesso</i>	Dispositivos IoT devem atender a funções básicas, garantir segurança e proporcionar boa experiência ao usuário (Kaleem <i>et al.</i> , 2019) & (Perez-Castillo <i>et al.</i> , 2018).
	<i>Abordagens para Elicitação e Especificação</i>	Modelo para eliciar requisitos de stakeholders em IoT, considerando diferentes níveis de granularidade (Costa <i>et al.</i> , 2016).
<i>Conflitos e Influências em Diferentes Camadas</i>	<i>Desafios de Múltiplas Camadas</i>	Sistemas IoT possuem diversas camadas com requisitos específicos que podem entrar em conflito (Paul <i>et. al.</i> , 2017).
	<i>Mitigação de Conflitos</i>	Métodos para mitigar conflitos entre requisitos em diferentes camadas (Nakajima & Komiya, 2019).
<i>Desafios na Engenharia de Requisitos para IoT</i>	<i>Características Únicas da IoT</i>	Elicitação, análise e especificação de requisitos em IoT apresentam desafios específicos devido à heterogeneidade dos dispositivos, distribuição geográfica e natureza dinâmica dos sistemas (Banerjee & Sheth., 2017).
	<i>Abordagens para Superar os Desafios</i>	Framework para eliciar requisitos em sistemas IoT, considerando as características únicas dessa tecnologia (Almeida, Peres & L'Erario., 2022).
<i>Importância das Estruturas de Requisitos de Qualidade</i>	<i>Padronização da Qualidade</i>	Normas como a ISO/IEC 25030 oferecem uma estrutura abrangente para avaliar a qualidade do software, incluindo critérios específicos para IoT (Nakajima & Komiya, 2019).
	<i>Aplicação da ISO/IEC</i>	Utilização da ISO/IEC 25030 para identificar requisitos críticos que

	25030	impactam diretamente a qualidade dos dispositivos IoT (Nakajima & Komiyama, 2019).
<i>Impacto dos Requisitos na Qualidade dos Dispositivos IoT</i>	<i>Requisitos para Dispositivos Confiáveis</i>	Requisitos bem definidos garantem a segurança, privacidade, confiabilidade e precisão dos dispositivos IoT (Shital <i>et. al.</i> , 2023 & (Lindquist <i>et al.</i> , 2022).
	<i>Exemplos de Falhas por Falta de Requisito</i>	Falhas em garantir a segurança, privacidade, confiabilidade e precisão podem levar a ataques cibernéticos, roubo de dados, mau funcionamento e outras consequências (Stergiou <i>et. al.</i> , 2018) & (Ge <i>et. al.</i> , 2018).

**Fonte:** Autoria própria

### 3.2.2 Análise sobre Qualidade de Software em IoT

Além da engenharia de requisitos, outro tema fortemente discutido na literatura refere-se à qualidade de software em sistemas IoT. Esta abordagem é considerada fundamental, uma vez que impacta diretamente a confiabilidade, segurança, usabilidade e eficiência das soluções desenvolvidas.

Diversos autores exploraram essa temática em seus estudos, propondo diretrizes para assegurar níveis adequados de qualidade em aplicações IoT. De acordo com Tyagi *et al.* (2018), Atzori, Iera e Morabito (2010) e Kaleem *et al.* (2019), a confiabilidade é um atributo central, visto que sistemas IoT operam em ambientes distribuídos e dinâmicos, nos quais falhas podem comprometer seriamente a coleta e o processamento de dados. A manutenção da integridade e consistência das informações, bem como a minimização de falhas, são aspectos importantes para garantir a confiança dos usuários e a eficiência dos sistemas.

A segurança, conforme destacam Alaba *et al.* (2018) e Stergiou *et al.* (2018), é igualmente prioritária, considerando que dispositivos IoT frequentemente operam em redes heterogêneas e são responsáveis pela manipulação de dados sensíveis. Autores ressaltam a necessidade de adotar mecanismos de proteção, como criptografia, autenticação e monitoramento contínuo, para mitigar riscos de ataques cibernéticos e violações de privacidade. A disponibilidade dos sistemas, mencionada por Kaleem *et al.* (2019) e Shah *et al.* (2021), é outro fator determinante para a qualidade. Em muitas aplicações IoT, a operação em tempo real é essencial, o que exige que os dispositivos e

serviços estejam acessíveis e operacionais de forma contínua, mesmo diante de falhas parciais ou instabilidades na infraestrutura de rede.

No que diz respeito ao desempenho, Tyagi *et al.* (2018), Minani *et al.* (2024) e Ameyed *et al.* (2023) enfatizam a importância de garantir baixa latência e alta capacidade de resposta em sistemas IoT, particularmente em cenários delicados, como automação industrial e monitoramento de saúde. O desempenho adequado depende de fatores como eficiência de processamento, otimização da comunicação e gerenciamento inteligente de recursos.

A usabilidade também se destaca como um aspecto relevante para a qualidade do software em IoT. Alaba *et al.* (2018) e Karkouch *et al.* (2016) defendem que interfaces simples, intuitivas e acessíveis são essenciais para promover a aceitação das soluções pelos usuários, especialmente em contextos com diversidade de perfis e níveis de familiaridade tecnológica. Além disso, a precisão dos dados coletados e processados é outro aspecto enfatizado na literatura (Kaleem et al., 2019), pois informações imprecisas ou inconsistentes podem comprometer a tomada de decisão e a confiabilidade geral do sistema. Estratégias de calibração de sensores e validação dos dados são fundamentais para assegurar a integridade das informações.

Por fim, os autores também apontam a utilidade das informações geradas como um fator chave para a qualidade em IoT (Tyagi *et al.*, 2018). Não basta apenas coletar dados; é necessário que esses dados sejam relevantes e que resultem em insights açãoáveis, capazes de agregar valor aos usuários e às organizações que adotam as soluções IoT. De forma geral, a análise da literatura revela um consenso sobre a importância de garantir uma abordagem sistêmica e integrada para a qualidade de software em sistemas IoT.

Os atributos discutidos — confiabilidade, segurança, disponibilidade, desempenho, usabilidade, precisão e utilidade — representam pilares que devem ser contemplados em todas as etapas do ciclo de vida dos sistemas, desde a concepção até a operação contínua. A Tabela 5 apresenta uma síntese consolidada dos principais aspectos de qualidade de software em IoT identificadas na revisão da literatura.

**Tabela 5** – Aspectos de Qualidade de Software

<i>Dimensão</i>	<i>Justificativa na Literatura</i>
<i>Confiabilidade</i>	Os dispositivos IoT devem funcionar de forma confiável e consistente, sem falhas frequentes ou interrupções (Tyagi, H <i>et al.</i> , 2018).
<i>Segurança</i>	Os dispositivos IoT devem ser seguros contra-ataques cibernéticos e proteger os dados coletados (Alaba <i>et al.</i> , 2018).
<i>Disponibilidade</i>	Os dispositivos IoT devem estar disponíveis para uso quando necessário (S. Kaleem <i>et al.</i> , 2019).
<i>Desempenho</i>	Os dispositivos IoT devem ter um bom desempenho, com latência e tempo de resposta baixos (Tyagi, H <i>et al.</i> , 2018).
<i>Usabilidade</i>	As interfaces dos dispositivos IoT devem ser fáceis de usar e entender (Alaba <i>et al.</i> , 2018).
<i>Precisão</i>	Os dados coletados pelos dispositivos IoT devem ser precisos e confiáveis (Kaleem <i>et al.</i> , 2019).
<i>Utilidade</i>	Os dados coletados pelos dispositivos IoT devem ser úteis e relevantes para o usuário (Tyagi, H <i>et al.</i> , 2018).

**Fonte:** Autoria própria

### 3.2.3 Discussão Sobre a Revisão da Literatura

A análise conjunta dos artigos revisados em engenharia de requisitos (Seção 3.2.1) e qualidade de software (Seção 3.2.2) evidencia que há uma relação direta e crítica entre a maturidade dos requisitos e a qualidade das soluções IoT. Os autores revisados convergem ao demonstrar que um processo estruturado e abrangente de levantamento de requisitos tem impacto direto não apenas na funcionalidade e segurança das soluções, mas também na sua usabilidade, interoperabilidade, desempenho e confiabilidade.

Autores como Costa *et al.* (2017), Kaleem *et al.* (2019), Almeida, Peres & L’Erario (2022), Nakajima & Komiya (2019), Lindquist *et al.* (2022), Ge *et al.* (2018), Shital *et al.* (2023), Stergiou *et al.* (2018), Paul *et al.* (2017), Perez-Castillo *et al.* (2018) e Banerjee & Sheth (2017) ressaltam que um levantamento de requisitos bem conduzido

em IoT deve considerar não apenas aspectos técnicos, mas também as expectativas dos usuários e a gestão dos conflitos entre diferentes camadas dos sistemas.

Já, aspectos como a funcionalidade, a segurança e a experiência do usuário emergem como elementos importantes, cuja ausência compromete diretamente a qualidade global das soluções.

De forma complementar, autores como Tyagi *et al.* (2018), Alaba *et al.* (2018), Kaleem *et al.* (2019), Atzori, Iera e Morabito (2010), Stergiou *et al.* (2018), Shah *et al.* (2021), Minani *et al.* (2024), Ameyed *et al.* (2023) e Karkouch *et al.* (2016) reforçam que a avaliação da qualidade em serviços IoT precisa contemplar, de maneira integrada, aspectos como confiabilidade, segurança, disponibilidade, desempenho, usabilidade, precisão e utilidade. Tais atributos não podem ser efetivamente garantidos sem uma engenharia de requisitos que antecipe e incorpore essas necessidades desde as fases iniciais do desenvolvimento.

A partir da síntese das contribuições revisadas, torna-se evidente que um levantamento de requisitos abrangente e iterativo permite atender de forma mais eficaz às necessidades e expectativas dos *stakeholders*, abrangendo usuários finais, gestores e técnicos. Isso se traduz em maior satisfação do cliente, melhor usabilidade e maior taxa de adoção das soluções (Almeida, Peres & L'Erario, 2022). Adicionalmente, a definição clara e precisa dos requisitos desde o início do projeto reduz a ocorrência de falhas de design, erros de implementação e retrabalho, contribuindo para a otimização de custos e cronogramas (Kaleem et al., 2019).

Outro ponto identificado é que a consideração explícita de requisitos relacionados à segurança e confiabilidade desde a concepção do sistema é um fator determinante para a robustez das soluções IoT (Alaba *et al.*, 2018; Tyagi *et al.*, 2018). Por fim, um levantamento de requisitos estruturado também facilita a integração com sistemas heterogêneos, promovendo interoperabilidade e padronização, aspectos fundamentais no ecossistema dinâmico da IoT (Alaba *et al.*, 2018).

A Tabela 6 a seguir apresenta uma síntese das principais constatações observadas nesta discussão, consolidando as contribuições identificadas na literatura em relação à engenharia de requisitos e à qualidade de software para sistemas IoT.

Tabela 6 – Melhorias Baseadas em Eng. Requisitos e Qualidade de Software

<i>Constatações</i>	<i>Descrição</i>	<i>Citação de Autores</i>
Atender às necessidades dos stakeholders	Garante que as soluções IoT atendam às expectativas de usuários finais, gestores e técnicos.	Maior satisfação do cliente, melhor usabilidade e adoção mais rápida das soluções (Almeida, Peres & L'Erario., 2022).
Reducir falhas e retrabalho	Evita falhas de design, erros de implementação e retrabalho desnecessário, diminuindo custos e otimizando o tempo de desenvolvimento.	Diminuição de custos e otimização do tempo de desenvolvimento (Kaleem <i>et al.</i> , 2019).
Melhorar a segurança e confiabilidade	Define medidas de proteção adequadas para garantir a segurança dos dados e a confiabilidade das soluções IoT.	Maior segurança dos dados e confiabilidade das soluções IoT (Tyagi, H <i>et al.</i> , 2018).
Promover a interoperabilidade	Facilita a integração de soluções IoT com diferentes sistemas e plataformas, promovendo a interoperabilidade e a padronização.	Maior interoperabilidade e padronização das soluções IoT (Alaba <i>et al.</i> , 2018).

**Fonte:** Autoria própria

Além disso, ao analisar de forma transversal os métodos e *frameworks* identificados na literatura, observa-se que a maioria das abordagens se concentra predominantemente na elicitação de requisitos e na garantia de qualidade, com ênfase em soluções voltadas à entrega rápida e à satisfação do usuário. Embora algumas propostas contemplam aspectos como segurança e interoperabilidade, ainda há uma lacuna perceptível quanto à adoção de abordagens que integrem, de maneira sistêmica, as diversas dimensões de qualidade e requisitos no ciclo de vida completo das soluções IoT.

Com o intuito de oferecer um panorama consolidado sobre os trabalhos analisados, a Tabela 7 apresenta uma síntese comparativa das características dos estudos revisados, considerando as seguintes dimensões: qualidade dos dados, segurança, usabilidade, engenharia de requisitos, aplicações, sistemas de monitoramento, tecnologias emergentes e *frameworks/modelos*.

**Tabela 7** – Síntese dos Trabalhos Analisados

<b>Referência</b>	<b>(QD)</b>	<b>(S)</b>	<b>(U)</b>	<b>(ER)</b>	<b>(A)</b>	<b>(SM)</b>	<b>(TE)</b>	<b>(FM)</b>
Noorzadeh <i>et. al</i> (2024)	X			X	X		X	
Plageras <i>et. al</i> (2018)	X	X				X	X	X
Aaqib, M <i>et. al.</i> (2023).		X	X		X	X		
Aimad Karkouch <i>et. al.</i> (2016)	X			X			X	
Ameyed, D. <i>et.al.</i> (2023)		X	X	X		X	X	
Costa, <i>et. al.</i> (2016)	X	X		X	X	X	X	
Costa, <i>et. al.</i> (2017)	X	X	X			X		X
Ahmed <i>et. al.</i> (2019)	X		X	X		X	X	X
Perera <i>et. al.</i> (2014)	X	X		X	X		X	X
Stergiou <i>et. al.</i> (2018)	X		X	X	X	X	X	X
Almeida, Peres e L’Erario (2022)	X		X	X	X	X		
Alaba, <i>et. al.</i> (2017)		X		X			X	X
Minani <i>et. al.</i> (2024)	X	X		X	X	X		
Shah <i>et. al.</i> (2021)	X	X		X		X	X	X
Khanna, A & Kaur, S (2020)		X		X	X	X	X	
Atzori, Iera e Morabito (2010)	X		X	X				
Médini <i>et. al.</i> (2017)		X	X		X	X	X	X
Ge <i>et. al.</i> (2018)	X		X	X	X			
Ray <i>et. al.</i> (2018)	X	X		X	X		X	
Paul <i>et. al.</i> (2017)				X		X	X	X
Perez-Castillo et al (2018)	X	X	X	X	X	X	X	
S. Kaleem, <i>et. al.</i> (2019)	X			X	X	X		X
Shital, B <i>et. al.</i> (2023)		X	X	X		X		
Nakajima <i>et. al.</i> (2019)			X		X	X	X	
Banerjee & A. Sheth, (2017)	X	X	X	X	X		X	X
Tyagi, H. <i>et. al.</i> (2020).	X	X		X	X	X	X	
Wyatt, Lindquist <i>et. al.</i> (2022)		X	X		X	X	X	
Qin, <i>et. al.</i> (2016)	X	X	X	X		X	X	X

Legenda: (QD) Qualidade dos Dados; (S) Segurança; (U) Usabilidade; (ER) Engenharia de Requisitos; (A) Aplicações; (SM) Sistemas de Monitoramento; (TE) Tecnologias Emergentes; (FM) Frameworks e Modelos

**Fonte:** Autoria própria

Em síntese, os resultados da revisão da literatura demonstram que a engenharia de requisitos bem estruturada é um fator importante para a obtenção de soluções IoT de alta qualidade, impactando diretamente aspectos técnicos e não técnicos. Essa compreensão fundamenta a proposta deste trabalho, que busca oferecer um *framework* capaz de integrar, de forma completa, as diversas dimensões identificadas como essenciais para a maturidade e qualidade dos requisitos em sistemas IoT.

### **3.3 Trabalhos Relacionados**

Esta seção apresenta os principais trabalhos relacionados identificados na revisão de literatura, com o objetivo de situar o *framework* proposto (*QualIoT*) no contexto do estado da arte. De modo a garantir uma análise mais precisa e comparável, os trabalhos foram organizados em duas categorias complementares. A primeira categoria (Seção 3.3.1) contempla estudos que propõem *frameworks* específicos e estruturados para avaliação da maturidade, qualidade de requisitos ou aspectos correlatos em sistemas IoT, permitindo assim uma análise comparativa mais direta com a proposta do *QualIoT*. A segunda categoria (Seção 3.3.2) inclui revisões de literatura e estudos gerais sobre engenharia de requisitos, qualidade de software e desafios emergentes em IoT. Embora esses trabalhos não apresentem *frameworks* formalizados ou aplicáveis diretamente como referência de comparação, eles contribuem significativamente para a fundamentação teórica e para a identificação das lacunas que o *QualIoT* busca preencher.

#### **3.3.1 Frameworks de Avaliação em IoT**

Diversos *frameworks* têm sido propostos na literatura com o objetivo de sistematizar a avaliação de requisitos, maturidade, riscos e segurança em sistemas IoT.

Nesta seção, são apresentados cinco *frameworks* selecionados, que se destacam por fornecerem abordagens metodológicas estruturadas e comparáveis ao *QualIoT* no escopo da presente pesquisa.

O *IoT Security Maturity Model* (IoT SMM), desenvolvido pelo *Industrial Internet Consortium* (IIC), constitui um modelo amplamente utilizado para avaliação da maturidade em segurança de sistemas IoT. Sua estrutura é baseada em níveis de maturidade e contempla múltiplas dimensões, incluindo governança, planejamento, tecnologia e gestão operacional. Além de fornecer diretrizes teóricas, o IoT SMM inclui um guia prático para a realização de autoavaliações em organizações que operam soluções IoT.

O *framework* *RETIoT* (*Requirements Engineering Technology for IoT*), apresentado por Valente da Silva *et al.* (2021), propõe um processo completo para a engenharia de requisitos em sistemas IoT. A abordagem contempla fases estruturadas

que vão desde a descrição de cenários e identificação de requisitos até a definição de *templates* e utilização de *checklists* para sistematizar a elicitação e validação. O RETIoT foi validado em estudos de caso práticos, destacando-se como uma contribuição relevante no campo da engenharia de requisitos.

Outro modelo de destaque é o *IoT Maturity Model* (IoT-MM), voltado para a avaliação da maturidade de adoção de tecnologias IoT, especialmente em ambientes industriais. Este *framework* considera diversas dimensões, incluindo ativos, processos, estratégia, dados, pessoas, tecnologia da informação, aspectos financeiros e produtos. Além da proposta conceitual, o IoT-MM oferece instrumentos práticos, como planilhas para autoavaliação, facilitando sua aplicação no contexto empresarial.

O *framework UCM4IoT (Use Case Modeling for IoT)*, proposto por Boutot *et al.* (2022), apresenta uma abordagem baseada em modelagem de casos de uso, com o objetivo de apoiar a elicitação e especificação de requisitos em cenários de IoT. O UCM4IoT fornece uma linguagem de modelagem específica para esse domínio, complementada por uma ferramenta textual que permite a documentação sistemática dos requisitos e sua rastreabilidade ao longo do ciclo de vida do sistema.

Por fim, destaca-se o *IoT Risk & Maturity Framework*, formulado por Griffioen e Sinopoli (2021), que integra uma abordagem de avaliação de riscos e maturidade em IoT. O *framework* fundamenta-se em uma taxonomia abrangente de ameaças e vulnerabilidades, oferecendo uma ferramenta interativa para avaliação e planejamento de ações de mitigação. Sua aplicação prática em ambientes industriais reforça a utilidade da abordagem na gestão de riscos em ecossistemas IoT.

Estes cinco *frameworks* representam diferentes perspectivas e enfoques dentro do amplo campo de avaliação de sistemas IoT. Embora cada um contribua significativamente em áreas específicas — como segurança, requisitos, maturidade organizacional ou gestão de riscos — observa-se que nenhum deles adota uma abordagem holística que integre, de forma coordenada, aspectos como qualidade dos dados, segurança, interoperabilidade, requisitos e evolução contínua. Tal lacuna reforça a originalidade e relevância da proposta do *QualIoT*, que busca justamente oferecer um *framework* abrangente e adaptável às múltiplas demandas dos sistemas IoT contemporâneos. A Tabela 8 a seguir sintetiza os principais critérios comparativos adotados entre esses cinco *frameworks* e o *QualIoT*.

**Tabela 8** – Síntese da Comparaçāo dos *Frameworks*

Framework	(QD)	(S)	(U)	(ER)	AM	GR	FP	VE
<i>IoT Security Maturity Model (IIC)</i>	Parcial	Sim	Não	Não	Sim	Sim	Sim	Sim
<i>RETIoT (Valente da Silva et al.)</i>	Não	Parcial	Parcial	Sim	Não	Não	Sim	Sim
<i>IoT Maturity Model (IoT-MM)</i>	Não	Parcial	Não	Parcial	Sim	Parcial	Sim	Parcial
<i>UCM4IoT (Boutot et al.)</i>	Não	Não	Sim	Sim	Não	Não	Sim	Parcial
<i>IoT Risk &amp; Maturity Framework</i>	Parcial	Sim	Não	Parcial	Sim	Sim	Sim	Sim
<b><i>QualIoT (Este estudo)</i></b>	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Legenda: (QD) Qualidade de Dados; (S) Segurança; (U) Usabilidade; (ER) Engenharia de Requisitos; (AM) Avaliação de Maturidade; (GR) Gestão de Risco; (FP) Ferramentas Práticas; (VE) Validação Empírica.

**Fonte:** Autoria própria

### 3.3.2 Análise Crítica dos Frameworks em Relação ao *QualIoT*

A análise dos cinco *frameworks* apresentados na Seção 3.3.1 permite identificar contribuições relevantes para o campo da avaliação de sistemas IoT, ao mesmo tempo que evidencia algumas lacunas que justificam o desenvolvimento de um framework mais integrado, como o *QualIoT*. Observa-se que a maioria dos *frameworks* se concentra em aspectos específicos ou setoriais.

O IoT Security Maturity Model e o IoT Risk & Maturity Framework, por exemplo, oferecem abordagens fundamentadas para avaliação de segurança e riscos, mas não contemplam de forma abrangente questões relacionadas à qualidade dos dados, usabilidade ou engenharia de requisitos. Já *frameworks* como o RETIoT e o UCM4IoT apresentam avanços significativos no apoio à elicitação e especificação de requisitos, mas não incorporam mecanismos estruturados para avaliação contínua de maturidade, nem ferramentas para gestão integrada de riscos e segurança.

Outro aspecto a ser considerado é a ausência, na maioria dos modelos analisados, de uma abordagem explícita para garantir a qualidade dos dados ao longo do ciclo de vida dos sistemas IoT. Essa dimensão é crítica, considerando o papel central que os dados desempenham na geração de valor em aplicações IoT. Apenas o *QualIoT*

propõe um conjunto integrado de critérios e métricas voltadas para a avaliação sistemática da qualidade dos dados. Além disso, aspectos como usabilidade e evolução contínua dos sistemas, que são fundamentais para garantir a aderência das soluções IoT às necessidades de usuários e organizações em contextos dinâmicos, são pouco explorados nos *frameworks* existentes. O *QualIoT* busca preencher essa lacuna ao incluir mecanismos de avaliação contínua e de adaptação, permitindo que as soluções IoT evoluam em consonância com mudanças tecnológicas e com a maturidade organizacional.

Finalmente, destaca-se que nem todos os *frameworks* analisados passaram por processos de validação empírica. Embora alguns tenham sido aplicados em ambientes de estudo de caso, ainda é limitada a disponibilidade de evidências práticas sobre sua efetividade em contextos diversos.

Nesse sentido, a proposta metodológica do *QualIoT*, que inclui validação por meio de um estudo de caso real, representa um diferencial importante, contribuindo para garantir a aplicabilidade e a utilidade prática do *framework*. Em síntese, a análise comparativa realizada reforça a originalidade e a relevância do *QualIoT*, ao evidenciar que sua abordagem holística e integrativa responde de maneira mais completa aos desafios complexos enfrentados no desenvolvimento e operação de sistemas IoT atuais.

A proposta aqui apresentada busca não apenas complementar as contribuições dos *frameworks* existentes, mas também avançar no sentido de oferecer uma ferramenta efetiva para apoiar a qualidade e a evolução contínua das soluções IoT. Em síntese, os trabalhos relacionados e os *frameworks* analisados demonstram avanços importantes na avaliação de aspectos específicos dos sistemas IoT, tais como segurança, engenharia de requisitos, riscos e usabilidade.

Contudo, observa-se que a maioria dessas abordagens carece de uma visão integrada que conte cole de forma sistemática a qualidade dos requisitos, a maturidade global do sistema e a evolução contínua das soluções IoT em ambientes dinâmicos. A análise realizada reforça a necessidade de um *framework* abrangente e flexível, capaz de apoiar tanto a definição quanto a avaliação e o aprimoramento dos requisitos ao longo do ciclo de vida dos sistemas IoT.

As dimensões contempladas pelo *QualIoT* foram inspiradas por princípios amplamente reconhecidos na literatura e em normas como a ISO/IEC 25010, que trata

da qualidade de produto de software. Apesar de adaptadas ao contexto específico da Internet das Coisas, muitas das categorias adotadas pelo *framework* refletem características como usabilidade, segurança, confiabilidade e manutenibilidade, promovendo alinhamento com boas práticas de engenharia de requisitos.

Nesse contexto, a seção seguinte apresenta de forma detalhada os diferenciais do *QualIoT*, evidenciando como a proposta deste estudo busca superar as limitações identificadas nos trabalhos relacionados e contribuir para o avanço do estado da arte.

### 3.4 Diferenciais de Pesquisa

Com base na análise crítica dos *frameworks* e estudos apresentados na seção anterior, torna-se evidente que ainda persistem lacunas importantes na abordagem integrada da qualidade e maturidade dos requisitos em sistemas IoT. A seção 3.4, portanto, detalha os diferenciais do *framework* *QualIoT*, concebido para superar essas limitações e oferecer uma contribuição inovadora ao estado da arte.

A análise comparativa realizada com os *frameworks* relacionados evidenciou que, embora existam propostas relevantes no campo da avaliação da qualidade e maturidade de requisitos em sistemas IoT, essas abordagens apresentam importantes limitações.

Conforme evidenciado na análise comparativa dos *frameworks* (Seção 3.3), os *frameworks* analisados tendem a focar em aspectos específicos, como segurança, análise de requisitos ou maturidade de processos, sem integrar de forma abrangente e flexível as múltiplas dimensões que caracterizam ecossistemas IoT complexos.

Além disso, a maioria das abordagens não contempla mecanismos explícitos para a personalização de critérios de avaliação nem processos que assegurem a evolução contínua dos requisitos, estes são aspectos importantes em ambientes altamente dinâmicos e heterogêneos, como os de sistemas IoT.

Diferentemente desses estudos, o *framework* *QualIoT* propõe uma abordagem holística e adaptável, que integra aspectos essenciais como qualidade dos dados, segurança, usabilidade, interoperabilidade, maturidade de requisitos e evolução contínua. Essa proposta foi fundamentada em uma revisão sistemática rigorosa da literatura e consolidada por meio de uma análise crítica dos *frameworks* existentes. O *QualIoT* busca, assim, atender às demandas reais dos projetos IoT, oferecendo suporte tanto para avaliação inicial quanto para o aprimoramento contínuo das soluções.

Outro diferencial importante reside na flexibilidade do *framework*, que permite sua adaptação a diferentes contextos e necessidades organizacionais. O *QualIoT* fornece instrumentos que possibilitam aos profissionais ajustarem as métricas e os critérios de avaliação conforme o domínio de aplicação e as particularidades de cada projeto. Isso confere ao *framework* uma aplicabilidade ampliada, alinhada com as demandas de um mercado em constante transformação. A Tabela 9 apresenta uma síntese consolidada dos principais diferenciais da proposta *QualIoT*.

**Tabela 9** – Síntese sobre os Diferenciais de Pesquisa

Diferencial	Descrição Detalhada
<i>Abordagem Holística</i>	Considera os principais aspectos do desenvolvimento de soluções IoT, desde a concepção até a implementação e avaliação. Isso garante uma visão completa do sistema e minimiza riscos.
<i>Personalização</i>	Permite adaptar a solução às necessidades específicas de cada projeto, tornando-a mais flexível e escalável. A classificação detalhada dos requisitos facilita essa personalização.
<i>Foco na Qualidade dos Dados</i>	Garante a obtenção de dados precisos e relevantes, o que se traduz em insights mais confiáveis e decisões mais assertivas. A coleta e análise cuidadosa dos dados são fundamentais para o sucesso da solução.
<i>Segurança</i>	Prioriza a proteção dos dados e a privacidade dos usuários. A inclusão da dimensão de privacidade e segurança garante que a solução esteja em conformidade com as regulamentações e as melhores práticas do setor.
<i>Evolução Contínua</i>	Permite que a solução evolua ao longo do tempo, acompanhando as mudanças tecnológicas e as necessidades emergentes. A avaliação da maturidade dos requisitos garante que a solução esteja sempre atualizada.
<i>Integração de Diferentes Aspectos</i>	Combina diferentes aspectos do desenvolvimento de soluções IoT, como coleta de dados, análise de dados e avaliação da segurança. Essa integração proporciona uma visão mais completa do sistema e facilita a identificação de oportunidades de melhoria.

**Fonte:** Autoria Própria

### 3.5 Proposta Metodológica da Pesquisa

O desenvolvimento do *framework* *QualIoT* foi orientado por uma metodologia estruturada, combinando rigor acadêmico e aplicação prática. O objetivo foi assegurar que a proposta tivesse fundamentação científica consistente, alinhamento com as necessidades de mercado e aplicabilidade em contextos reais. A metodologia foi organizada em quatro etapas principais, descritas a seguir:

- (i) Revisão Bibliográfica – Realizou-se uma análise sistemática da literatura especializada em engenharia de requisitos, qualidade de software e sistemas IoT. Essa etapa teve como finalidade mapear lacunas, identificar tendências e reunir boas práticas que orientassem a construção do framework.
- (ii) Definição do *Framework* – Com base nas evidências levantadas, foi modelado o *framework QualIoT*. Essa fase incluiu a seleção e organização das dimensões de análise, a elaboração das perguntas norteadoras, a definição de critérios de avaliação e a construção dos mecanismos de pontuação. O processo buscou garantir tanto aderência às boas práticas identificadas na literatura quanto flexibilidade de aplicação em diferentes cenários.
- (iii) Validação do Framework – O modelo proposto foi aplicado em um estudo de caso real, envolvendo diferentes dispositivos IoT. Essa etapa permitiu verificar sua eficácia prática, identificar pontos fortes e apontar ajustes necessários, assegurando consistência metodológica e utilidade em contextos aplicados.
- (iv) Disseminação dos Resultados – Por fim, os resultados obtidos foram sistematizados e compartilhados em publicações científicas e apresentações acadêmicas. Essa etapa visou contribuir para a comunidade científica, validar a relevância da proposta e fomentar discussões sobre a evolução da engenharia de requisitos em IoT.

A Tabela 10 sintetiza as quatro etapas da metodologia, destacando seus objetivos e principais tarefas.

**Tabela 10** – Proposta de Metodologia de Pesquisa

<b>Etapa</b>	<b>Descrição</b>	<b>Principais Tarefas</b>
1. Revisão Bibliográfica	Levantamento e análise da literatura científica sobre engenharia de requisitos, qualidade de software e IoT.	<ul style="list-style-type: none"> <li>- Definir a questão de pesquisa.</li> <li>- Selecionar bases de dados e <i>string</i> de busca.</li> <li>- Aplicar critérios de inclusão e exclusão.</li> <li>- Mapear lacunas e tendências.</li> </ul>
2. Definição do <i>Framework</i>	Construção do modelo conceitual do <i>QualIoT</i> , com base nas evidências identificadas.	<ul style="list-style-type: none"> <li>- Selecionar dimensões e subdimensões.</li> <li>- Elaborar perguntas norteadoras.</li> <li>- Estabelecer critérios e métricas de avaliação.</li> <li>- Definir mecanismo de pontuação e classificação.</li> </ul>
3. Validação do <i>Framework</i>	Aplicação do <i>QualIoT</i> em um estudo de caso real, com dispositivos IoT de diferentes categorias.	<ul style="list-style-type: none"> <li>- Selecionar os dispositivos avaliados.</li> <li>- Aplicar o <i>framework</i> completo e registrar os resultados.</li> <li>- Analisar dados quantitativos e qualitativos.</li> <li>- Identificar ajustes e melhorias.</li> </ul>
4. Disseminação dos Resultados	Comunicação científica e acadêmica dos resultados obtidos.	<ul style="list-style-type: none"> <li>- Elaborar artigos e relatórios técnicos.</li> <li>- Submeter a eventos e periódicos.</li> <li>- Compartilhar contribuições e limitações da pesquisa.</li> </ul>

**Fonte:** Autoria Própria

Essa organização metodológica assegura a clareza do percurso adotado e oferece condições para que o *framework QualIoT* seja compreendido não apenas como uma proposta teórica, mas também como uma solução aplicável, replicável e passível de evolução em futuros trabalhos.

### 3.6 Conclusão do Capítulo

O Capítulo 3 apresentou a revisão sistemática da literatura e os trabalhos relacionados, permitindo identificar os principais desafios, práticas e lacunas no campo da engenharia de requisitos e da qualidade de software aplicados a sistemas IoT. A análise evidenciou que, embora existam propostas relevantes, ainda há carência de frameworks integrados que contemplam múltiplas dimensões de forma abrangente, flexível e adaptável.

Além da revisão teórica, o capítulo também sistematizou os critérios metodológicos adotados nesta pesquisa. Foram descritos o processo de seleção dos estudos, os critérios de inclusão e exclusão aplicados e as etapas de análise que sustentaram a construção da proposta. A Tabela 10 organizou esse percurso metodológico em quatro etapas principais: revisão bibliográfica, definição do *framework*, validação por estudo de caso e disseminação dos resultados. Essa estrutura buscou assegurar rigor científico, transparência e replicabilidade no desenvolvimento da investigação.

A análise crítica dos *frameworks* existentes reforçou a necessidade de uma abordagem mais completa, que vá além de soluções parciais voltadas apenas para segurança, riscos ou elicitação de requisitos. A proposta metodológica aqui delineada, portanto, constitui o fio condutor da pesquisa e estabelece a base conceitual e prática para a criação do framework *QualIoT*.

Dessa forma, o Capítulo 3 não apenas consolidou a fundamentação teórica, mas também apresentou a estrutura metodológica que orientará o restante do trabalho. Essa organização garante que o *framework* desenvolvido seja coerente com o estado da arte, validado em cenário real e aplicável em diferentes contextos de IoT. O próximo capítulo detalha a proposta do *QualIoT*, descrevendo sua estrutura conceitual, suas dimensões de avaliação e o processo de cálculo do nível de maturidade.

## 4. O Framework *QualIoT*: Proposta e Estrutura

A crescente complexidade dos ecossistemas IoT impõe novos desafios para a engenharia de requisitos, tornando insuficientes as abordagens tradicionais de validação e gestão da qualidade. Como evidenciado no capítulo anterior, embora diversos *frameworks* e modelos existentes ofereçam suporte parcial para aspectos como segurança, interoperabilidade ou usabilidade, ainda persiste a necessidade de um referencial que integre essas múltiplas dimensões em uma abordagem unificada, flexível e orientada à prática. Para responder a essa lacuna, este capítulo apresenta em detalhe o *framework QualIoT*, concebido como uma solução abrangente para mensuração da maturidade e da qualidade dos requisitos em projetos IoT.

O *QualIoT* não apenas organiza e orienta a coleta de requisitos com foco em qualidade, como também atua como um instrumento de controle da maturidade. Isso significa que, ao mesmo tempo em que garante clareza e completude dos critérios avaliativos, o *framework* também permite mensurar o nível de evolução das soluções IoT analisadas, funcionando como um controlador de maturidade que evidencia pontos fortes e lacunas em cada dimensão avaliada.

O capítulo se inicia com a descrição do processo de elaboração do *framework*, apresentado na Seção 4.1, onde se discute como a análise crítica da literatura e a identificação das principais lacunas fundamentaram a concepção da proposta. Em seguida, a Seção 4.2 descreve a arquitetura geral do *QualIoT* e os princípios que regem sua estrutura conceitual e prática. A Seção 4.3 aprofunda a proposta de solução detalhada, abordando o fluxo de validação de requisitos, as perguntas norteadoras elaboradas para orientar as avaliações, o sistema de ranking e o cálculo dos níveis de maturidade, permitindo uma avaliação comparativa das soluções IoT.

### 4.1 Elaboração do Framework *QualIoT*

A concepção do *framework QualIoT* foi diretamente motivada pelas constatações extraídas da revisão sistemática da literatura e da análise crítica dos trabalhos relacionados apresentadas no Capítulo 3. A definição das dimensões que compõem o *QualIoT* foi orientada por dois critérios principais. Em primeiro lugar, buscou-se refletir as categorias de qualidade de software e engenharia de requisitos mais enfatizadas nos estudos analisados, assegurando alinhamento com as melhores práticas da área. Em

segundo, procurou-se garantir que essas dimensões fossem suficientemente abrangentes para capturar as especificidades dos sistemas IoT contemporâneos, sem comprometer a aplicabilidade prática do *framework*.

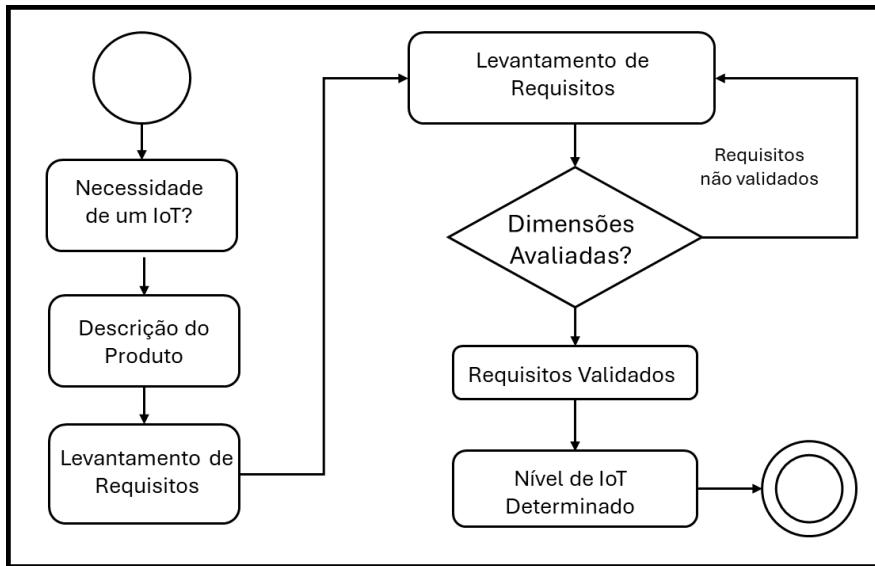
O termo “dimensão” é utilizado para representar as categorias principais de requisitos avaliados pelo *framework QualIoT*. Cada dimensão refere-se a um aspecto das soluções IoT, como segurança, privacidade ou qualidade de dados. Para evitar ambiguidade, o uso de “dimensão” neste contexto está restrito às áreas funcionais cobertas pelo modelo de avaliação proposto.

Com base nesses princípios, a estrutura do *QualIoT* foi consolidada em torno de um conjunto de dimensões e perguntas norteadoras, organizadas de maneira a cobrir aspectos técnicos e não técnicos do desenvolvimento de sistemas IoT. Além disso, foi concebido um mecanismo de pontuação e classificação que permite quantificar a maturidade dos requisitos e, consequentemente, fornecer um diagnóstico objetivo e comparável da qualidade das soluções avaliadas.

Por fim, o *framework* foi consolidado em um modelo metodológico e operacional, complementado pelo desenvolvimento do software *QualIoT*, que viabiliza sua aplicação prática e sistemática. A seguir, as próximas seções detalham a estrutura do *framework*, os componentes de sua arquitetura conceitual e as soluções propostas para garantir uma avaliação integrada e flexível da maturidade de requisitos em sistemas IoT.

## 4.2 Estrutura Conceitual do *Framework QualIoT*

O *QualIoT* foi concebido para fornecer uma abordagem sistemática e iterativa de validação de requisitos em projetos de Internet das Coisas (IoT). Sua estrutura foi desenhada para garantir que os sistemas IoT atendam aos níveis desejados de qualidade, maturidade e adequação aos requisitos de segurança, interoperabilidade, usabilidade, análise de dados e confiabilidade. A Figura 2 apresenta o Macroprocesso do *QualIoT*, que sintetiza as principais etapas que compõem este fluxo de validação.



**Figura 2.** Macroprocesso do *framework* *QualIoT*. **Fonte:** Autoria Própria

O processo tem início com a identificação da Necessidade de um IoT. Nessa etapa, busca-se entender claramente qual problema ou oportunidade de solução IoT pretende atender. É fundamental que essa necessidade esteja bem caracterizada, pois ela orientará todas as etapas subsequentes do *framework*.

Em seguida, realiza-se a Descrição do Produto. Aqui, descreve-se a solução IoT proposta, incluindo seus objetivos, o contexto de uso e as premissas técnicas iniciais. Essa descrição serve como base para que os requisitos possam ser levantados de forma consistente e alinhada com a expectativa dos *stakeholders*.

A etapa seguinte é o Levantamento de Requisitos, onde são identificados e documentados os requisitos necessários para que a solução IoT atenda à necessidade inicial. Esta etapa envolve tanto requisitos funcionais quanto não funcionais, considerando aspectos como hardware, software, comunicação, segurança e experiência do usuário.

Após o levantamento inicial, inicia-se o ciclo de Perguntas Norteadoras por Dimensão. As perguntas norteadoras, organizadas por dimensão do *framework* (como Objeto, Sensores, Transmissão, *Cloud*, Privacidade, Análise e Uso), são aplicadas para avaliar e refinar os requisitos identificados.

Cada dimensão é avaliada de forma independente, assegurando que aspectos críticos do projeto sejam analisados com profundidade. O *framework* prevê um ciclo iterativo de validação. Caso, durante a aplicação das perguntas norteadoras, algum requisito ou dimensão não seja validado, o processo retorna ao ciclo de análise e

refinamento. Esse mecanismo permite revisões contínuas, garantindo que os requisitos finais sejam completos, claros e consistentes.

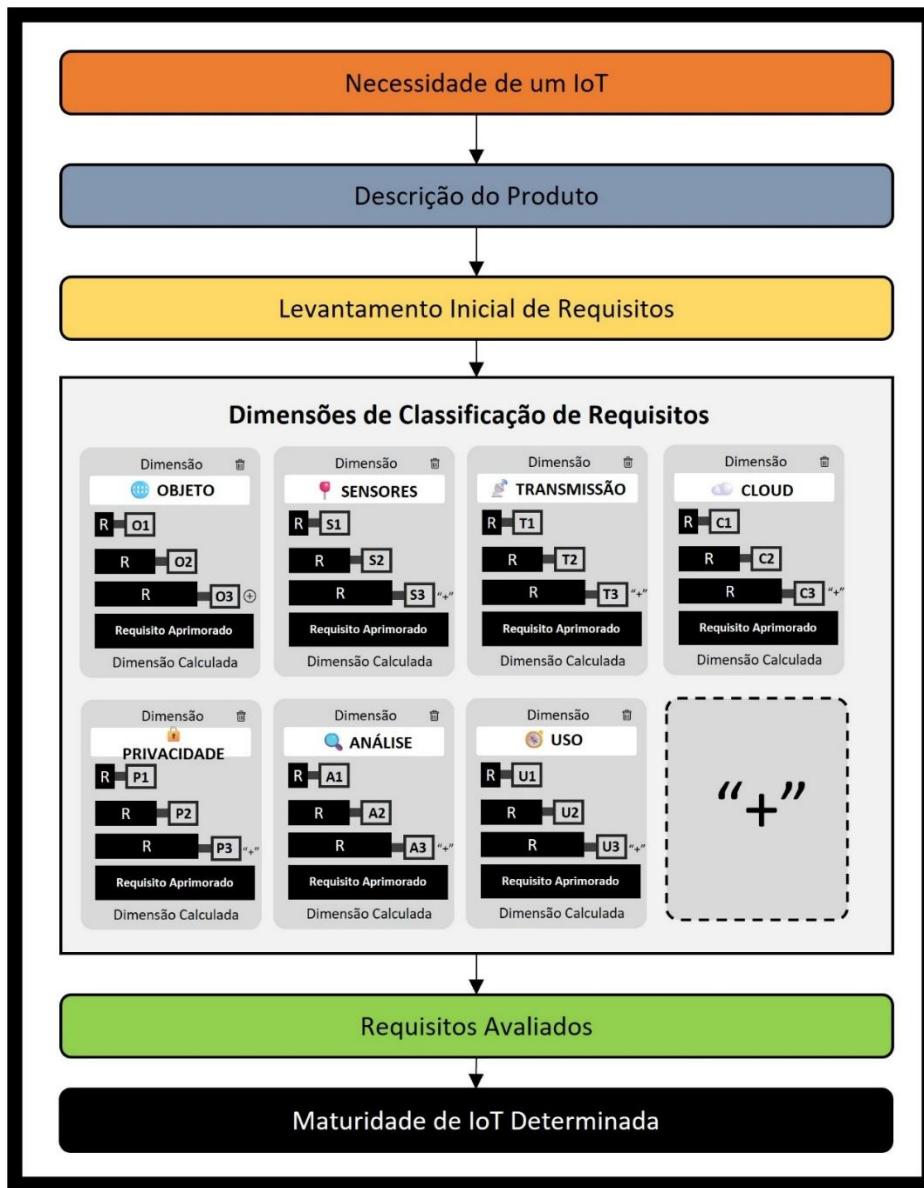
Quando todas as dimensões forem avaliadas com sucesso e os respectivos requisitos forem validados, o processo avança para a etapa de Determinação do Nível de Maturidade de IoT. Essa classificação fornece uma visão objetiva e consolidada do grau de evolução e qualidade da solução, permitindo identificar pontos fortes e áreas que demandam melhorias.

Em síntese, o macroprocesso do *QualIoT* organiza o fluxo de validação de requisitos em um ciclo iterativo e orientado a resultados, promovendo maior qualidade, maturidade e consistência no desenvolvimento de soluções IoT.

### **4.3. Estrutura Detalhada do *Framework QualIoT***

Para complementar o macroprocesso descrito anteriormente, o *framework QualIoT* conta com uma estrutura detalhada que organiza e operacionaliza a avaliação das soluções IoT.

Esta estrutura permite que cada requisito seja avaliado com base em um conjunto de dimensões cuidadosamente definidas, proporcionando uma análise granular e sistemática da maturidade da solução. A Figura 3 apresenta o detalhamento do *framework*, destacando as etapas que compõem o fluxo de avaliação e como as diferentes dimensões de requisitos são tratadas.



**Figura 3.** Detalhamento do framework *QualIoT*. **Fonte:** Autoria própria

Para mensurar a maturidade dos requisitos, o framework *QualIoT* adota uma abordagem quantitativa baseada em um índice normalizado. O cálculo do Índice Geral de Maturidade de Dispositivos IoT ( $i\_IoTM$ , General IoT Device Maturity Index) é realizado por meio da seguinte equação:  $i\_IoTM = \sum (i\_IoTQ_i \times WSd_i)$  onde:

- (i)  $i\_IoTQ_i$  (*IoT Quality Index*) representa o índice de qualidade da subdimensão  $i$ , obtido a partir da pontuação atribuída aos requisitos avaliados em uma escala de 0 a 10, posteriormente convertida para uma escala de 0 a 1;
- (ii)  $WSd_i$  (*Weight of Subdimension*) corresponde ao peso relativo da subdimensão  $i$ , calculado por meio da fórmula:  $WSd_i = w_i / \sum w_i$

(iii) Em que  $w_i$  representa o peso bruto atribuído à subdimensão  $i$ , definido com base na sua relevância no contexto de aplicação, e  $\Sigma w_i$  é a soma total dos pesos atribuídos a todas as subdimensões.

Essa abordagem de normalização assegura que diferentes subdimensões contribuam de maneira proporcional para o índice final, independentemente da quantidade de critérios utilizados ou da variação nos pesos individuais. Como diferencial, o *QualIoT* oferece um modelo adaptável a diversos cenários de avaliação, promovendo flexibilidade, comparabilidade e consistência na análise da qualidade e maturidade de requisitos em sistemas IoT. A utilização desta fórmula garante que as diferentes dimensões, independentemente de seu número ou peso original, contribuam de forma proporcional e equilibrada para o score final. Este mecanismo de normalização automática dos pesos é um diferencial do *QualIoT*, assegurando flexibilidade e consistência na avaliação de sistemas IoT com diferentes perfis e requisitos.

O processo inicia com a etapa “Necessidade de um IoT”, que consiste em compreender o propósito e o contexto de uso da solução IoT. Em seguida, realiza-se a Descrição do Produto, documentando suas características e funcionalidades previstas.

A partir dessas informações, é conduzido o “Levantamento Inicial de Requisitos”, no qual são identificados os requisitos necessários para atender à necessidade identificada. A etapa central da estrutura é a Classificação de Requisitos por Dimensões. O *QualIoT* adota um conjunto de dimensões que abrangem aspectos críticos para a qualidade e maturidade de soluções IoT. Cada dimensão é avaliada por meio de um conjunto de perguntas norteadoras e subcritérios específicos, que orientam a análise e a atribuição de pontuações. As dimensões atualmente contempladas no *QualIoT* são:

- (i) Objeto: aspectos relacionados ao item físico ou dispositivo IoT.
- (ii) Sensores: características dos sensores utilizados e sua calibração.
- (iii) Transmissão: aspectos relacionados à comunicação de dados.
- (iv) *Cloud*: armazenamento e processamento de dados em nuvem.
- (v) Privacidade e Segurança: proteção de dados e segurança da informação.
- (vi) Análise: capacidades de análise e geração de *insights*.
- (vii) Uso: experiência do usuário, usabilidade e acessibilidade.

Cada uma dessas dimensões é representada visualmente no *framework*, permitindo ao usuário visualizar o progresso e o nível de validação alcançado em cada aspecto da solução. Para cada dimensão, os requisitos são avaliados e classificados, permitindo identificar quais pontos foram plenamente validados e quais ainda necessitam de aprimoramento. A etapa “Requisitos Avaliados” consolida as informações obtidas na avaliação das diferentes dimensões. Com base nas pontuações atribuídas, é possível calcular um índice de maturidade para cada dimensão e para a solução como um todo.

Por fim, a estrutura do *framework* permite determinar a “Maturidade de IoT” da solução avaliada. Este resultado fornece uma visão objetiva e comparável do nível de maturidade da solução, servindo como base para a tomada de decisões sobre seu desenvolvimento, implementação ou necessidade de ajustes.

Essa estrutura detalhada garante que o *framework* seja flexível, adaptável e capaz de evoluir com o tempo, permitindo a inclusão de novas dimensões ou ajustes nas perguntas norteadoras, conforme as demandas do mercado e os avanços tecnológicos no campo da IoT.

Com base nesta estrutura detalhada, o *framework QualIoT* proporciona um fluxo de trabalho bem definido, que orienta o usuário desde a identificação inicial da necessidade de IoT até a avaliação final da maturidade da solução. As etapas descritas são apoiadas por um conjunto de componentes e interações que asseguram a consistência do processo e a rastreabilidade dos resultados obtidos.

Para um entendimento mais aprofundado de como o *framework* opera na prática, as subseções a seguir apresentam, de forma detalhada, cada parte do fluxo estruturado: a Seção 4.3.1 descreve o fluxo operacional completo do *framework*; a Seção 4.3.2 introduz as perguntas norteadoras que apoiam a avaliação dos requisitos; a Seção 4.3.3 discute o sistema de pontuação utilizado para mensurar a qualidade dos requisitos; a Seção 4.3.4 apresenta a pontuação por categoria e sua respectiva classificação; e a Seção 4.3.5 aborda o cálculo do nível de maturidade das soluções IoT.

### **4.3.1 Fluxo Estruturado do *Framework***

O fluxo estruturado do *framework QualIoT* organiza o processo de avaliação de requisitos de maneira sequencial e iterativa, permitindo que os diversos elementos

envolvidos no desenvolvimento de soluções IoT sejam analisados e validados de forma sistemática. Este fluxo foi concebido para garantir que todas as etapas sensíveis sejam devidamente consideradas, desde a concepção inicial até a determinação do nível de maturidade da solução. A partir do macroprocesso apresentado anteriormente, é possível observar que o fluxo abrange seis grandes momentos que se encadeiam logicamente e sustentam a proposta metodológica do *framework*.

A primeira etapa do fluxo consiste na identificação da “Necessidade de IoT”. É a partir dessa etapa que todo o trabalho de avaliação é iniciado, sendo fundamental compreender com clareza o problema a ser resolvido ou a oportunidade que se busca explorar por meio de uma solução IoT. Neste momento, os *stakeholders* devem articular os objetivos do projeto e suas expectativas, definindo o propósito central da solução a ser desenvolvida.

Em seguida, ocorre o processo de “Levantamento de Requisitos”. Nesta etapa, são coletadas informações detalhadas que irão compor o conjunto de requisitos da solução. Esse levantamento é realizado de forma colaborativa, envolvendo usuários finais, especialistas técnicos, gestores e demais partes interessadas. Os requisitos são classificados em dimensões específicas, que serão exploradas em profundidade nas subseções seguintes.

A partir do levantamento, dá-se início à etapa de “Análise das Dimensões”. Cada requisito é avaliado de acordo com as diferentes dimensões consideradas pelo *framework QualIoT* como funcionalidade, segurança, privacidade, interoperabilidade, usabilidade, entre outras. O objetivo é garantir uma análise holística que contemple todos os aspectos críticos para a qualidade da solução.

Com base nessa análise, procede-se à etapa de “Validação dos Requisitos”. Aqui, os requisitos são confrontados com os objetivos definidos na etapa inicial e verificados quanto à sua clareza, consistência, viabilidade e relevância. Essa validação é essencial para garantir que apenas requisitos bem formulados e alinhados às necessidades do projeto sejam incorporados à solução.

Após a validação, é realizada a “Mensuração da Maturidade”. Nesta etapa, os requisitos validados são avaliados quantitativamente, com base em critérios e pesos previamente estabelecidos, resultando em uma pontuação que reflete a qualidade e a

maturidade da solução IoT. Essa mensuração possibilita não apenas um diagnóstico preciso do estágio atual da solução, mas também orienta futuras ações de melhoria.

Por fim, com base nos resultados obtidos, é possível realizar a “Determinação do Nível de IoT”. A partir da pontuação consolidada, o *framework* classifica a solução em um dos níveis de maturidade propostos, oferecendo uma visão clara de seu grau de sofisticação, integração e alinhamento com as melhores práticas do mercado. Esse fluxo estruturado proporciona uma abordagem prática e replicável para o desenvolvimento de soluções IoT, apoiando as equipes de projeto na tomada de decisões informadas e na busca contínua por soluções de alta qualidade.

### 4.3.2 Perguntas Norteadoras

A seguir, apresentam-se as perguntas norteadoras que compõem o *framework QualIoT*. Essas perguntas foram organizadas em Dimensões e Subdimensões, visando apoiar a avaliação da maturidade dos requisitos em projetos IoT. As perguntas devem ser adaptadas conforme o contexto de cada solução, sendo possível incluir ou excluir perguntas e dimensões, de modo a garantir a flexibilidade e aderência da abordagem a diferentes realidades. Visando organizar a seção, a tabela 11 apresenta os elementos seguintes e sua disposição:

**Tabela 11 – Disposição das perguntas norteadoras**

Dimensão e Definições	1ª Pergunta Norteadora	2ª Pergunta Norteadora	3ª Pergunta Norteadora
-----------------------	------------------------	------------------------	------------------------

Fonte: Autoria Própria

**(i) Dimensão - OBJETO:** A dimensão Objeto aborda as características essenciais do dispositivo IoT em si — o “corpo físico” da solução. A avaliação considera aspectos como identificação única do dispositivo, capacidade de atualização remota e gestão de consumo energético, elementos fundamentais para garantir rastreabilidade, manutenção contínua e eficiência no uso de recursos.

*O1 - Pergunta norteadora:* Qual é o identificador único do objeto IoT (por exemplo, número de série ou ID de dispositivo) e como ele é gerado e gerenciado?

*O2 - Pergunta norteadora:* O objeto IoT pode receber atualizações de firmware/software? Como o processo de atualização é gerenciado?

*O3 - Pergunta norteadora:* Quais são as expectativas de consumo de energia e vida útil da bateria do objeto IoT? Existem modos de economia de energia?

**(ii) Dimensão - SENSORES:** A dimensão Sensores trata dos componentes responsáveis pela coleta de dados em um sistema IoT. Avalia-se a adequação e precisão dos sensores, bem como sua robustez frente a condições ambientais adversas, assegurando que a informação captada pelo sistema seja fidedigna e relevante.

*S1 - Pergunta norteadora:* Quais tipos de sensores são utilizados e para quais finalidades específicas?

*S2 - Pergunta norteadora:* Qual é a precisão necessária dos sensores e como a calibração é realizada e mantida?

*S3 - Pergunta norteadora:* Como os sensores lidam com variações ambientais como temperatura, umidade e interferências?

**(iii) Dimensão - TRANSMISSÃO DE DADOS:** A dimensão Transmissão de Dados refere-se aos mecanismos e protocolos utilizados para transportar as informações coletadas entre dispositivos e sistemas de *backend*. A avaliação contempla eficiência da comunicação, resiliência a falhas e gestão inteligente do uso de banda.

*T1 - Pergunta norteadora:* Quais protocolos de comunicação são suportados (por exemplo, MQTT, CoAP, HTTP, etc.) e por quê?

*T2 - Pergunta norteadora:* Como será gerenciado o uso da banda de rede, especialmente em ambientes com recursos limitados? Existem mecanismos de adaptação à variação da banda?

*T3 - Pergunta norteadora:* Existem mecanismos para garantir a entrega de dados em caso de falhas de transmissão?

**(iv) Dimensão - CLOUD (Armazenamento e Processamento):** A dimensão Cloud abrange aspectos relacionados ao armazenamento, processamento e gestão dos dados em plataformas em nuvem. Avalia-se a capacidade da solução de escalar conforme o volume de dados cresce, bem como a resiliência frente a falhas e a qualidade dos dados armazenados.

*C1 - Pergunta norteadora:* Como a solução em nuvem lida com o aumento do número de dispositivos e do volume de dados?

*C2 - Pergunta norteadora:* Quais são os planos de recuperação de desastres e continuidade de negócios?

*C3 - Pergunta norteadora:* Como será garantida a qualidade dos dados armazenados? Quais os mecanismos de validação e limpeza dos dados?

**(v) Dimensão - PRIVACIDADE E SEGURANÇA:** A dimensão Privacidade e Segurança é central em qualquer sistema IoT, dado o potencial de coleta de dados sensíveis e a ampla superfície de ataque desses ecossistemas. A avaliação examina como a solução protege os dados dos usuários, controla o acesso às informações e assegura a conformidade com normas de segurança e privacidade.

*P1 - Pergunta norteadora:* Quais medidas são adotadas para garantir a coleta, o armazenamento e o uso seguros e transparentes dos dados pessoais dos usuários, incluindo o consentimento informado e o cumprimento dos direitos dos titulares dos dados?

*P2 - Pergunta norteadora:* Como o sistema protege as informações dos usuários contra acessos não autorizados, ataques cibernéticos e perda de dados, garantindo a confidencialidade, integridade e disponibilidade das informações?

*P3 - Pergunta norteadora:* Como o sistema controla o acesso às informações, atribui permissões aos usuários e garante a rastreabilidade das ações realizadas no sistema, visando a segurança e a conformidade?

**(vi) Dimensão - ANÁLISE:** A dimensão Análise contempla o tratamento e a interpretação dos dados gerados pela solução IoT. Avalia-se a capacidade do sistema de realizar análises locais ou na nuvem, gerar *insights* para o negócio e apresentar visualizações comprehensíveis e úteis para os usuários.

*A1 - Pergunta norteadora:* Como os dados são processados e analisados? Existem capacidades de processamento de borda (*edge computing*)?

*A2 - Pergunta norteadora:* Como os *insights* são extraídos dos dados e como eles podem ser utilizados para a tomada de decisões?

*A3 - Pergunta norteadora:* Quais ferramentas de visualização são utilizadas para representar os dados de forma comprehensível para os usuários finais?

**(vii) Dimensão - USO:** A dimensão Uso refere-se à qualidade da experiência proporcionada ao usuário final da solução IoT. Considera-se a usabilidade, acessibilidade e a experiência geral do usuário ao interagir com os dispositivos, sistemas e interfaces.

*U1 - Pergunta norteadora:* O sistema oferece uma experiência intuitiva, consistente e personalizada, guiando o usuário de forma clara e eficiente desde o início da interação?

*U2 - Pergunta norteadora:* O sistema é acessível a todos os usuários, independentemente de suas habilidades ou deficiências, garantindo igualdade de acesso e uso?

*U3 - Pergunta norteadora:* O sistema é fácil de aprender, usar e eficiente para realizar as tarefas desejadas, minimizando erros e maximizando a satisfação do usuário?

Conforme apresentado no Capítulo 2, as perguntas norteadoras constituem uma técnica reconhecida para apoiar a avaliação qualitativa de sistemas complexos, como os de IoT (Lincoln & Guba, 1985; Patton, 2002; Stake, 1995). No contexto do *framework QualIoT*, essas perguntas foram estruturadas com o objetivo de garantir uma análise reflexiva e abrangente dos requisitos e funcionalidades dos sistemas IoT avaliados. Além de promover uma compreensão aprofundada das diferentes dimensões envolvidas, o uso de perguntas norteadoras facilita a triangulação de informações e o envolvimento de stakeholders, contribuindo para a robustez e a credibilidade da avaliação realizada.

A utilização das perguntas norteadoras, organizadas por Dimensões e Subdimensões, proporciona uma análise estruturada e aprofundada dos requisitos de um sistema IoT. Este processo não apenas apoia a identificação de lacunas e oportunidades de melhoria, mas também promove a uniformização da avaliação entre diferentes soluções e projetos. Dessa forma, assegura maior transparência e consistência na validação dos requisitos.

A seguir, será apresentada a proposta de mecanismo de ranking e cálculo do nível de maturidade, que complementa este processo, permitindo uma mensuração objetiva e comparativa da qualidade e da aderência das soluções IoT aos requisitos analisados.

### 4.3.3 Ranking baseados em Requisitos para IoT

Como apresentado no Capítulo 2, a utilização de rankings constitui uma prática amplamente consolidada no campo da avaliação de sistemas complexos, incluindo a Internet das Coisas (Saaty, 1980; Zanella *et al.*, 2014; Ali *et al.*, 2018). O ranking permite estruturar e comparar soluções ou componentes de forma sistemática e objetiva, promovendo não apenas uma priorização consistente de aspectos críticos, mas também uma comunicação mais clara e acessível dos resultados aos diferentes *stakeholders*. Ao incorporar essa técnica ao *framework QualIoT*, busca-se complementar a análise qualitativa realizada por meio das perguntas norteadoras com uma abordagem quantitativa que permita mensurar e comparar a maturidade de diferentes soluções IoT de maneira estruturada e replicável.

Essa abordagem está alinhada com as práticas de avaliação multicritério destacadas por Hwang e Yoon (1981), permitindo que as soluções IoT sejam avaliadas e comparadas de forma dinâmica e orientada a decisões de melhoria contínua.

No contexto do *QualIoT*, cada uma das subdimensões associadas às perguntas norteadoras recebe uma pontuação, ponderada de acordo com sua importância relativa. Dessa forma, é possível gerar um índice global para cada solução avaliada, que servirá como referência para orientar decisões de desenvolvimento, evolução e priorização de melhorias. A seguir, descreve-se o processo de construção do ranking no âmbito do *framework QualIoT*:

- (i) *Pontuação das subdimensões* — Para cada subdimensão associada às perguntas norteadoras, atribui-se uma pontuação (score) em uma escala de 0 a 10, refletindo o grau de aderência e qualidade observada naquele aspecto específico da solução.
- (ii) *Peso relativo das subdimensões* — Cada subdimensão possui um peso relativo dentro da respectiva dimensão, representando sua importância na avaliação global. Este peso pode variar entre 0,1 e 0,5, e deve ser calibrado com base em critérios técnicos ou estratégicos, conforme o contexto do projeto.
- (iii) *Cálculo da pontuação ponderada* — A pontuação ponderada de cada subdimensão é obtida pela multiplicação da pontuação atribuída pelo peso correspondente.

O somatório das pontuações ponderadas das subdimensões de uma mesma dimensão permite calcular a contribuição total daquela dimensão para o resultado final. Em seguida, os resultados das diferentes dimensões são integrados para o cálculo do Índice Geral de Maturidade do dispositivo IoT ( $i\text{-}IoTM}$ ), valor que será utilizado nas etapas seguintes do *framework*. A fórmula aplicada para cada subdimensão é:  $i\text{-}IoTQ_i = Nota_i \times WSd_i$  em que:

- (i)  $Nota_i$  é a pontuação atribuída à subdimensão  $i$  (em uma escala de 0 a 10);
- (ii)  $WSd_i$  (*Weight of Subdimension*) é o peso relativo da subdimensão  $i$ , normalizado conforme sua importância.

Como exemplo, caso uma subdimensão receba uma nota 7 e um peso de 0,3, o índice de qualidade dessa subdimensão será:  $i\text{-}IoTQ_i = 7 \times 0,3 = 2,1$

Esse cálculo é realizado de forma consistente para cada subdimensão considerada no modelo. O somatório de todas as contribuições individuais resulta no índice geral ( $i\text{-}IoTM$ ) da solução, que representa sua maturidade consolidada a partir dos requisitos avaliados.

A seguir, apresenta-se a Tabela 12, que exemplifica a aplicação prática do ranking, utilizando dados simulados para fins ilustrativos. Cabe reforçar que os pesos, dimensões e perguntas norteadoras do *framework QualIoT* foram projetados para serem flexíveis. Assim, é plenamente possível adaptar a estrutura às necessidades específicas de cada projeto, incluindo ou excluindo perguntas e dimensões, sem que isso comprometa a lógica de cálculo e análise.

**Tabela 12** – Ranking para Requisitos IoT

Dimensão	Sigla	Subdimensão	Peso	Pontuação	Observações
				(0 - 10)	
Objeto	O1	Identificação Única	3	5	Possui número de série único e gerenciado.
	O2	Capacidade de Atualização	3	7	Permite atualizações de <i>firmware/software</i>
	O3	Consumo de Energia	4	6	Baixo consumo de energia com modos de economia de energia
		<b>Subtotal</b>		<b>8,3</b>	<b>Alto</b>
Sensores	S1	Tipos de Sensores	4	8	Utiliza sensores de temperatura e umidade de alta precisão.
	S2	Precisão e Calibração	3	7	Calibração anual realizada por laboratório

					certificado.
	S3	Resiliência Ambiental	3	6	Supora temperaturas entre -10°C e 50°C e umidade entre 20% e 80%.
	<b>Subtotal</b>		<b>7,5</b>		<b>Médio</b>
Transmissão de Dados	T1	Protocolos de Comunicação	4	8	Utiliza protocolos completos e criptografia.
	T2	Gerenciamento de Banda	3	7	Aplicação de Mecanismos para variação de banda.
	T3	Estratégias de Retransmissão	3	6	Possui mecanismo de retransmissão automática em caso de falhas.
	<b>Subtotal</b>		<b>7,3</b>		<b>Médio</b>
Cloud	C1	Escalabilidade	4	8	Supora alto volume de dados com escalabilidade horizontal.
	C2	Recuperação de Desastres	3	7	Possui <i>backup</i> redundante e plano de recuperação de desastres.
	C3	Qualidade de Dados	3	6	Aplica Mecanismos de Validação dos Dados
	<b>Subtotal</b>		<b>7</b>		<b>Médio</b>
Privacidade e Segurança	P1	Privacidade e Proteção de Dados	4	8	Garante a coleta, armazenamento e uso seguros e transparentes dos dados pessoais, com consentimento informado e cumprimento dos direitos dos titulares.
	P2	Segurança da Informação	3	7	Usa Técnicas que sistema protege as informações dos usuários contra acessos não autorizados, ataques cibernéticos e perda de dados.
	P3	Gerenciamento de Acesso e Auditoria	3	6	Controla o acesso às informações, atribui permissões aos usuários e garante a rastreabilidade das ações realizadas no sistema
	<b>Subtotal</b>		<b>7</b>		<b>Médio</b>
Análise	A1	Processamento de Dados	4	4	Capacidade de processamento de borda ( <i>edge computing</i> ) para análise em tempo real.
	A2	<i>Insights</i>	3	4	Algoritmos de inteligência artificial para gerar <i>insights</i> .
	A3	Visualização de Dados	3	3	Painéis intuitivos e personalizáveis para visualização de dados.
	<b>Subtotal</b>		<b>3,7</b>		<b>Baixo</b>

Uso	U1	Experiência do Usuário	4	4	As abordagens guiam o usuário de forma clara e eficiente desde o início da interação
	U2	Acessibilidade	.3	4	O sistema é acessível a todos, independentemente de habilidades ou deficiências, garantindo igualdade de acesso.
	U3	Usabilidade	3	3	Facilidade de aprender e usar, eficiente para realizar tarefas, minimizando erros e maximizando a satisfação do usuário.
	<b>Subtotal</b>		<b>3,7</b>		<b>Baixo</b>

**Fonte:** Autoria própria

Ao final do cálculo, o ranking proporciona uma visão quantitativa e equilibrada da qualidade e maturidade da solução IoT avaliada, servindo como base para decisões de aprimoramento e evolução da arquitetura do sistema. Como etapa seguinte, será apresentada a forma como as pontuações obtidas em cada dimensão podem ser interpretadas qualitativamente, a fim de identificar com clareza os aspectos mais consolidados e aqueles que ainda requerem atenção. Esta abordagem será detalhada na próxima seção.

#### 4.3.4 Pontuação por Categoria

Após o cálculo das pontuações ponderadas de cada subdimensão e o somatório para cada dimensão, o framework *QualIoT* propõe um mecanismo adicional de interpretação qualitativa dos resultados, denominado Pontuação por Categoria. Esta abordagem complementa a avaliação quantitativa com uma classificação que facilita a compreensão e comunicação dos resultados para os diversos stakeholders envolvidos no projeto.

Como discutido no Capítulo 2, a utilização de notas e escalas é uma prática consolidada para transformar avaliações subjetivas e técnicas em indicadores quantitativos que possam ser facilmente interpretados (Likert, 1932; Trochim, 2006). Em especial no contexto de sistemas IoT, a apresentação de resultados em categorias (Alto, Médio, Baixo) permite uma análise rápida e objetiva sobre a maturidade e a aderência dos requisitos avaliados. No framework *QualIoT*, a Pontuação por Categoria é atribuída a cada dimensão com base na média ponderada das subdimensões correspondentes. A interpretação qualitativa segue os seguintes critérios:

(i) *Classificação - ALTO*: Quando a média ponderada da dimensão se encontra entre 8,0 e 10 pontos. Esta classificação indica que os requisitos avaliados na dimensão são considerados fundamentais para o sucesso da solução IoT e foram plenamente atendidos. A implementação dos itens avaliados é decisivo para garantir a confiabilidade, a segurança, a usabilidade e a experiência positiva do usuário.

(ii) *Classificação - MÉDIO*: Quando a média ponderada da dimensão se situa entre 5,0 e 7,9 pontos. Esta classificação sugere que os requisitos são importantes e que contribuem para a qualidade geral da solução, mas que podem ser aprimorados. Embora sua implementação não seja crítica para o funcionamento básico, sua melhoria trará benefícios significativos.

(iii) *Classificação - BAIXO*: Quando a média ponderada da dimensão está entre 0,0 e 4,9 pontos. Nesta situação, os requisitos avaliados possuem um impacto menos direto na funcionalidade principal da solução, sendo considerados complementares. Sua implementação deve ser priorizada conforme recursos e estratégias de evolução do sistema.

Essa categorização visa apoiar as equipes técnicas e gerenciais no processo de priorização e tomada de decisão, permitindo identificar rapidamente quais aspectos da solução estão bem consolidados e quais demandam maior atenção. Além disso, a classificação por categorias proporciona uma visão estratégica que facilita a comunicação dos resultados para públicos não técnicos, como executivos e clientes.

Por fim, destaca-se que a abordagem utilizada no *framework QualIoT* é flexível e pode ser ajustada conforme as especificidades de cada projeto. Tanto as faixas de pontuação quanto os critérios de interpretação podem ser adaptados, mantendo-se o princípio central de promover uma avaliação estruturada, comprehensível e orientada a melhorias contínuas.

### 4.3.5 Cálculo do Índice de Maturidade

Como discutido no Capítulo 2, a utilização de rankings e análise multicritério é uma abordagem consolidada na avaliação de sistemas complexos (Saaty, 1980; Hwang & Yoon, 1981; Zanella et al., 2014). No cenário da Internet das Coisas (IoT), esta técnica é particularmente eficaz, pois permite consolidar múltiplos aspectos

qualitativos e quantitativos em uma métrica única e compreensível, facilitando a tomada de decisão e a comunicação dos resultados aos stakeholders (Ali et al., 2018).

No contexto do *framework QualIoT*, o índice geral de maturidade (*i-IoTM*, *General IoT Device Maturity Index*) é construído a partir das pontuações ponderadas obtidas para cada subdimensão (vide Seção 4.3.4) e agregadas de forma normalizada. O objetivo é fornecer uma visão sintética, comparável e replicável da qualidade e maturidade dos requisitos de cada solução IoT avaliada. O processo de cálculo do índice final segue os seguintes passos:

**(i)** Cálculo do índice por subdimensão — Para cada subdimensão  $i$ , é atribuído um índice de qualidade ( $i\text{-}IoTQ_i$ ), resultante da pontuação dos requisitos avaliados em uma escala de 0 a 10, convertida posteriormente para uma escala de 0 a 1.

**(ii)** Aplicação dos pesos relativos — Cada subdimensão  $i$  possui um peso relativo ( $WSd_i$ ), refletindo sua importância na avaliação. Esse peso é calculado pela fórmula:

$$WSd_i = \frac{w_i}{\sum w_i} \quad (1.0)$$

onde  $w_i$  representa o peso bruto atribuído à subdimensão  $i$ , e  $\sum w_i$  corresponde à soma total dos pesos atribuídos a todas as subdimensões consideradas.

**(iii)** Cálculo do índice final — O índice geral de maturidade (*i\_IoTM*) é então obtido por meio da seguinte equação:

$$i\text{-}IoTM = \sum_{i=1}^N (i - IoTQ_i \times WSd_i) \quad (1.1)$$

Esta fórmula é composta pelos seguintes elementos, que detalham a lógica de cálculo do score final:

- (i)  $i\text{-}IoTQ_i$ : índice de qualidade da subdimensão  $i$ , em escala de 0 a 1;
- (ii)  $WSd_i$ : peso relativo da subdimensão  $i$ ;
- (iii)  $N$ : número total de subdimensões consideradas na avaliação.

Essa abordagem garante que o índice *i\_IoTM* seja proporcional ao desempenho observado nas diversas subdimensões, ponderado pela sua relevância no contexto da solução IoT analisada. Um aspecto importante desta metodologia é sua flexibilidade:

caso novas subdimensões sejam adicionadas, ou alguma seja removida, os pesos e o cálculo se ajustam automaticamente, mantendo a consistência e comparabilidade dos resultados. Após o cálculo do índice final, o valor (em escala de 0 a 1, ou convertido para percentual de 0% a 100%) é classificado conforme os níveis de maturidade apresentados na Tabela 13.

Tabela 13 – Níveis de Maturidade em IoT

Pontuação (%)	Nível de IoT	Descrição (Exemplo)
0 a 29%	Básico	Funcionalidades limitadas, por exemplo: apenas coleta de dados e conectividade direta.
30 a 39%	Iniciante	Funcionalidades básicas, como algumas integrações simples e análise de dados pontual.
40 a 49%	Intermediário	Funcionalidades mais avançadas, como por exemplo: integração com sistemas e análises de dados.
50 a 79%	Proficiente	Funcionalidades complexas, por exemplo: uso de IA, análise de dados aprofundada e integração com APIs.
80 a 100%	Avançado	Funcionalidades de ponta, como por exemplo: IA preditiva, personalização em tempo real e interoperabilidade ampla.

**Fonte:** Autoria própria

Como exemplo de aplicação prática, suponha que uma solução IoT avaliada tenha alcançado os seguintes subtotais por dimensão, com pesos previamente definidos:

- (i) *Dimensão Objeto*: 8,3 (peso 15%)
- (ii) *Dimensão Sensores*: 7,5 (peso 15%)
- (iii) *Dimensão Transmissão de Dados*: 7,3 (peso 15%)
- (iv) *Dimensão Cloud*: 7,0 (peso 15%)
- (v) *Dimensão Privacidade e Segurança*: 7,0 (peso 15%)
- (vi) *Dimensão Análise*: 3,7 (peso 12.5%)
- (vii) *Dimensão Uso*: 3,7 (peso 12.5%)

Aplicando a fórmula de score final:

$$t_{IoT} = \left( \frac{8,3}{10} \times 15 \right) + \left( \frac{7,5}{10} \times 15 \right) + \dots + \left( \frac{3,7}{10} \times 12,5 \right) \quad (2.0)$$

Após o cálculo completo, suponha que o score final consolidado resulte em **63,2%**. Segundo a Tabela 13, essa solução seria classificada no nível *Proficiente*,

indicando um alto grau de maturidade, com funcionalidades complexas, análise de dados avançada e integração completa.

Este processo fornece aos avaliadores e *stakeholders* uma visão quantitativa objetiva da maturidade da solução IoT, permitindo identificar de forma transparente os pontos fortes e as áreas que ainda requerem atenção ou aprimoramento. Além disso, o uso combinado de perguntas norteadoras, rankings e score final promove uma avaliação completa, que integra aspectos qualitativos e quantitativos, em consonância com as melhores práticas discutidas no Capítulo 2 (Saaty, 1980; Lincoln & Guba, 1985; Hwang & Yoon, 1981; Basili & Boehm, 2001).

Com a definição do score final de maturidade e a classificação correspondente, o *framework QualIoT* entrega aos avaliadores uma visão consolidada e objetiva sobre a qualidade e a aderência dos requisitos em soluções IoT. Essa abordagem quantitativa, complementada pelo uso de perguntas norteadoras, rankings e escalas de maturidade, possibilita uma avaliação completa e replicável, alinhada às melhores práticas de mensuração identificadas na literatura. No entanto, para que essa metodologia se torne efetivamente aplicável no contexto real de desenvolvimento e avaliação de sistemas IoT, é fundamental que ela seja operacionalizada por meio de ferramentas práticas, que viabilizem a aplicação dos conceitos e processos definidos no *framework* de forma simples e eficiente. Nesse sentido, o presente estudo também contempla o desenvolvimento de uma ferramenta de software específica concebido para apoiar a implementação prática do *framework* em projetos IoT.

## 4.7 Conclusão do Capítulo

A partir da definição do *framework QualIoT*, foram estabelecidos os elementos necessários para conduzir a avaliação da maturidade de requisitos em sistemas IoT com base em critérios estruturados e métricas quantificáveis. Para viabilizar sua aplicação em contextos práticos, foi desenvolvida uma ferramenta digital que incorpora os componentes do *framework* de forma integrada. O próximo capítulo apresenta o *Software QualIoT*, sua concepção, arquitetura e principais funcionalidades, com foco na operacionalização do modelo proposto.

## 5. Software *QualIoT*

O *Software QualIoT* foi concebido como uma ferramenta de apoio essencial para a aplicação prática do *framework QualIoT* em contextos reais de avaliação de requisitos em sistemas IoT. Sua missão é proporcionar aos projetistas, desenvolvedores e demais stakeholders um ambiente estruturado e amigável para conduzir a avaliação das soluções IoT, assegurando a consistência metodológica e a reproduzibilidade dos resultados.

Ao integrar conceitos de engenharia de requisitos, qualidade de software e métricas de avaliação, o *Software QualIoT* automatiza o processo de aplicação das perguntas norteadoras, cálculo de *rankings* e definição do nível de maturidade. Além disso, a ferramenta foi projetada para garantir flexibilidade, permitindo que usuários personalizem as perguntas, pesos e dimensões de acordo com as especificidades de cada projeto IoT. A Figura 4 a seguir apresenta a tela principal do *Software QualIoT*, destacando suas principais funcionalidades e a organização das dimensões de avaliação, oferecendo uma visão inicial do ambiente de uso da ferramenta.

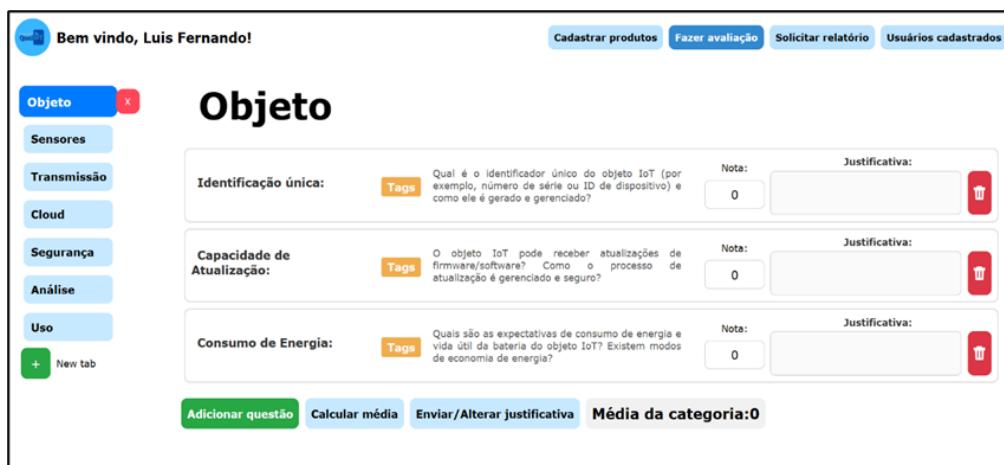


Figura 4. Tela principal do Software *QualIoT*. Fonte: Autoria própria

O desenvolvimento do Software seguiu uma arquitetura modular e escalável, com o objetivo de assegurar facilidade de manutenção e evolução futura. Também foram consideradas diretrizes de usabilidade e acessibilidade, de modo a favorecer uma experiência fluida para os diversos perfis de usuários que podem interagir com a ferramenta.

Nas seções subsequentes, serão detalhados os principais aspectos do Software *QualIoT*, abrangendo sua arquitetura técnica, modelo de funcionamento, componentes essenciais e exemplos de aplicação prática. Tal abordagem visa demonstrar como o Software materializa a proposta conceitual do *framework*, viabilizando sua aplicação em diferentes cenários de avaliação de soluções IoT.

## 5.1 Arquitetura Técnica

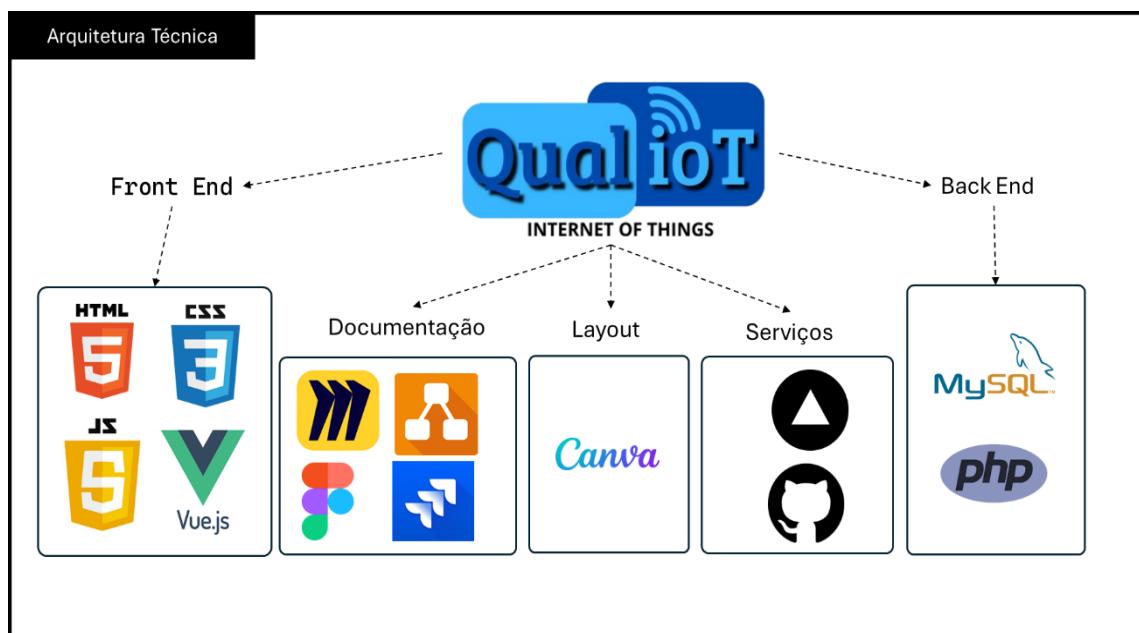


Figura 5. Arquitetura Técnica. **Fonte:** Autoria Própria

O sistema foi desenvolvido com uma arquitetura técnica atual, utilizando tecnologias e ferramentas que garantem eficiência e escalabilidade em todas as suas camadas conforme Figura 5. O sistema foi utilizando tecnologias e ferramentas que asseguram eficiência, escalabilidade e usabilidade.

O *front-end* foi construído utilizando <sup>1</sup>HTML, <sup>2</sup>CSS, <sup>3</sup>JavaScript e o *framework* <sup>4</sup>Vue.js, permitindo a criação de uma interface de usuário dinâmica, reativa e modular. Essa abordagem garante uma experiência fluida e intuitiva para os usuários. Além disso, o sistema implementa funcionalidades de exportação de relatórios em PDF e Excel, por meio de bibliotecas especializadas, assegurando a geração de documentos padronizados e acessíveis.

<sup>1</sup> HTML (HyperText Markup Language): <https://developer.mozilla.org/en-US/docs/Web/HTML>

<sup>2</sup> CSS (Cascading Style Sheets): <https://developer.mozilla.org/en-US/docs/Web/CSS>

<sup>3</sup> JavaScript: <https://developer.mozilla.org/en-US/docs/Web/JavaScript>

<sup>4</sup> Vue.js: <https://vuejs.org/>

No *back-end*, foi utilizado o <sup>5</sup>PHP para implementar a lógica de negócios e estabelecer a comunicação com o banco de dados. O <sup>6</sup>MySQL foi escolhido como banco de dados relacional, proporcionando uma estrutura sólida e eficiente para o armazenamento e a manipulação de informações, destacando-se pela confiabilidade e suporte a consultas complexas, essenciais para a robustez do sistema.

O sistema foi hospedado na plataforma <sup>7</sup>Vercel, que fornece um ambiente confiável, seguro e otimizado para a entrega de aplicações web, garantindo alta disponibilidade e um desempenho superior. O código-fonte do projeto foi versionado e armazenado no <sup>8</sup>GitHub, que facilitou a colaboração entre os desenvolvedores, o controle de versões e a rastreabilidade das alterações, elementos cruciais para a organização e a eficiência do desenvolvimento. O planejamento e a modelagem do sistema foram suportados por ferramentas colaborativas e especializadas.

O <sup>9</sup>Miro foi utilizado para mapear fluxos de trabalho e realizar o planejamento estratégico, enquanto o <sup>10</sup>Figma foi empregado para a criação de protótipos de alta fidelidade das interfaces. O <sup>11</sup>Draw.io desempenhou um papel essencial na criação de diagramas técnicos e arquiteturais detalhados, assegurando uma documentação clara e precisa dos processos e estruturas do sistema. Para o design e a criação do logotipo, foi utilizado o <sup>12</sup>Canva, que ofereceu recursos intuitivos e versáteis para desenvolver uma identidade visual e alinhada à proposta do sistema.

O gerenciamento de demandas e tarefas do projeto foi realizado por meio do <sup>13</sup>Jira, que possibilitou a organização eficiente das atividades, o monitoramento do progresso do desenvolvimento e a execução de *sprints* baseadas em metodologias ágeis. Essa abordagem integrada, combinando o uso de *Vue.js*, PHP, MySQL, Vercel, GitHub e ferramentas como Figma, Miro, Draw.io e Canva, garantiu a entrega de um sistema completo, escalável, visualmente atraente e perfeitamente alinhado às necessidades do projeto e à experiência dos usuários.

---

<sup>5</sup> PHP: <https://www.php.net/>

<sup>6</sup> MySQL: <https://www.mysql.com/>

<sup>7</sup> Vercel: <https://vercel.com/>

<sup>8</sup> GitHub: <https://github.com/>

<sup>9</sup> Miro: <https://miro.com/>

<sup>10</sup> Figma: <https://www.figma.com/>

<sup>11</sup> Draw.io: <https://app.diagrams.net/>

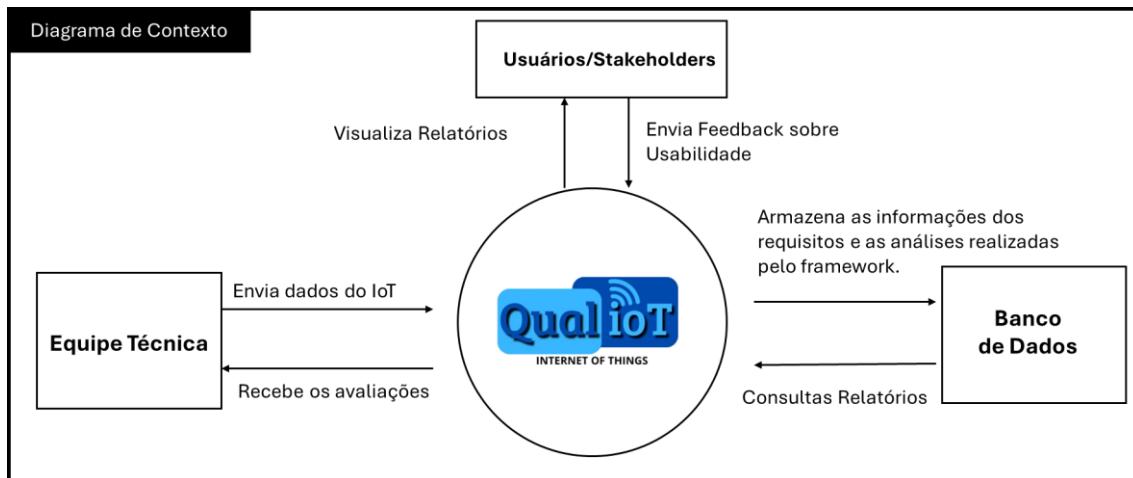
<sup>12</sup> Canva: <https://www.canva.com/>

<sup>13</sup> Jira: <https://www.atlassian.com/software/jira>

## 5.2 Contexto de Software

O framework *QualIoT* interage diretamente com a Equipe Técnica, que fornece os dados técnicos e requisitos provenientes dos sistemas IoT para análise. Em troca, o framework retorna relatórios detalhados sobre a maturidade dos requisitos avaliados, permitindo à equipe técnica realizar ajustes e tomadas de decisão baseadas em informações concretas e estruturadas.

Para facilitar o entendimento do funcionamento do framework *QualIoT*, apresentamos o diagrama de contexto (Figura 6) que ilustra suas principais interações com os atores envolvidos. Esse diagrama destaca de forma clara como o sistema se conecta com os usuários, a equipe técnica e o banco de dados, evidenciando suas funcionalidades centrais.



**Figura 6.** Diagrama de Contexto. **Fonte:** Autoria Própria

Os Usuários e *Stakeholders* têm um papel fundamental ao interagir com o sistema. Eles visualizam os relatórios gerados, obtendo insights valiosos sobre o desempenho e qualidade dos requisitos IoT. Além disso, contribuem para o aprimoramento contínuo do framework ao enviar *feedbacks* relacionados à usabilidade do sistema e à clareza das informações apresentadas nos relatórios.

O Banco de Dados serve como uma infraestrutura essencial para o armazenamento e consulta das informações geradas. Ele registra os requisitos avaliados e os resultados das análises, garantindo a rastreabilidade dos dados e possibilitando a geração de relatórios históricos. Essa estrutura centralizada permite análises comparativas ao longo do tempo, promovendo melhorias contínuas nos sistemas IoT.

avaliados pelo *framework*. O diagrama, assim, sintetiza de maneira clara e objetiva as relações entre os atores e o *framework*, evidenciando sua funcionalidade e eficiência.

### 5.3 Sitemap

Para visualizar de forma clara e estruturada a organização das funcionalidades do *software QualIoT*, a Figura 7 apresenta o sitemap do sistema. Este diagrama fornece uma visão geral das principais seções e caminhos de navegação, destacando como cada funcionalidade está hierarquicamente organizada.

O objetivo é facilitar a compreensão do fluxo de uso e evidenciar as interações que o sistema proporciona para atender às necessidades dos usuários de maneira eficiente e intuitiva.

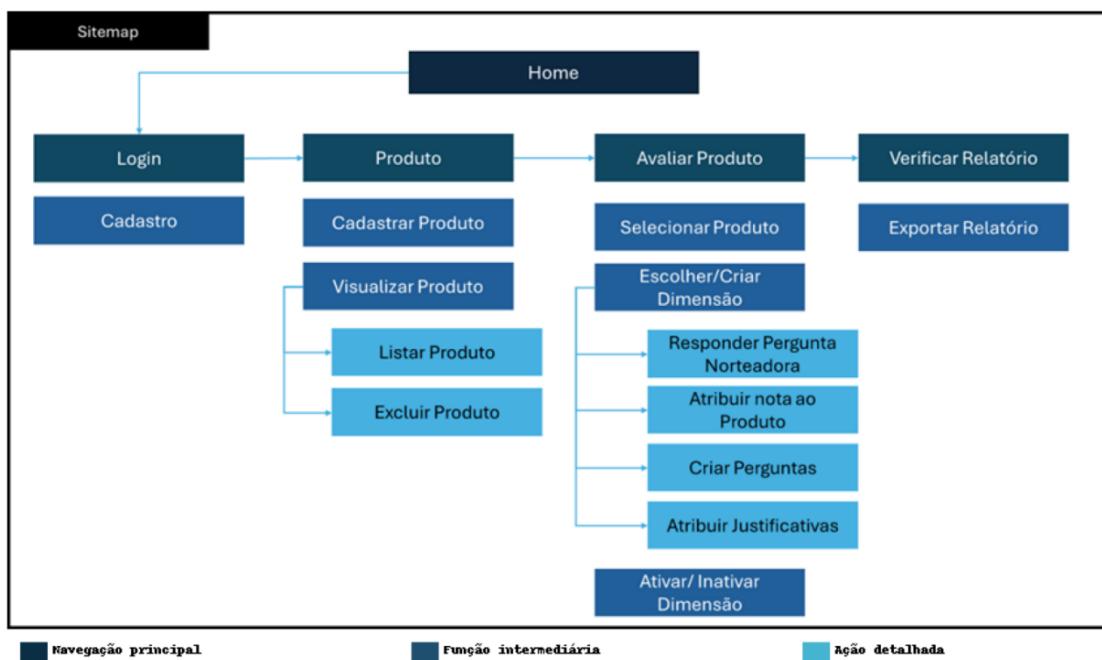


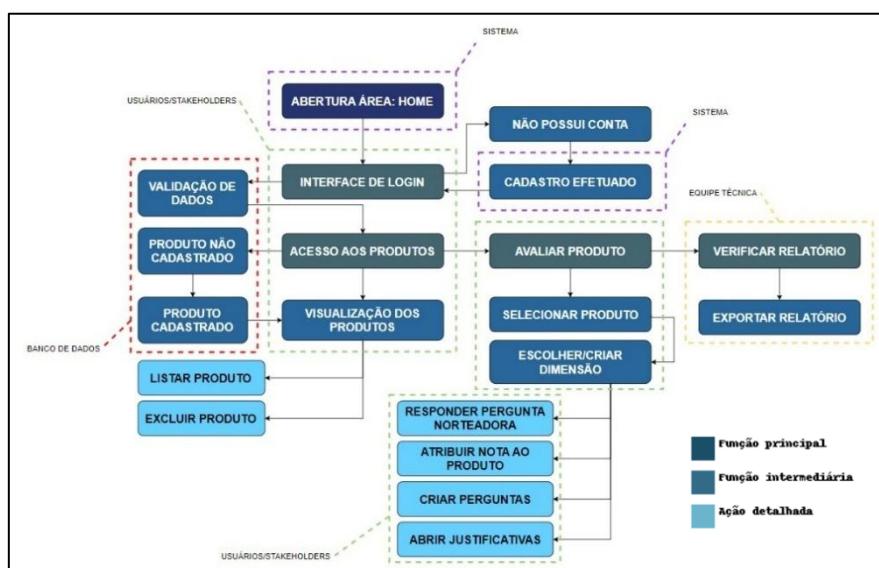
Figura 7. Sitemap. Fonte: Autoria Própria

O *sitemap* apresentado detalha a estrutura funcional do *software QualIoT*, destacando as principais seções e ações disponíveis para o usuário. Ele começa pela página inicial (*Home*), que serve como ponto de acesso central para as diversas funcionalidades do sistema, organizadas em seções como *Login*, *Produto*, *Avaliar Produto* e *Verificar Relatório*. Essa estrutura hierárquica facilita a navegação e a compreensão dos fluxos de uso, promovendo uma experiência intuitiva e eficiente.

A primeira seção, *Login*, é responsável por autenticar os usuários e fornecer acesso seguro ao sistema. Associado ao login, há a funcionalidade de Cadastro, que permite a inclusão de novos usuários ao sistema. Essa etapa inicial garante que apenas pessoas autorizadas possam acessar as funções e informações sensíveis, contribuindo para a segurança e rastreabilidade das interações. A seção *Produto* organiza as funcionalidades relacionadas ao gerenciamento dos produtos. Ela inclui opções para cadastrar novos produtos, visualizar os já cadastrados, listar os produtos disponíveis e excluir aqueles que não são mais necessários. Essa seção é essencial para manter uma base de dados atualizada, permitindo que os usuários realizem avaliações precisas e consistentes dos produtos registrados no sistema.

A funcionalidade de *Avaliar Produto* é o núcleo do sistema, permitindo aos usuários selecionarem produtos, escolher ou criar dimensões de avaliação e responder perguntas norteadoras. Os usuários podem atribuir notas aos produtos, criar novas perguntas e justificar as avaliações realizadas, assegurando um processo de análise detalhado e bem fundamentado. Complementando o fluxo, a seção *Verificar Relatório* possibilita a exportação de relatórios, garantindo que as informações coletadas possam ser compartilhadas e analisadas fora do sistema. Essa estrutura integrada destaca a flexibilidade e eficiência do *QualloT* para gerenciar e avaliar produtos de maneira abrangente.

## 5.4 Fluxograma Funcional



**Figura 8.** Fluxograma Funcional. **Fonte:** Autoria Própria

Para ilustrar de forma técnica e detalhada os principais processos do sistema de avaliação de produtos, utilizaremos um fluxograma funcional que organiza as etapas críticas do sistema, desde o acesso inicial até a exportação de relatórios. O diagrama descreve a interação entre os principais atores envolvidos, incluindo usuários, o sistema e o banco de dados, destacando as ações e decisões em cada ponto do processo. Cada bloco representa um componente operacional essencial, facilitando a análise técnica e funcional das operações. Iniciamos com a abertura da área *Home*, onde o usuário é direcionado para a interface de login. Caso não possua credenciais cadastradas, o sistema o redireciona para a etapa de criação de conta, garantindo acesso controlado. Após a autenticação bem-sucedida, o usuário pode navegar para a área de produtos, ponto central para a execução de funcionalidades relacionadas ao gerenciamento e avaliação. A partir desse ponto, o fluxo se desdobra em diversas interações, de acordo com as ações selecionadas.

Na área de produtos, o usuário pode visualizar itens cadastrados no sistema. Caso o produto desejado não esteja registrado, o fluxo segue para a validação de dados, onde o sistema verifica a disponibilidade no banco de dados. Produtos previamente cadastrados são disponibilizados para operações como listagem ou exclusão, permitindo que o usuário gerencie o catálogo de forma direta e eficiente.

Para proceder à avaliação de um produto, o usuário segue para o módulo de avaliação, que inclui a seleção do item e a escolha ou criação de dimensões personalizadas. Nessas dimensões, o usuário pode realizar ações específicas, como responder perguntas norteadoras, atribuir notas, criar perguntas adicionais ou registrar justificativas. Esse processo é projetado para garantir flexibilidade e profundidade na análise dos itens avaliados, atendendo a diferentes cenários e requisitos.

Na etapa final, os dados gerados pelas avaliações são consolidados em relatórios estruturados. O sistema, em conjunto com a equipe técnica, oferece a funcionalidade de verificação dos relatórios, permitindo que o conteúdo seja revisado antes da exportação final. Essa etapa assegura a integridade e a precisão dos dados, concluindo o fluxo com a geração de relatórios para uso externo. Este modelo funcional detalhado proporciona uma visão sistêmica e técnica das etapas e interações, viabilizando a otimização e evolução contínua do sistema.

## 5.5 Fluxo BPMN

Para demonstrar o funcionamento detalhado, utilizaremos um fluxo BPMN (*Business Process Model and Notation*). O BPMN é uma ferramenta eficiente para representar processos de forma clara e organizada, possibilitando uma visão ampla das etapas e interações entre usuários e o sistema. A Figura 9 apresenta o BPMN proposto neste projeto.

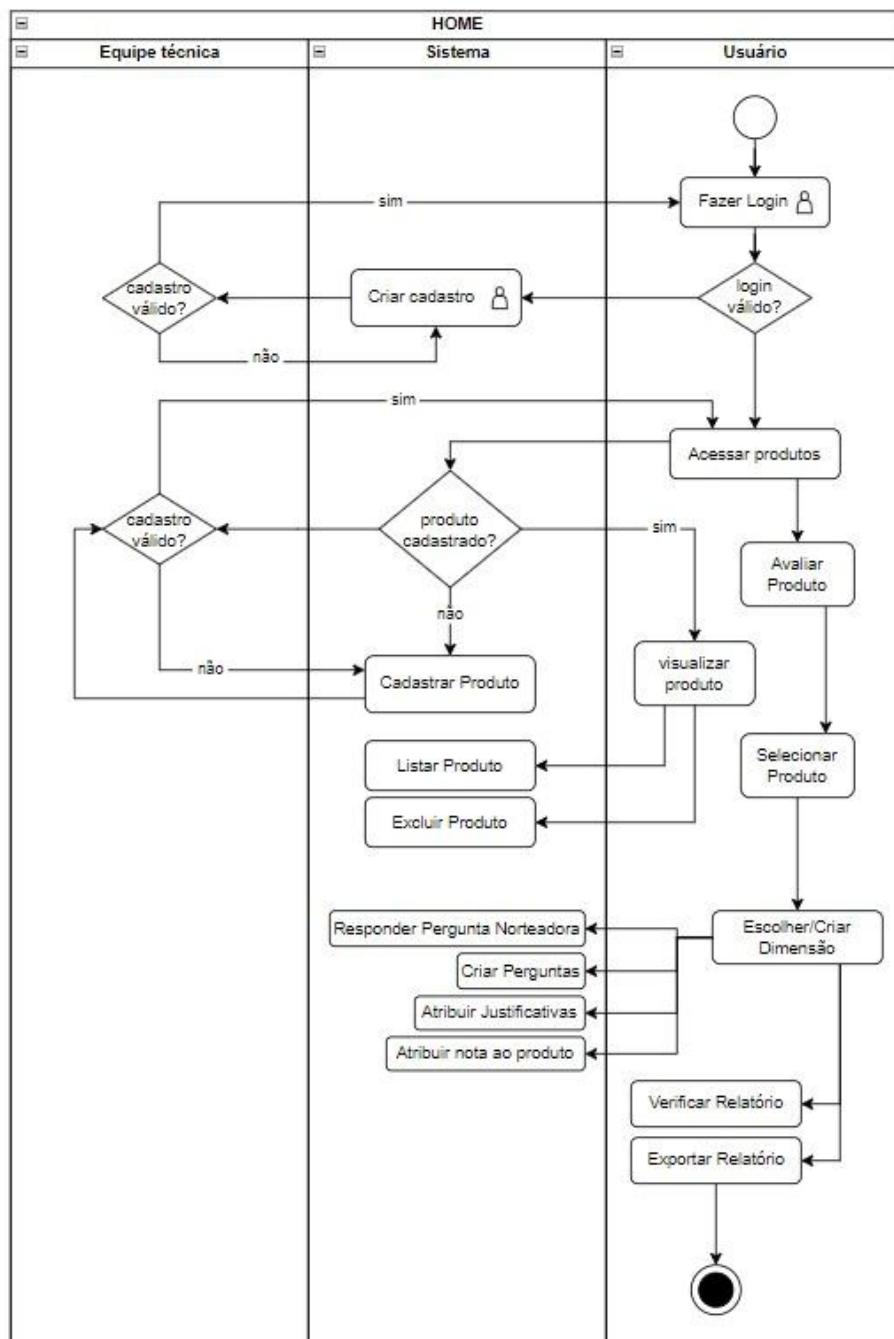


Figura 9: BPMN. Fonte: Autoria Própria

O fluxo apresentado destaca as principais ações, decisões e fluxos de informações, desde o login inicial até a exportação de relatórios. O processo inicia com o usuário fazendo login no sistema. Caso ele não tenha cadastro, é direcionado para criá-lo. Após o login, o usuário acessa a área de produtos, onde pode visualizar detalhes de itens, avaliá-los com critérios personalizáveis ou cadastrar novos produtos. Além disso, há funcionalidades para listar ou excluir produtos, promovendo uma gestão eficiente da base de dados. Em seguida, o usuário pode selecionar produtos para criar relatórios, configurando critérios de avaliação personalizados, como inclusão de perguntas normativas, justificativas ou notas atribuídas. Essas configurações tornam os relatórios mais adequados às necessidades específicas, oferecendo flexibilidade no processo de análise.

Por fim, o usuário verifica o relatório gerado antes de exportá-lo, garantindo a precisão e a completude das informações. A exportação finaliza o fluxo, permitindo o uso dos dados em outros contextos. Esse modelo BPMN proporciona uma visão abrangente e detalhada do processo, contribuindo para o alinhamento entre os envolvidos no desenvolvimento e na utilização do sistema.

## 5.6 Arquitetura Funcional

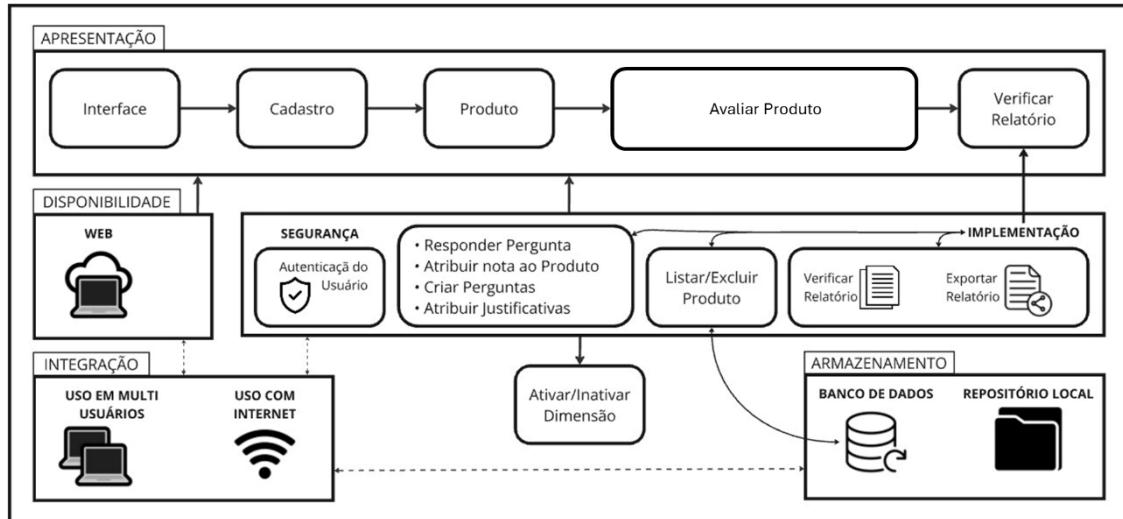


Figura 10: Arquitetura Funcional. Fonte: Autoria Própria

A arquitetura funcional apresentada na Figura 10 ilustra de maneira detalhada os componentes principais e as interações do software *QualloT*, evidenciando as camadas de Apresentação, Implementação, Disponibilidade, Integração e Armazenamento. A camada de Apresentação organiza o fluxo do usuário, desde a Interface inicial até a

funcionalidade de Verificar Relatório, destacando módulos como Cadastro, Gerenciamento de Produtos e Avaliação. Cada módulo está diretamente vinculado a funcionalidades específicas, como atribuição de notas, criação de perguntas e justificativas, garantindo flexibilidade e clareza no processo de avaliação.

Essas operações são integradas à camada de Implementação, que viabiliza ações críticas, como ativação ou inativação de dimensões e exportação de relatórios, promovendo eficiência e padronização nos resultados gerados.

A camada de Armazenamento é fundamental para a robustez do sistema, utilizando Banco de Dados e Repositório Local para gerenciar informações de forma segura e eficiente. Além disso, as camadas de Disponibilidade e Integração garantem o uso em multiusuários, conectividade com a internet e autenticação de usuários, reforçando a segurança e escalabilidade do sistema. Essa integração permite que o *QualIoT* seja acessível e funcional em ambientes colaborativos e distribuídos, atendendo às demandas de diferentes *stakeholders*. Assim, a arquitetura do sistema suporta uma abordagem modular e adaptável, capaz de evoluir conforme as necessidades de projetos IoT específicos, sem comprometer sua integridade ou usabilidade.

## 5.7 Diagrama de Caso de Uso

Diagrama de Caso de Uso apresentado detalha as principais funcionalidades do software *QualIoT* e os papéis desempenhados pelos atores envolvidos. Nele, o "Usuário" desempenha um papel central, interagindo diretamente com funções essenciais, como "Cadastrar Produto", "Avaliar Produto", "Gerar Relatório" e "Gerenciar Dados". A partir dessas ações, observa-se uma hierarquia de casos de uso relacionados, que incluem subprocessos como "Criar Perguntas", "Atribuir Notas" e "Excluir Produtos". Além disso, o sistema apresenta interações secundárias com outros atores, como "Equipe de Qualidade" e "Stakeholders", que participam do processo de validação e feedback. Essa estrutura modular permite que cada funcionalidade seja claramente definida e associada a suas dependências, como extensões e inclusões, assegurando que todas as interações entre atores e o sistema sejam comprehensíveis e bem mapeadas.

O diagrama também enfatiza a segurança e a integridade das informações através de funcionalidades relacionadas à autenticação, como "*Logar*" e "*Gerenciar Usuários*", garantindo que apenas indivíduos autorizados possam acessar os módulos sensíveis. As funcionalidades mais complexas, como "*Gerar Relatórios*" e "*Exportar Dados*", estão vinculadas a extensões, como "*Configurar Parâmetros de Exportação*", que garantem a personalização e a adaptabilidade dos resultados às necessidades dos usuários. A interação entre os módulos é representada por linhas e conectores que destacam dependências funcionais e a modularidade do sistema. Esse detalhamento demonstra a complexidade do *framework*, que incorpora boas práticas de design para viabilizar tanto operações simples quanto análises mais sofisticadas, como o uso de relatórios detalhados para tomadas de decisão.

Adicionalmente, o diagrama reflete a escalabilidade do sistema, permitindo a colaboração entre múltiplos usuários, equipes técnicas e *stakeholders*. As funcionalidades de maior impacto, como "*Revisar Requisitos*" e "*Gerar Insights*", estão conectadas diretamente aos objetivos centrais do sistema, como garantir a qualidade e maturidade dos requisitos IoT. As setas de extensão mostram como certos processos podem ser expandidos ou complementados por outros, enquanto as dependências entre casos de uso asseguram que fluxos mais complexos sejam corretamente implementados.

Por fim, o diagrama também destaca a importância de documentação e controle, permitindo que o sistema não só atenda às demandas iniciais dos usuários, mas também evolua continuamente em alinhamento com os padrões de mercado e as práticas emergentes da área.

## Diagrama de Caso de Uso

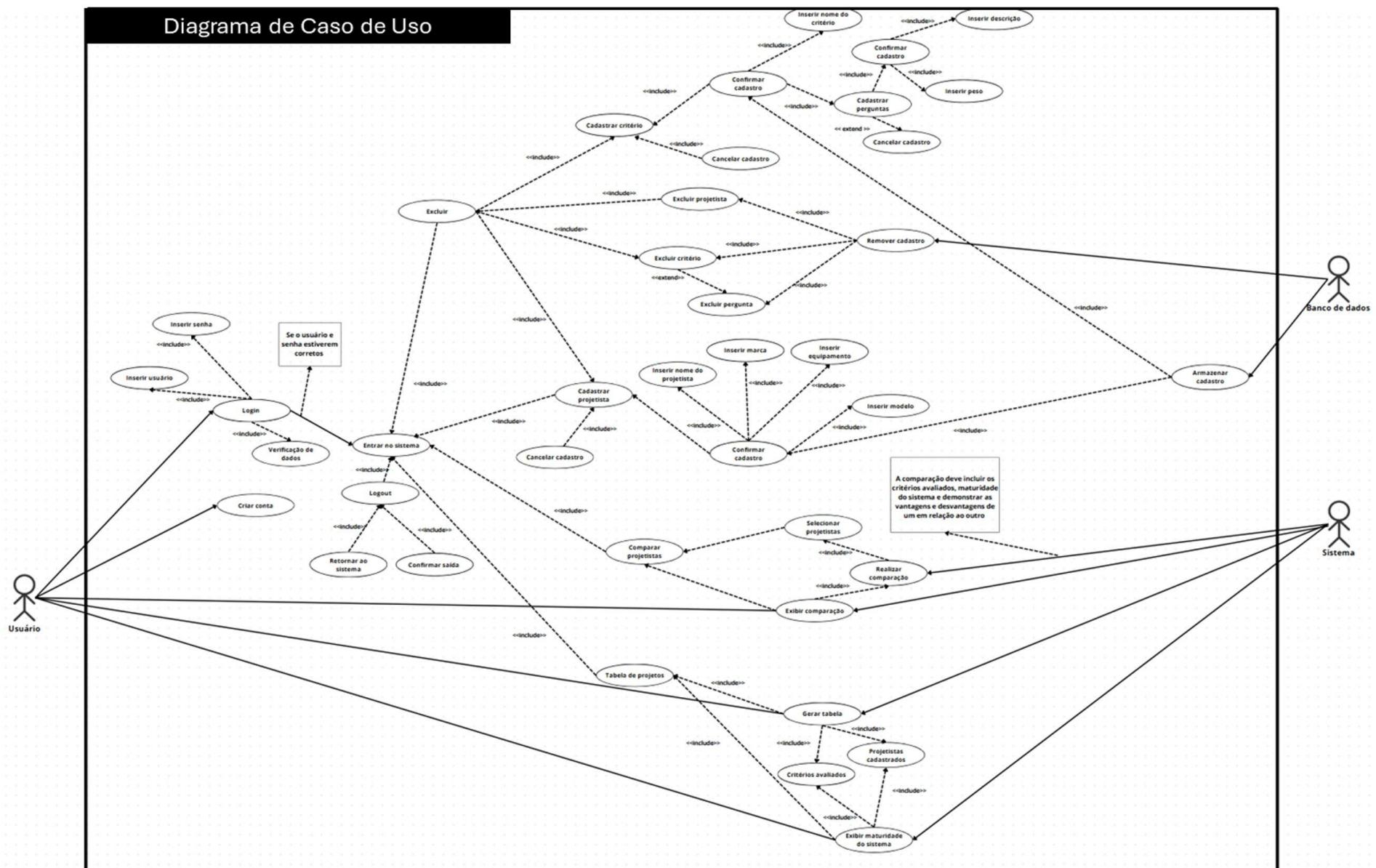


Figura 11: Diagrama de Caso de Uso. **Fonte:** Autoria Própria

## 5.8 Conclusão do Capítulo

O desenvolvimento do *Software QualIoT* representou um passo fundamental para a concretização prática do framework proposto, traduzindo conceitos teóricos em uma ferramenta aplicável, flexível e eficiente para a avaliação de requisitos em sistemas IoT. Ao longo deste capítulo, foram detalhados os principais elementos que estruturam a solução, desde sua arquitetura técnica e funcional até os diagramas de contexto, fluxos e casos de uso que dão suporte ao entendimento de seu funcionamento.

A adoção de uma arquitetura modular, o uso de tecnologias consolidadas no mercado e a integração de ferramentas de apoio ao design e ao gerenciamento de projeto garantiram não apenas a qualidade técnica do sistema, mas também sua escalabilidade e manutenibilidade. Além disso, o foco em usabilidade, acessibilidade e personalização reforça o compromisso do *QualIoT* em atender às necessidades de diferentes perfis de usuários e contextos de aplicação.

Os fluxogramas, *sitemaps*, diagramas de casos de uso e representações arquiteturais apresentados evidenciam como a ferramenta organiza suas funcionalidades de forma clara e coerente, possibilitando a realização de análises detalhadas, a geração de relatórios estruturados e a promoção de melhorias contínuas em soluções IoT.

Assim, o *Software QualIoT* consolida-se como um instrumento inovador que viabiliza a operacionalização do framework, promovendo consistência metodológica, suporte à tomada de decisão e evolução da qualidade em projetos de Internet das Coisas. Esse caráter aplicado será aprofundado nos próximos capítulos, nos quais serão explorados exemplos práticos de uso e validação da ferramenta em cenários reais.

O software está online e disponível pelo endereço: <<https://QualIoT.vercel.app>> e pode ser usado para eventuais testes de funcionamento ou funcionalidades.

## 6. Estudo de Caso

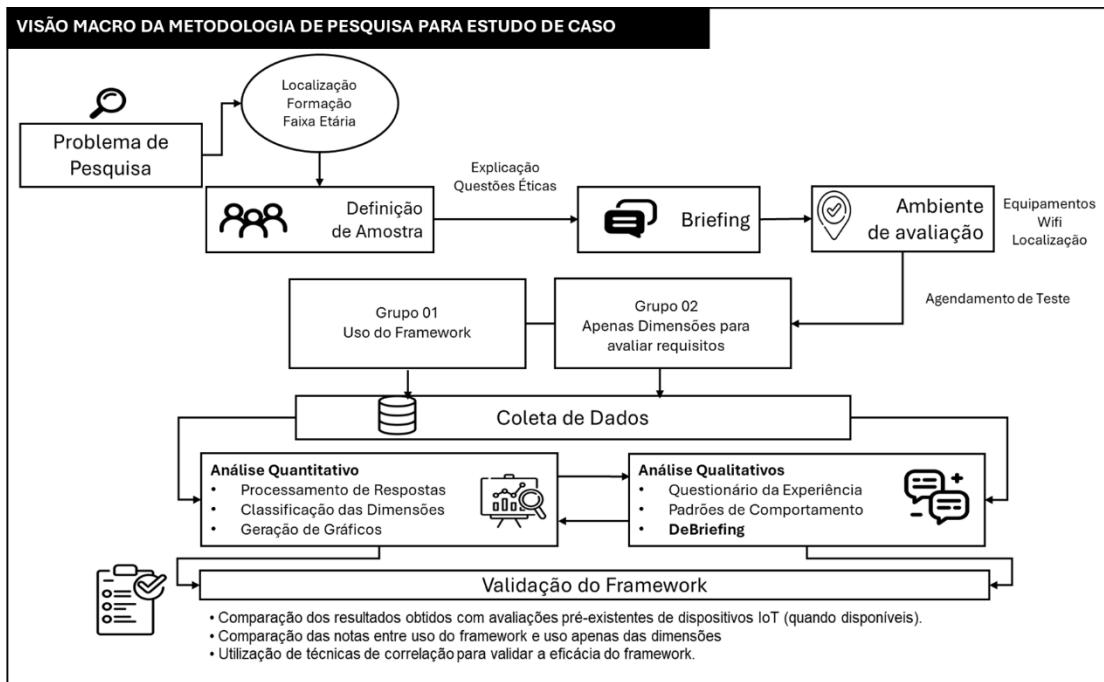
A metodologia adotada neste estudo foi desenhada com o objetivo de oferecer uma avaliação detalhada dos requisitos de sistemas de IoT, utilizando um *framework* específico que abrange sete dimensões e sua comparação com o desenvolvimento das atividades sem o uso do *framework* completo. Segundo Yin (2018), uma metodologia bem definida orienta a coleta e análise de dados, garantindo replicabilidade e contribuindo significativamente para o desenvolvimento de conhecimento completo e aplicável.

Neste estudo, foram formados dois grupos de 13 estudantes do 3º e 4º semestre no do curso de Sistemas de Informação na disciplina Análise de Sistemas das Faculdades Integradas Rio Branco. O primeiro grupo utilizou o *framework* completo para a avaliação dos requisitos IoT, enquanto o segundo grupo foi instruído a identificar apenas as dimensões do *framework* com conhecimento prévio adquirido no curso, sem o detalhamento completo das ferramentas metodológicas atreladas ao *framework* proposto. Essa divisão permitiu uma comparação direta entre os dois métodos de avaliação, verificando a eficácia do *framework* proposto em relação ao uso isolado das dimensões.

Além disso, a metodologia foi elaborada para atender às recomendações de Creswell (2014), que sugere a importância de alinhar os métodos aos objetivos específicos de cada pesquisa, especialmente em estudos envolvendo tecnologias emergentes e de alta complexidade.

A aplicação deste *framework* promove uma avaliação multidimensional, considerando não apenas variáveis técnicas, mas também fatores de usabilidade e segurança, abordando as necessidades holísticas dos sistemas IoT. Este capítulo detalha todas as etapas envolvidas, desde a definição da amostra até a coleta, análise e interpretação dos dados, considerando também as limitações metodológicas encontradas.

Para garantir uma estrutura rigorosa no estudo de caso, foi proposta uma arquitetura de visão macro apresentada na Figura 12 especificando a metodologia elaborada para este estudo.



**Figura 12:** Visão Macro da Metodologia. **Fonte:** Autoria Própria

A visão macro da metodologia de pesquisa apresentada visa proporcionar uma compreensão ampla sobre como o estudo foi estruturado para validar o *framework* proposto para avaliação de requisitos em dispositivos IoT. Este fluxo destaca as etapas essenciais, desde a formulação do problema de pesquisa até a validação do *framework*, enfatizando as estratégias de coleta e análise de dados, tanto quantitativas quanto qualitativas. Assim, o objetivo principal é estabelecer uma visão geral das conexões entre as fases do processo, evidenciando a relação entre a definição de amostra, o *briefing*, o ambiente de avaliação e a aplicação prática dos métodos de análise. Posteriormente, cada etapa será detalhada com maior profundidade, abordando os critérios específicos utilizados em cada fase.

## 6.1 Critérios de Seleção

A seleção da amostra é fundamental para assegurar a qualidade e validade dos resultados da pesquisa. Participaram 26 estudantes de Análise de Sistemas, todos com formação acadêmica homogênea em Sistemas de Informação. Segundo Patton (2015), a escolha de uma amostra homogênea é importante em pesquisas que envolvem inovação tecnológica, como é o caso da IoT, pois permite que o grupo compartilhe um nível adequado de compreensão técnica para avaliar os dispositivos. A amostra foi definida com base em critérios de formação acadêmica, faixa etária (entre 18 e 35 anos) e

localização geográfica (região metropolitana de Cotia), garantindo homogeneidade e controle sobre variáveis externas. Como destacam Maxwell (2013) e Sandelowski (1995), esses critérios facilitam a comparação das respostas e reduzem variações significativas, aumentando a confiabilidade dos resultados. Os critérios de seleção incluíram três principais eixos: formação acadêmica, faixa etária e localização geográfica. Todos os participantes estão matriculados em cursos de Sistemas de Informação reconhecidos pelo Ministério da Educação (MEC), garantindo que tenham a base técnica necessária para entender e avaliar os requisitos IoT. A faixa etária de 18 a 35 anos foi selecionada por compreender indivíduos familiarizados com tecnologias emergentes, conforme sugerido por Bryman (2016). A localização geográfica dos participantes na região metropolitana de Cotia também garantiu consistência nas condições tecnológicas e de infraestrutura, facilitando a comparação dos resultados. A população investigada se restringe aos alunos dos cursos supracitados.

## **6.2 Briefing**

Antes de iniciar o teste, foi realizado um *briefing* detalhado para os participantes. O *briefing* explicou todas as etapas da pesquisa e esclareceu os objetivos e aspectos éticos envolvidos, conforme sugerido por Israel e Hay (2006). Além disso, serão dadas instruções sobre a utilização do *framework* para o primeiro grupo e sobre as dimensões para o segundo grupo, garantindo que os participantes compreendam claramente suas funções. Os testes ocorrerão em um ambiente que simulará condições reais de uso, conforme sugerido por Bronfenbrenner (1979), com infraestrutura de rede adequada e suporte técnico durante todo o período de interação com os dispositivos IoT. Vale ressaltar que, visando a preparação dos grupos, foram conduzidos estudos de casos práticos relacionados à modelagem de requisitos em situações concretas. Essa etapa teve como objetivo ambientar os participantes na temática e reforçar a importância da aplicação prática dos conceitos, em consonância com a premissa de que a prática é essencial para a consolidação do aprendizado.

### **6.2.1 Pré-avaliação e divisão do grupo de pesquisa.**

Uma pré-avaliação (ou pré-teste) das habilidades dos alunos foi conduzida com o objetivo de garantir a formação de grupos equilibrados em termos de conhecimento e

competências relacionadas à análise de requisitos, especialmente no contexto de sistemas IoT. A avaliação foi estruturada em três partes principais: (1) conhecimento teórico de requisitos, (2) habilidade prática de especificação de requisitos e (3) análise de requisitos mal especificados.

Com essa abordagem, foi possível avaliar as competências dos alunos e formar grupos平衡ados, evitando que disparidades de conhecimento inicial prejudicassem os resultados do experimento. A aplicação da avaliação teve duração de 30 a 60 minutos, e os alunos foram classificados com base na pontuação obtida, visando uma distribuição justa e equilibrada nos grupos experimentais. Na primeira etapa, os alunos responderam a um questionário teórico que abordou temas fundamentais sobre a definição e a importância dos requisitos de software em sistemas IoT, incluindo requisitos funcionais e não funcionais, problemas comuns em requisitos mal especificados e os princípios de qualidade de requisitos (clareza, completude, verificabilidade).

A segunda etapa colocou à prova a habilidade prática dos alunos, que, diante de um cenário simples de IoT, listaram os requisitos funcionais e não funcionais do sistema, garantindo que estivessem alinhados com critérios de qualidade. Por fim, na última etapa da pré-avaliação, os alunos analisaram requisitos mal especificados, identificaram problemas de ambiguidade e inconsistência e propuseram soluções para aprimorar os requisitos fornecidos. Cada seção foi pontuada com base na clareza e profundidade das respostas, em uma escala de 0 a 10 pontos. Ao final, os alunos foram classificados como "alto", "médio" ou "baixo" em relação à sua habilidade de análise de requisitos. Com base nessa classificação, os grupos A e B foram compostos de forma a manter a distribuição proporcional de habilidades em cada grupo. Após a realização do pré-teste, os grupos foram submetidos a condições distintas: o Grupo 1 recebeu treinamento e utilizou o framework QualIoT em sua forma completa, enquanto o Grupo 2 realizou as atividades apenas com base em dimensões isoladas, sem o suporte do framework. Ao final do experimento, ambos os grupos responderam ao mesmo questionário de pós-teste, elaborado com os mesmos critérios do pré-teste, permitindo a comparação direta entre os resultados e assegurando a equivalência metodológica.

## 6.2.2 Questionário de Pré-Avaliação

O questionário foi elaborado para avaliar conhecimentos específicos e práticos relacionados à análise e especificação de requisitos em sistemas IoT. Cada questão aborda um aspecto crítico dos requisitos, com foco em conceitos teóricos, habilidades práticas e tomada de decisão. As questões foram formuladas com base em literatura científica e padrões amplamente aceitos na área de IoT e engenharia de requisitos, como os princípios de clareza, completude, verificabilidade e rastreabilidade. A Tabela 14 apresenta as perguntas, pontuação e pesos.

**Tabela 14 – Questionário de Pré-Avaliação**

Pergunta	Alternativa A	Alternativa B	Alternativa C
1. Defina requisitos funcionais e não funcionais:	Requisitos funcionais descrevem o que o sistema deve fazer; requisitos não funcionais se referem a desempenho e segurança do sistema. (Peso 8)	Requisitos funcionais descrevem funções específicas que o sistema deve executar, enquanto requisitos não funcionais abrangem características de desempenho, segurança e usabilidade. (Peso 10)	Requisitos funcionais são específicos de hardware, enquanto requisitos não funcionais são específicos de software. (Peso 2)
2. Por que é importante ter requisitos bem especificados em projetos IoT?	Para reduzir o custo do projeto, mas sem impacto direto na segurança. (Peso 3)	Porque requisitos bem especificados garantem a segurança, confiabilidade e eficiência dos sistemas IoT, evitando retrabalho e falhas. (Peso 10)	Para assegurar que todas as funcionalidades sejam implementadas da maneira mais rápida possível. (Peso 5)
3. Quais problemas são comuns em requisitos mal especificados e como podem ser evitados?	Problemas como ambiguidades e inconsistências; podem ser evitados com revisão e validação de requisitos. (Peso 10)	Atrasos no desenvolvimento; são evitados definindo prazos mais curtos para cada etapa. (Peso 4)	Problemas de comunicação com os <i>stakeholders</i> ; podem ser evitados com reuniões frequentes. (Peso 6)
4. Por que a rastreabilidade de requisitos é importante em projetos IoT?	A rastreabilidade permite acompanhar mudanças e garante a adequação do sistema às necessidades dos <i>stakeholders</i> . (Peso 10)	A rastreabilidade é uma ferramenta de documentação de processos, mas não é essencial para a qualidade final. (Peso 3)	Ela ajuda a reduzir custos no desenvolvimento e na manutenção do sistema. (Peso 5)
5. Quais seriam os requisitos funcionais de um sistema IoT que monitora temperatura e umidade?	O sistema deve monitorar e registrar a temperatura e a umidade, com alertas para valores fora do normal. (Peso 10)	O sistema deve monitorar temperatura e umidade em tempo real. (Peso 7)	O sistema deve coletar dados de temperatura e umidade sem alertas para anomalias. (Peso 4)

6. Quais seriam requisitos não funcionais para garantir o desempenho e a segurança de um sistema IoT?	O sistema deve ter um tempo de resposta rápido e implementar criptografia para segurança de dados. (Peso 10)	O sistema deve funcionar 24/7 e enviar dados com frequência regular. (Peso 6)	O sistema deve coletar e enviar dados de forma eficiente. (Peso 4)
7. Como deve ser apresentada a interface de monitoramento para os dados dos sensores?	A interface deve ser intuitiva e permitir visualização de histórico, gráficos e alertas. (Peso 10)	A interface deve exibir a temperatura e umidade em números, com opção de verificação manual. (Peso 6)	A interface deve apresentar apenas dados numéricos em tempo real. (Peso 4)
8. Quais condições devem gerar alertas no sistema ao detectar dados anômalos?	Condições de temperatura e umidade fora de um intervalo seguro, com alertas em tempo real. (Peso 10)	Quando a temperatura ou umidade atinge um nível crítico. (Peso 6)	Apenas quando o sistema detecta um erro de conexão. (Peso 2)
9. Quais são os problemas no requisito: "O sistema deve monitorar o ambiente."?	O requisito é vago; ele deveria especificar o que será monitorado (ex.: temperatura, umidade) e como. (Peso 10)	Está adequado, pois deixa espaço para adaptações futuras. (Peso 3)	É direto e cobre o objetivo do sistema. (Peso 2)
10. Proponha uma melhoria para o requisito: "O sistema deve emitir alertas de problema."	Especificando tipos de problema e métodos de alerta, como "alertas para variação extrema de temperatura por SMS e e-mail". (Peso 10)	Acrescentar apenas que o alerta será emitido em tempo real. (Peso 6)	O requisito já está claro e não precisa de melhorias. (Peso 2)
11. Qual é a importância da conectividade segura em um sistema IoT?	Impede acessos não autorizados e protege a integridade dos dados. (Peso 10)	Reduz custos de transmissão de dados. (Peso 5)	Facilita a troca de dados entre dispositivos sem necessidade de autenticação. (Peso 2)
12. Como o uso de padrões de interoperabilidade beneficia os sistemas IoT?	Permite que dispositivos de diferentes fabricantes se comuniquem de forma eficaz. (Peso 10)	Garante que todos os dispositivos utilizem a mesma interface gráfica. (Peso 4)	Aumenta a velocidade de processamento dos dispositivos. (Peso 3)

**Fonte:** Autoria Própria

### 6.2.3 Atribuição de Pesos e Classificação

Cada alternativa de resposta foi atribuída com um peso que reflete sua proximidade em relação ao conceito correto e à prática recomendada. O peso varia de 2 a 10, sendo que: *(i) 10 pontos*: Respostas completas e conceitualmente corretas, alinhadas às boas práticas de engenharia de requisitos. *(ii) 5-7 pontos*: Respostas parcialmente corretas ou incompletas. *(iii) 2-4 pontos*: Respostas incorretas ou que demonstram confusão conceitual. Os pesos foram atribuídos para diferenciar níveis de conhecimento, permitindo a identificação de lacunas específicas em conceitos e práticas dos participantes. A soma das pontuações de todas as respostas gera a nota total do participante.

Os participantes foram classificados com base na soma das pontuações de todas as respostas. A pontuação total reflete o nível de conhecimento e habilidade prática em requisitos de IoT. A classificação foi definida de acordo com faixas de pontuação, como apresentado na Tabela 15.

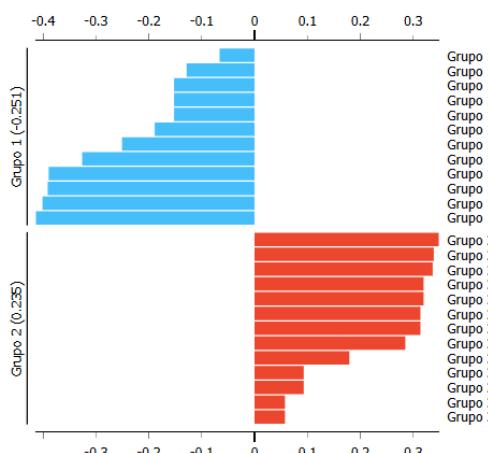
**Tabela 15 – Classificação de Pontuação**

Status	Pontos	Explicação
Projetista	120–150	Domínio avançado dos conceitos e práticas.
Profissional	100–119	Domínio intermediário, com bons conhecimentos.
Bom	70–99	Conhecimentos suficientes, mas com lacunas em práticas específicas.
Regular	40–69	Conhecimentos básicos, com muitas lacunas teóricas ou práticas.
Iniciante	0–39	Conhecimento inicial ou ausência de domínio.

**Fonte:** Autoria Própria

#### 6.2.4 Divisão dos Grupos

Cada grupo foi composto de forma que tenha a mesma quantidade de alunos de diferentes níveis de habilidade, assegurando que não haja vantagens iniciais significativas de um grupo sobre o outro. Essa abordagem de pré-avaliação traz diversos benefícios para o experimento, como a redução de vieses, a formação de grupos平衡ados e a obtenção de um diagnóstico inicial das habilidades da turma. Esse processo garantirá que os resultados do experimento reflitam a eficácia dos métodos de avaliação e não as disparidades nas habilidades dos participantes. Conforme apresenta a Figura 13:



**Figura 13:** Gráfico - Mediana de pontos na Pré-Avaliação. **Fonte:** Autoria Própria

O gráfico apresentado na Figura 13 ilustra as distribuições medianas das pontuações dos participantes entre os dois grupos. Ele está dividido em dois eixos, com o Grupo 1 destacado na parte superior e o Grupo 2 na parte inferior. As barras horizontais indicam as pontuações relativas, evidenciando que ambos os grupos possuem um equilíbrio em termos de habilidades e desempenhos.

Essa distribuição balanceada reflete diretamente o objetivo de formar grupos com perfis homogêneos em termos de níveis de habilidade, como mencionado no texto. Isso assegura que nenhum grupo tenha uma vantagem inicial significativa sobre o outro. Essa abordagem é essencial para a redução de vieses e para garantir que os resultados obtidos durante o experimento reflitam a eficácia das metodologias aplicadas, em vez de disparidades iniciais nas habilidades dos participantes. Portanto, os dados sugerem que os grupos foram bem distribuídos, garantindo a validade do experimento.

### 6.3 Ambiente de Pesquisa

A pesquisa foi realizada no laboratório de hardware das Faculdades Integradas Rio Branco, um ambiente tecnológico e controlado, visando garantir a confiabilidade e a precisão dos experimentos. O espaço foi projetado para atender às demandas de estudos avançados, com infraestrutura de ponta que incluiu computadores atuais e fontes de alimentação de alto desempenho, garantindo o suporte necessário para testes e análises.

Além disso, o laboratório contou com um sistema de climatização adequado, mantendo os equipamentos em temperaturas ideais para funcionamento e preservação, reforçando o compromisso com a qualidade e a segurança das pesquisas.

A conectividade foi um ponto importante para o sucesso da pesquisa. O laboratório estava equipado com uma rede *Wi-Fi* de banda larga de alta capacidade, oferecendo uma velocidade consistente e confiável, essencial para o processamento de dados e a comunicação entre os dispositivos. A rede foi configurada e controlada exclusivamente para os experimentos, assegurando que não houvesse interferências externas e permitindo a integração fluida entre os equipamentos avaliados. Essa infraestrutura tecnológica permitiu que as atividades fossem conduzidas de forma eficiente, refletindo a excelência do ambiente de pesquisa proporcionado pela instituição.

Durante o experimento, foram avaliados diversos dispositivos IoT representando diferentes categorias (básico, intermediário e avançado), permitindo uma análise abrangente das dimensões de requisitos consideradas pelo *framework QualIoT*. Os detalhes sobre os dispositivos e suas avaliações estão apresentados no Capítulo 7.

Cada equipamento foi testado minuciosamente em condições padronizadas, garantindo que os resultados fossem comparáveis e isentos de variáveis externas. Esse dinamismo na avaliação reforça o papel do laboratório como um espaço não apenas de aprendizado, mas de inovação, destacando-se como um local propício para a realização de pesquisas tecnológicas avançadas e de alto impacto acadêmico.

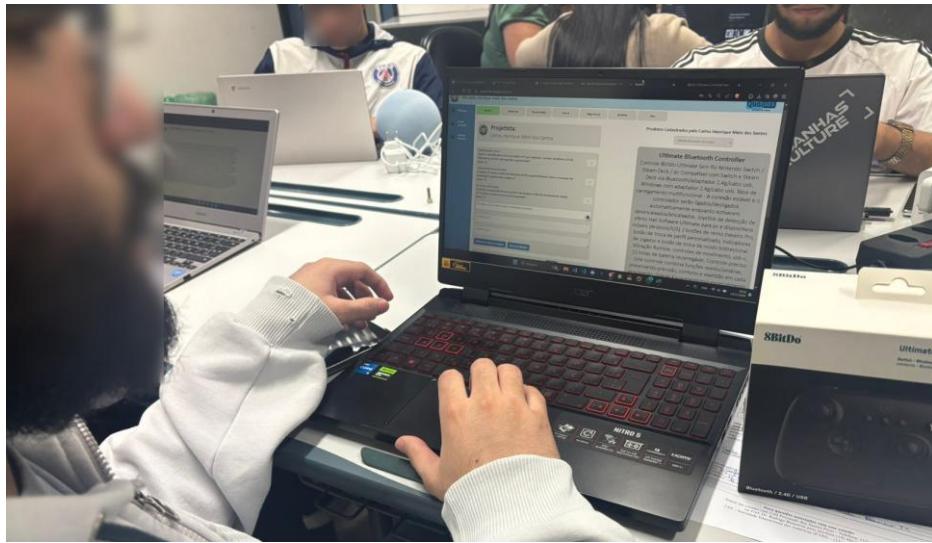
## 6.4 Coleta de Dados

A coleta de dados foi planejada em duas etapas principais, visando proporcionar uma análise abrangente e comparativa das metodologias aplicadas para avaliação de requisitos IoT. Para isso, os participantes foram divididos em dois grupos: o Grupo 1, que utilizou o *framework* completo, abrangendo as sete dimensões propostas; e o Grupo 2, que trabalhou apenas com as dimensões como um guia básico, mas sem o suporte detalhado do *framework*. Essa abordagem permitiu explorar não apenas as diferenças na aplicação prática, mas também as implicações na consistência, clareza e precisão das avaliações realizadas pelos dois métodos. A Figura 14 apresenta os participantes da pesquisa no ambiente no qual ela foi realizada.



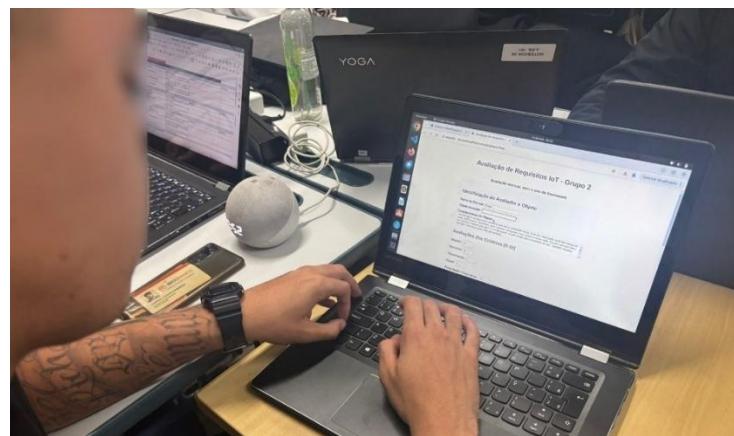
**Figura 14:** Registro Fotográfico – Participantes

O Grupo 1 teve à disposição perguntas norteadoras que guiavam suas análises, permitindo uma avaliação mais estruturada e consistente. As perguntas foram elaboradas para facilitar a identificação de pontos críticos e assegurar uma classificação coerente, promovendo uma abordagem sistemática e detalhada no levantamento de requisitos. A Figura 15 apresenta os participantes utilizando o *framework* durante a pesquisa.



**Figura 15:** Registro Fotográfico de participantes utilizando *framework* QualIoT

O Grupo 2 realizou a avaliação de forma manual, utilizando um formulário simplificado, conforme apresentado na figura 17. Como os participantes do Grupo 2 não tiveram acesso às perguntas norteadoras do *framework*, eles tiveram uma maior liberdade na classificação, mas também exigiu maior esforço cognitivo para estruturar as respostas. A Figura 16 apresenta um participante aplicando as respostas sem o uso do *framework*.



**Figura 16:** Registro Fotográfico de participantes sem o uso do *framework*

O formulário foi composto por campos abertos e notas para cada uma das dimensões, sem o suporte das diretrizes específicas, o que resultou em uma abordagem mais subjetiva. A ausência de detalhamento dificultou a padronização das respostas, levando os participantes a dependerem exclusivamente de sua interpretação individual. A Figura 17 apresenta o formulário respondido pelo grupo 2 para fazer a avaliação das soluções de IoT.

### Avaliação de Requisitos IoT - Grupo 2

Avaliação manual, sem o uso do framework

#### Identificação do Avaliador e Objeto

Nome da Pessoa:

Objeto Avaliado:

Características do Objeto:

#### Avaliações dos Critérios (0-10)

Objetos:

Sensores:

Transmissão:

Cloud:

Privacidade e Segurança:

Análises:

Uso:

#### Justificativas das Notas

Justificativa das notas (Objetos):

Justificativa das notas (Sensores):

Justificativa das notas (Transmissão):

Justificativa das notas (Cloud):

Justificativa das notas (Privacidade e Segurança):

Justificativa das notas (Análises):

Justificativa das notas (Uso):

#### Classificação Final

Escolha a Classificação Final:

Média Geral da Avaliação: 0

**Figura 17:** Formulário -Grupo 2. **Fonte:** Autoria Própria

Essa distinção de métodos foi intencional para avaliar o impacto do uso de um *framework* estruturado em contraste com uma abordagem próxima à manual, *i.e.*, sem o uso do *framework*. A Figura 18 regista de forma anonimizada, os participantes em ambientes dos grupos 1 e 2 durante o experimento.



**Figura 18:** Registro Fotográfico – Grupos de Pesquisa

Durante a coleta, foram utilizados questionários estruturados para a obtenção de dados quantitativos e a observação direta dos participantes enquanto realizavam as avaliações. A observação foi essencial para capturar comportamentos, dificuldades e estratégias adotadas por cada grupo ao interagir com os dispositivos IoT. Essa abordagem permitiu identificar, por exemplo, que o Grupo 2 frequentemente solicitava esclarecimentos sobre critérios e enfrentava desafios para justificar suas notas de forma objetiva, devido à ausência de orientações claras.

A análise dos dados coletados foi conduzida por meio de métodos quantitativos e qualitativos. Estatisticamente, foram aplicados testes como ANOVA e Teste T para verificar se existem diferenças significativas entre as médias das avaliações dos dois grupos. Esses testes ajudaram a mensurar o impacto do uso do *framework* estruturado na precisão e confiabilidade das respostas. Complementarmente, a análise qualitativa

buscou entender como os participantes do Grupo 2 lidaram com a falta de perguntas norteadoras, identificando lacunas e oportunidades de melhoria futuras.

Por fim, a triangulação foi aplicada para integrar os resultados das análises quantitativa e qualitativa, fornecendo uma visão mais completa dos fenômenos observados. Os resultados detalhados dessa análise e sua interpretação serão apresentados no próximo capítulo.

## 6.5 *Debriefing*

Após a realização dos testes, foi conduzido um *debriefing* final com os participantes, momento importante para coletar feedbacks detalhados sobre suas experiências com o *framework* e as dimensões avaliadas. Esse processo teve como objetivo compreender a percepção dos usuários em relação à aplicação prática do *framework* e identificar possíveis melhorias para torná-lo mais eficiente e aplicável em contextos futuros. A atividade foi estruturada para garantir que todos os participantes tivessem a oportunidade de compartilhar suas impressões e contribuições de forma aberta e colaborativa. O *debriefing* foi dividido em duas etapas principais.

Na primeira, os participantes preencheram um formulário estruturado, no qual puderam registrar suas opiniões de forma individual e anônima. Esse formulário incluiu questões sobre a facilidade de uso, clareza das dimensões avaliadas e possíveis dificuldades encontradas durante a aplicação do *framework*. A Figura 19 apresenta o formulário de *debriefing* apresentado ao término do experimento.

## Formulário de Debriefing de Projeto

1. Como você descreveria sua experiência geral com o projeto?

2. Quais desafios você enfrentou durante o projeto? Como lidou com eles?

3. Em uma escala de 0 a 10, como você avaliaria a comunicação na equipe?

4. Em uma escala de 0 a 10, como você avaliaria o suporte das ferramentas utilizadas?

5. Em uma escala de 0 a 10, qual foi seu nível de satisfação geral com o projeto?

6. Você recomendaria participar de projetos semelhantes no futuro?

- Sim
- Talvez
- Não

Por quê?

**Enviar Respostas**

**Figura 19:** Formulário *Debriefing*. **Fonte:** Autoria Própria

Essa etapa permitiu capturar percepções iniciais e individuais, fornecendo dados quantitativos e qualitativos para análise posterior. Na segunda etapa, foi promovida uma discussão aberta entre os participantes, criando um espaço para reflexões coletivas sobre as experiências vivenciadas. Essa discussão focou em aspectos como a praticidade do *framework*, as limitações percebidas no processo de avaliação e comparações diretas entre as abordagens utilizadas pelos dois grupos. Os participantes

puderam destacar os pontos fortes e fracos de cada método, bem como propor sugestões de melhoria para futuras implementações. A abordagem colaborativa facilitou o aprofundamento nas percepções coletivas e possibilitou uma análise mais detalhada.

A comparação dos dois grupos foi um ponto central da discussão. Essa etapa do *debriefing* destacou não apenas os resultados obtidos pelos dois grupos, mas também a relevância da interação entre os participantes para validar e enriquecer os achados da pesquisa. As percepções e feedbacks qualitativos coletados durante o debriefing também contribuíram para a interpretação dos resultados apresentados no Capítulo 6, complementando a análise quantitativa das avaliações realizadas.

## 6.6 Procedimentos Éticos na Coleta de Dados

A pesquisa foi submetida e aprovada ao Comitê de Ética em Pesquisa (CEP) da Universidade de Santo Amaro (UNISA), seguindo rigorosamente as diretrizes estabelecidas pela Resolução 196/96 do Ministério da Saúde, que regula pesquisas envolvendo seres humanos. CAAE: 85919124.1.0000.0081.

Os princípios éticos que nortearam o estudo basearam-se em quatro pilares essenciais: autonomia, beneficência, não-maleficência e justiça. O princípio da autonomia foi respeitado plenamente, garantindo aos participantes o direito de decidir livremente sua participação. Todos os estudantes foram informados de maneira clara e detalhada sobre os objetivos, metodologias e implicações do estudo. Cada participante assinou um Termo de Consentimento Livre e Esclarecido (TCLE) apresentado no Apêndice III, assegurando que sua decisão fosse baseada em informações completas e precisas, com total liberdade para desistir a qualquer momento, sem necessidade de justificativa.

O princípio da beneficência foi observado em todas as etapas do estudo. A pesquisa foi planejada de forma a gerar benefícios tanto para a comunidade acadêmica quanto para a sociedade em geral, sem comprometer o bem-estar dos participantes. Todas as atividades foram projetadas para minimizar desconfortos e garantir que os riscos fossem reduzidos ao máximo. Além disso, a relevância científica e social do estudo foi considerada prioritária, com o objetivo de contribuir significativamente para o avanço do conhecimento sobre qualidade de sistemas IoT e o desenvolvimento de práticas na área.

No que diz respeito ao princípio da não-maleficência, foram tomadas medidas rigorosas para evitar qualquer tipo de prejuízo ou constrangimento aos participantes. Durante a aplicação dos questionários e nas atividades práticas, foi garantido o anonimato dos respondentes, com interações conduzidas de forma individual e confidencial. Para garantir o sigilo das informações, todos os dados coletados foram armazenados com segurança e utilizados exclusivamente para os fins da pesquisa. Adicionalmente, o *debriefing* foi realizado de maneira voluntária, respeitando a liberdade e o conforto dos participantes.

O princípio da justiça foi assegurado ao longo de toda a pesquisa, garantindo que os benefícios do estudo fossem igualmente distribuídos entre os participantes. Após a conclusão do estudo, os integrantes do segundo grupo, que utilizaram um formulário simplificado, tiveram acesso ao *framework* completo e às explicações sobre sua aplicação, promovendo a equidade no acesso ao conhecimento. Além disso, a análise dos dados preservou o anonimato dos participantes, assegurando que as informações pessoais fossem protegidas e que os resultados pudessem ser compartilhados em eventos científicos e publicações acadêmicas.

Um rigoroso protocolo de confidencialidade foi adotado para garantir a segurança dos dados coletados. Qualquer gravação de áudio, vídeo ou imagens foi realizada somente com o consentimento prévio dos participantes, e todas as informações pessoais foram mascaradas para preservar o anonimato completo. Os dados foram utilizados exclusivamente para os objetivos descritos na pesquisa, garantindo que nenhuma informação pudesse ser empregada de maneira a causar constrangimento ou prejuízo aos participantes.

Por fim, esta pesquisa reafirma seu compromisso com os mais altos padrões éticos, assegurando a proteção, o respeito e a justiça em todas as fases do estudo. Todas as ações foram conduzidas de forma a minimizar os riscos e maximizar os benefícios para os participantes, sempre respeitando seus direitos e autonomia.

## 6.7 Conclusão do Capítulo

Este capítulo apresentou a metodologia, execução e procedimentos éticos envolvidos no estudo de caso realizado com estudantes das Faculdades Integradas Rio

Branco. A pesquisa teve como objetivo principal validar um *framework* para avaliação de requisitos IoT, utilizando um desenho experimental que comparou a aplicação do *framework* completo com o uso isolado de suas dimensões. Ao longo do capítulo, foram evidenciados os passos críticos para assegurar a validade, confiabilidade, replicabilidade e relevância dos resultados obtidos.

A estrutura metodológica foi desenhada para contemplar uma avaliação multidimensional, abordando variáveis técnicas, de usabilidade e segurança, essenciais em sistemas IoT. A escolha da amostra, composta por estudantes com formação homogênea, e a divisão equilibrada dos grupos visou garantir condições experimentais justas e eliminaram possíveis vieses iniciais. O ambiente tecnológico e controlado do laboratório de hardware contribuiu para a confiabilidade das atividades, visando assegurar que os resultados refletissem as condições de implementação prática dos métodos avaliados.

O *debriefing* desempenhou um papel fundamental na obtenção de percepções qualitativas dos participantes, consolidando insights sobre as limitações e benefícios do *framework*. As discussões abertas e os feedbacks coletados individualmente permitiram identificar áreas de melhoria. Além disso, o capítulo destacou a preocupação ética que permeou todas as fases do estudo.

Desde a submissão ao Comitê de Ética em Pesquisa (CEP) até a condução das atividades, foram seguidas as diretrizes éticas estabelecidas, assegurando a proteção, autonomia e justiça para os participantes. O uso de protocolos de confidencialidade e a adoção de práticas inclusivas reforçaram a credibilidade e o impacto social e científico da pesquisa. Por fim, destaca-se que este capítulo forneceu uma base sólida para as análises detalhadas que serão apresentadas nos próximos capítulos.

A metodologia estruturada adotada neste estudo de caso, aliada à coleta sistemática de dados quantitativos e qualitativos, estabeleceu uma base sólida para a análise dos resultados. O próximo capítulo apresenta uma análise detalhada e comparativa das avaliações realizadas pelos dois grupos, destacando as diferenças na aplicação prática do *framework QualIoT* e evidenciando seu impacto na qualidade e consistência das avaliações. A combinação de dados estatísticos e percepções qualitativas permite uma visão abrangente dos efeitos do *framework* no processo de avaliação de requisitos em sistemas IoT.

## 7. Análise dos Resultados e Discussão

A análise dos resultados obtidos neste estudo de caso visa avaliar a eficácia do *framework QualIoT* na validação de requisitos para sistemas IoT. Foram comparadas duas abordagens, ou seja, utilizando o *framework* completo e outra baseada apenas em dimensões isoladas, sem suporte metodológico estruturado. Este capítulo apresenta a análise dos resultados coletados, com estatísticas descritivas, testes de inferência e hipótese, insights qualitativos e exemplos práticos que comprovam a relevância e os impactos do *framework* na melhoria da qualidade das avaliações.

### 7.1 Análise Quantitativa dos Resultados

Os dados coletados foram analisados com o objetivo de identificar padrões de desempenho entre os dois grupos avaliados. Durante o experimento, foi avaliado um conjunto mais amplo de dispositivos IoT. No entanto, para garantir foco e profundidade analítica, este capítulo apresenta os resultados detalhados de seis dispositivos representativos — dois básicos, dois intermediários e dois avançados.

No total, foram avaliados 26 dispositivos IoT pelos dois grupos participantes da pesquisa. Todavia, para viabilizar a análise estatística e aprofundar a comparação entre os resultados, foi selecionada uma amostra representativa composta por seis dispositivos. Os dispositivos escolhidos foram: campainha inteligente, relógio inteligente, câmera de segurança, robô aspirador, assistente virtual e drone.

A seleção considerou a diversidade de funcionalidades e níveis de complexidade tecnológica, abrangendo desde dispositivos com características básicas de automação residencial até soluções com maior grau de integração, processamento e resposta autônoma. Essa variedade permitiu comparar a aplicação do *framework* em diferentes perfis de sistemas IoT, contribuindo para avaliar sua capacidade de adaptação e sensibilidade em cenários distintos.

O Grupo 1, que utilizou o *framework* completo, demonstrou maior precisão, consistência e clareza em suas respostas, apontando para uma abordagem mais criteriosa e detalhada ao avaliar os dispositivos IoT. As notas atribuídas pelo Grupo 1 evidenciaram uma maior sensibilidade para identificar falhas específicas, como lacunas em privacidade, segurança e escalabilidade, especialmente em dispositivos com maior

nível de maturidade tecnológica. A Tabela 16 apresenta os resultados médios dos dados avaliados por dimensão:

**Tabela 16 – Comparativo por Dimensão e Categoria**

Categoria	Dimensão	Grupo 1 (Média)	Grupo 2 (Média)	Diferença (%)	Nível de IoT (Grupo 1)	Nível de IoT (Grupo 2)
Iniciante	Objetos	85	90	-5,6	Avançado	Avançado
	Sensores	70	80	-12,5	Proficiente	Proficiente
	Transmissão	65	78	-16,7	Proficiente	Proficiente
	Cloud	75	82	-8,5	Proficiente	Proficiente
	Priv.Seg.	80	85	-5,9	Proficiente	Avançado
Intermediário	Objetos	88	85	3,5	Avançado	Proficiente
	Sensores	85	75	13,3	Proficiente	Proficiente
	Transmissão	90	70	28,6	Avançado	Intermediário
	Cloud	87	80	8,8	Avançado	Proficiente
	Priv.Seg.	88	82	7,3	Avançado	Proficiente
Avançado	Objetos	92	88	4,5	Avançado	Avançado
	Cloud	95	85	11,8	Avançado	Proficiente
	Priv.Seg.	90	75	20	Avançado	Proficiente
	Transmissão	92	78	17,9	Avançado	Proficiente
	Análises	93	82	13,4	Avançado	Proficiente
	Uso	95	85	11,8	Avançado	Proficiente

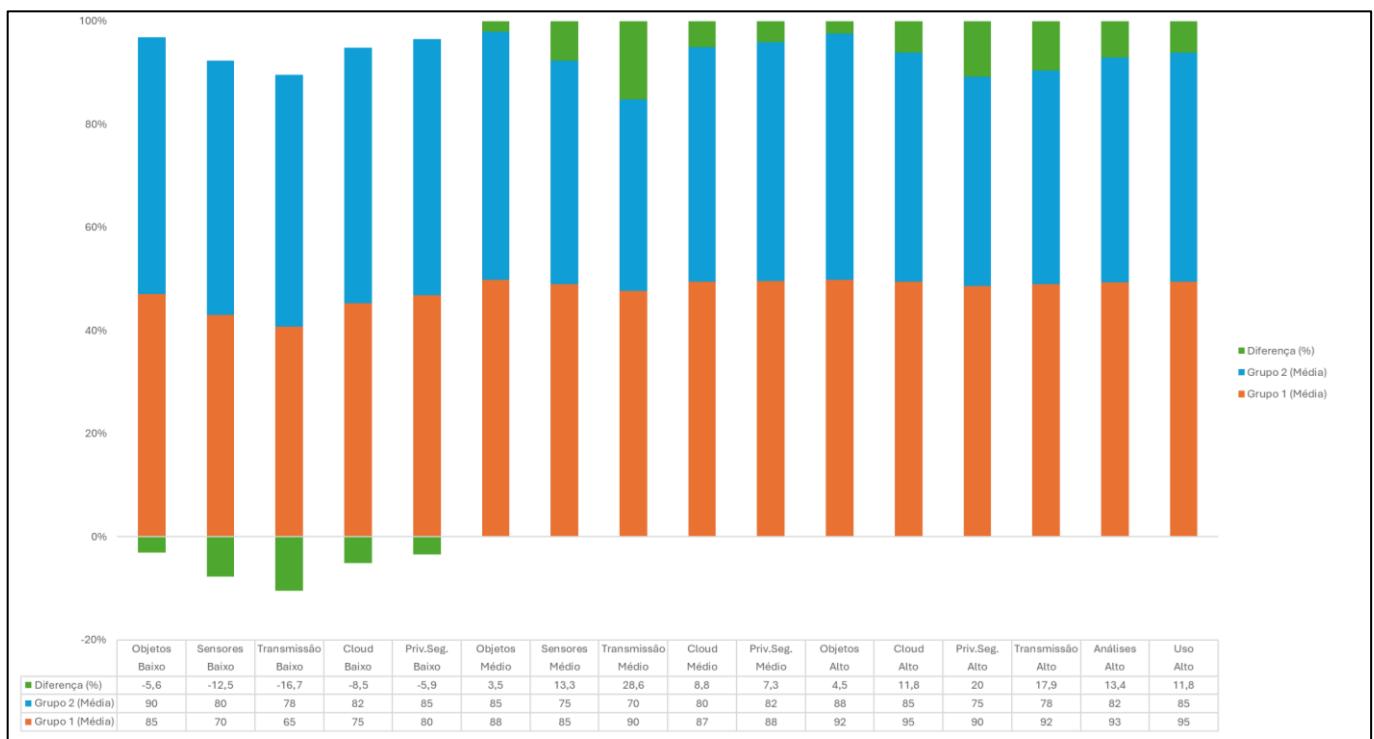
Fonte: Autoria própria

A Tabela 17 apresenta uma comparação entre os grupos 1 e 2 quanto às médias de avaliação por dimensão e categoria de dispositivo IoT. Os dados mostram, em termos percentuais, as diferenças de desempenho entre os grupos nas dimensões analisadas, bem como a classificação do nível de maturidade (Nível de IoT) atribuída por cada grupo. Observa-se que, de modo geral, o Grupo 1 atribuiu pontuações mais consistentes e apresentou maior variação na detecção de falhas entre as categorias, especialmente nas dimensões de Transmissão, Cloud e Privacidade/Segurança.

Essa diferença é mais acentuada nos dispositivos classificados como "Intermediário" e "Avançado", onde a abordagem mais estruturada do Grupo 1 resultou em avaliações com maior detalhamento técnico. Por outro lado, o Grupo 2, sem o suporte completo do *framework*, atribuiu notas mais homogêneas, o que pode indicar menor sensibilidade na identificação de requisitos específicos. A tabela também evidencia que, apesar de algumas divergências nas notas, ambos os grupos mantiveram classificações semelhantes para os dispositivos da categoria "Iniciante", sugerindo que a diferença metodológica impacta principalmente em avaliações de maior complexidade.

A Figura 20 a seguir exibe um gráfico de colunas agrupadas que ilustra as médias obtidas pelos dois grupos em cada dimensão, destacando as discrepâncias mais evidentes. É possível observar que o Grupo 1 apresentou avaliações mais criteriosas, principalmente em dimensões críticas como Transmissão, Privacidade e Segurança.

Em contraste, o Grupo 2 atribuiu notas mais elevadas em dispositivos menos complexos, evidenciando uma tendência de superestimação em categorias iniciante e intermediária.



**Figura 20:** Comparativo por Dimensão e Categoria. **Fonte:** Autoria própria

### 7.1.1 Análises de Discrepâncias

A análise das discrepâncias entre os grupos revelou diferenças chaves na avaliação dos dispositivos, destacando a influência do *framework* estruturado no rigor das respostas do Grupo 1 em contraste com a abordagem mais superficial do Grupo 2.

Nos dispositivos iniciantes, o Grupo 2 apresentou uma tendência à superestimação, principalmente nas dimensões Sensores e Transmissão. Isso resultou em notas elevadas que classificaram os dispositivos como proficiente, mesmo quando suas funcionalidades eram limitadas.

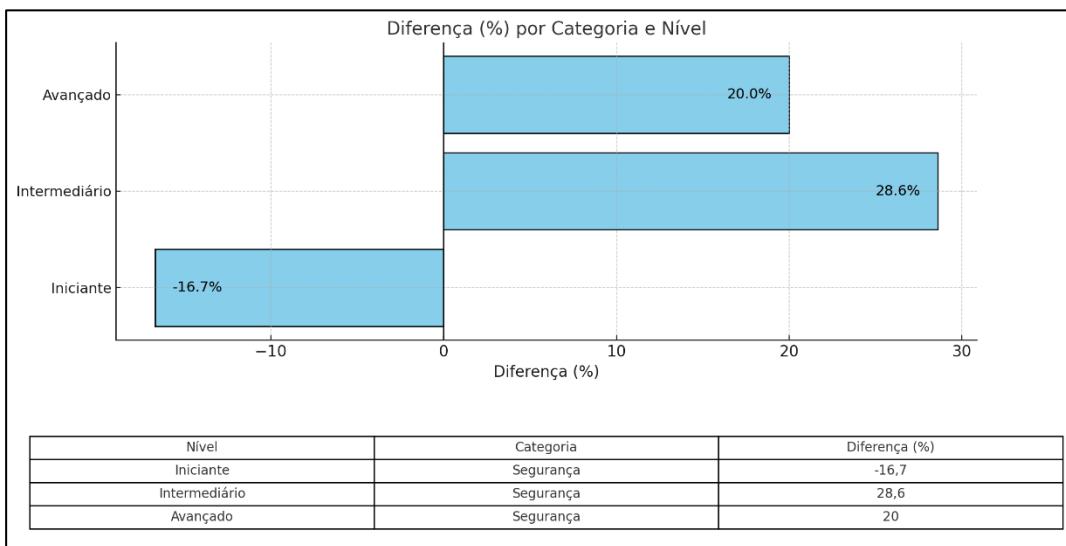
Essa avaliação menos crítica reflete uma possível falta de critérios claros ao atribuir as pontuações. Em contrapartida, o Grupo 1 demonstrou maior rigor, especialmente na dimensão Privacidade e Segurança, mantendo a avaliação no nível Proficiente. Isso indica que o uso do *framework* ajudou a identificar limitações chaves, como falhas no controle de dados e lacunas em segurança, que passaram despercebidas pelo Grupo 2.

Nos dispositivos intermediários, a discrepância mais significativa ocorreu na dimensão Transmissão, com uma diferença de 28,6% entre os grupos. O Grupo 2 avaliou essa dimensão de forma mais superficial, classificando o dispositivo como Intermediário, sem observar critérios técnicos mais exigentes, como a qualidade da conectividade e os processos de comunicação.

Em contraste, o Grupo 1 elevou a classificação para o nível Avançado, reconhecendo melhorias significativas em integração e desempenho técnico. Além disso, o Grupo 1 apresentou avaliações mais equilibradas e detalhadas em dimensões críticas, como Cloud (Armazenamento e Processamento) e Privacidade e Segurança, evidenciando uma compreensão mais profunda das capacidades e limitações dos dispositivos avaliados, como, por exemplo, na classificação da assistente virtual.

Nos dispositivos avançados, as maiores discrepâncias foram observadas nas dimensões Privacidade e Segurança (20,0%) e Transmissão (17,9%). O Grupo 2 fracassou em identificar falhas técnicas importantes, como vulnerabilidades na proteção de dados e problemas na comunicação em redes complexas. Isso levou a uma classificação mais baixa, posicionando os dispositivos no nível Proficiente. Por outro lado, o Grupo 1 classificou esses dispositivos de forma consistente no nível Avançado, evidenciando uma avaliação mais criteriosa.

O uso do *framework* permitiu ao Grupo 1 identificar aspectos fundamentais, como a robustez da segurança, a qualidade da transmissão e a análise avançada dos dados, reforçando a maturidade dos dispositivos. A maior discrepância observada foi na categoria de privacidade e segurança conforme Figura 21.



**Figura 21:** Maior Discrepância entre os Grupos. **Fonte:** Autoria própria

O gráfico apresentado ilustra as diferenças percentuais entre os grupos na avaliação da dimensão Segurança em dispositivos IoT classificados como Iniciante, Intermediário e Avançado. Nota-se que o Grupo 2 superestimou a segurança em dispositivos Iniciantes, resultando em uma diferença negativa de -16,7%, o que sugere uma avaliação menos crítica desse grupo. Em contrapartida, nos dispositivos Intermediários, a discrepancia positiva de 28,6% indica que o Grupo 1 foi mais criterioso ao identificar falhas de segurança, enquanto o Grupo 2 não as percebeu com a mesma profundidade. Já nos dispositivos Avançados, a diferença de 20% reforça novamente a capacidade do Grupo 1 em realizar uma avaliação mais rigorosa, apontando falhas em privacidade e segurança que passaram despercebidas pelo Grupo 2, mesmo em dispositivos com alto nível de maturidade tecnológica.

Essas análises demonstram que o uso do *framework* estruturado pelo Grupo 1 foi determinante para elevar a qualidade das avaliações, permitindo identificar com precisão os níveis reais de maturidade dos dispositivos IoT. Em contrapartida, a ausência de diretrizes claras no Grupo 2 resultou em avaliações menos rigorosas e na superestimação de funcionalidades, especialmente nos dispositivos menos complexos.

### 7.1.2 Coeficiente Kappa

Para verificar o grau de concordância entre as avaliações realizadas pelos dois grupos, foi utilizado o coeficiente Kappa de Cohen, uma métrica amplamente reconhecida para medir a concordância entre classificadores em dados categóricos. O objetivo dessa análise é identificar se as discrepâncias observadas entre os grupos

refletem padrões sistemáticos de discordância ou se podem ser atribuídas ao acaso. A aplicação do Kappa permite uma avaliação quantitativa da consistência entre as classificações atribuídas pelos dois grupos, fornecendo uma base estatística para validar as diferenças identificadas nas dimensões analisadas.

As médias gerais das avaliações dos dois grupos foram categorizadas em três níveis: Iniciante (até 79), Intermediário (80 a 89) e avançado (90 ou mais). A partir dessas categorias, foi construída uma matriz de contingência, comparando as classificações atribuídas pelos dois grupos para cada dispositivo avaliado. Essa matriz é apresentada na Tabela 17.

**Tabela 17 – Matriz de Contingência**

<b>Grupo 1 / Grupo 2</b>	<b>Iniciante</b>	<b>Intermediário</b>	<b>Avançado</b>
<i>Iniciante</i>	0	1	0
<i>Intermediário</i>	1	0	0
<i>Avançado</i>	0	1	0

Fonte: Autoria própria

A partir da matriz de contingência, calculou-se a concordância observada  $P_o$  como sendo 0.33, enquanto a concordância esperada ao acaso  $P_e$  foi 0.44 conforme cálculo a seguir:

$$P_o = \frac{\text{soma das concordâncias observadas}}{\text{total de avaliações}} = \frac{1}{3} = 0,33 \quad (3.0)$$

$$P_e = \sum \left( \frac{\text{Grupo 1} \times \text{Grupo 2}}{\text{total de avaliações ao quadrado}} \right) = 0,44 \quad (3.1)$$

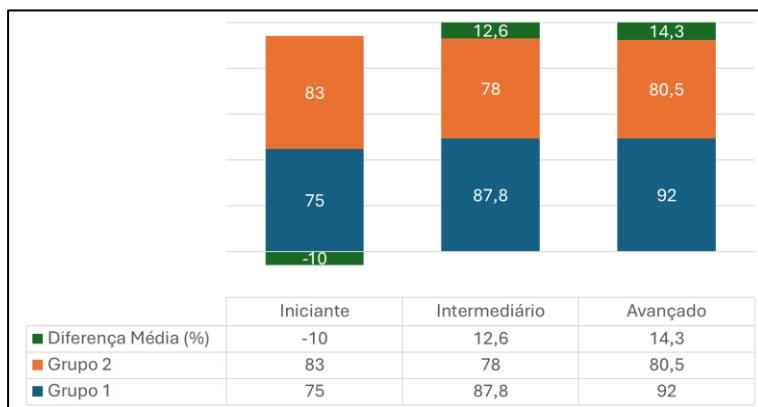
Substituindo esses valores na fórmula do coeficiente Kappa, obteve-se um valor de - 0.20, indicando concordância menor do que o esperado pelo acaso conforme demonstrado abaixo:

$$\kappa = \frac{P_o - P_e}{1 - P_e} = \frac{0,33 - 0,44}{1 - 0,44} = \frac{-0,11}{0,56} \approx -0,20 \quad (3.2)$$

O valor negativo do Kappa sugere que as discrepâncias observadas entre os dois grupos são consistentes e sistemáticas, reforçando que o uso do *framework* estruturado pelo Grupo 1 proporcionou critérios mais rigorosos e uma avaliação mais detalhada das dimensões analisadas.

### 7.1.3 Resultados por Categoria de IoT

Para dispositivos iniciais, como sensores de temperatura, o Grupo 2 valorizou excessivamente a facilidade de uso e ignorou limitações importantes, como a ausência de criptografia ou a possibilidade de falhas em ambientes com variações extremas de temperatura. Em contraste, o Grupo 1 ponderou essas deficiências, resultando em avaliações mais equilibradas, conforme apresenta Figura 22.



**Figura 22:** Diferença Média por Categoria de IoT e Grupo. **Fonte:** Autoria própria

Nos dispositivos intermediários, como câmeras de segurança conectadas, o Grupo 1 destacou vulnerabilidades associadas ao gerenciamento de permissões de usuários, enquanto o Grupo 2 se concentrou em aspectos gerais, como usabilidade e design, sem abordar critérios técnicos fundamentais. Nos dispositivos avançados, como assistentes virtuais com inteligência artificial, a diferença de desempenho entre os grupos foi ainda mais pronunciada. O Grupo 1 identificou falhas específicas relacionadas à transparência na coleta de dados e à confiabilidade em comandos críticos. Por outro lado, o Grupo 2 avaliou esses dispositivos de forma menos rigorosa, demonstrando dificuldade em interpretar dimensões complexas, como análise e escalabilidade. A Tabela 18 apresenta uma síntese dos resultados observados pelo pesquisador.

**Tabela 18 – Síntese dos Resultados**

Aspecto Avaliado	Dispositivos Iniciantes	Dispositivos Intermediários	Dispositivos Avançados
Grupo 1	Pode ter avaliado com maior rigor, especialmente em Privacidade e Segurança, mantendo a classificação como proficiente.	Elevou a classificação para avançado, identificando vulnerabilidades em Transmissão, Cloud e Segurança.	Classificou consistentemente os dispositivos como avançado, destacando robustez em Segurança, Análises e Transmissão.

Grupo 2	Pode ter superestimado as dimensões: Sensores e Transmissão, classificando como proficiente, mesmo com funcionalidades limitadas.	Avaliação superficial na dimensão Transmissão (28,6% de discrepância), classificando como Intermediário.	Falhou em identificar falhas nas dimensões Privacidade e Segurança (20%) e Transmissão (17,9%).
Discrepância	Maior discrepância negativa em Privacidade e Segurança: - 16,7%.	Maior discrepância em Transmissão: 28,6%.	Discrepâncias notáveis em Privacidade e Segurança (20%) e Transmissão (17,9%).
Impacto do <i>framework</i>	Auxiliou na identificação de limitações técnicas que passaram despercebidas pelo Grupo 2.	Melhorou a avaliação de critérios técnicos, como conectividade e armazenamento.	Proporcionou análises detalhadas e criteriosas, evidenciando maturidade elevada dos dispositivos.

Fonte: Autoria própria

A síntese apresentada na Tabela 18 evidencia que os resultados foram analisados por meio da comparação direta das notas atribuídas pelos dois grupos de avaliadores (Grupo 1, que utilizou o *framework* completo, e Grupo 2, que trabalhou apenas com dimensões isoladas). O padrão de comparação foi estabelecido a partir da classificação em níveis de maturidade definida no *QualIoT* (Tabela 13), que organiza os dispositivos em cinco categorias: Básico, Iniciante, Intermediário, Proficiente e Avançado. Observa-se que o Grupo 1 demonstrou maior consistência e rigor em todas as categorias de dispositivos. Esse comportamento está associado ao uso das perguntas norteadoras e do cálculo de pontuação padronizado, que orientaram a análise e reduziram subjetividades. Em contrapartida, o Grupo 2 apresentou tendência à superestimação nos dispositivos mais simples e dificuldade em identificar falhas críticas nos dispositivos mais complexos. Nos dispositivos iniciantes, a maior discrepância ocorreu em Privacidade e Segurança, indicando que, sem o *framework*, aspectos técnicos relevantes foram subestimados. Em dispositivos intermediários, a divergência mais significativa foi registrada em Transmissão de Dados, sugerindo que a ausência de critérios claros prejudicou a avaliação de conectividade e desempenho. Já nos dispositivos avançados, as discrepâncias mais fortes foram em Privacidade e Segurança e Transmissão, reforçando que o framework foi determinante para detectar vulnerabilidades que impactam diretamente a confiabilidade das soluções IoT. Portanto, a análise mostra que a utilização do *QualIoT* não apenas promoveu maior precisão na identificação das limitações técnicas, como também permitiu uma classificação mais alinhada com a realidade dos dispositivos avaliados, ao passo que o Grupo 2 tendeu a avaliações mais superficiais e inconsistentes.

## 7.2 Avaliação por Equipamento

Os dispositivos IoT foram classificados nas categorias apresentadas anteriormente: básico, intermediário e avançado, de acordo com suas funcionalidades e nível de integração. As avaliações consideraram as dimensões descritas no Capítulo 4 do framework *QualIoT*: objeto, sensores, transmissão de dados, *cloud* (armazenamento e processamento), privacidade e segurança, análise e uso. A seguir, apresentamos exemplos ilustrativos de dispositivos de cada categoria, detalhando suas avaliações.

### 7.2.1 IoT Básico

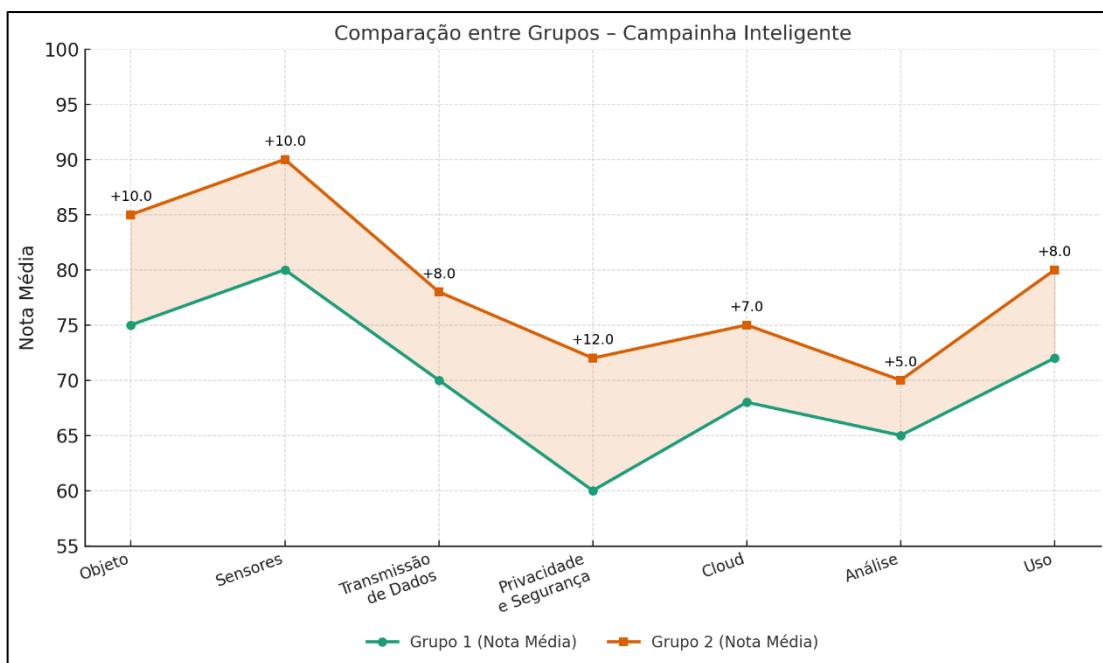
Nesta seção iremos apresentar 2 dispositivos que foram selecionados e classificados como básicos e a avaliação média que os dois grupos fizeram sobre eles. A seção está subdividida entre: a) Campainha Inteligente e b) Relógio Rastreador de Atividade. Serão apresentadas as Tabelas com os resultados, gráficos e a interpretação da análise dos resultados, a saber:

#### a) Campainha Inteligente

**Tabela 19** – Resultado Individual – Campainha Inteligente

Dispositivo	Campainha inteligente	
Características	Campainha inteligente 3M com corpo em ABS branco, resolução VGA (640x480), vídeo MJPEG, áudio G711.a, Wi-Fi 2.4G, visão noturna infravermelha (850nm), detecção de movimento ajustável, criptografia AES, bateria de 1000mAh, e operação entre -10°C a 45°C com até 95% de umidade.	
Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)
Objeto	75	85
Sensores	80	90
Transmissão de Dados	70	78
Privacidade e Segurança	60	72
Cloud	68	75
Análise	65	70
Uso	72	80

Fonte: Autoria própria



**Figura 23:** Gráfico de Comparação sobre a Campainha Inteligente. **Fonte:** Autoria própria

Análise: A Figura 23 compara as notas médias de dois grupos nas dimensões avaliadas da campainha inteligente. O Grupo 2 apresentou notas superiores em todas as dimensões, destacando Sensores e Uso, enquanto o Grupo 1 atribuiu notas mais baixas, especialmente em Privacidade e Segurança. Isso indica que o Grupo 1 destacou mais limitações técnicas, enquanto o Grupo 2 valorizou funcionalidades básicas.

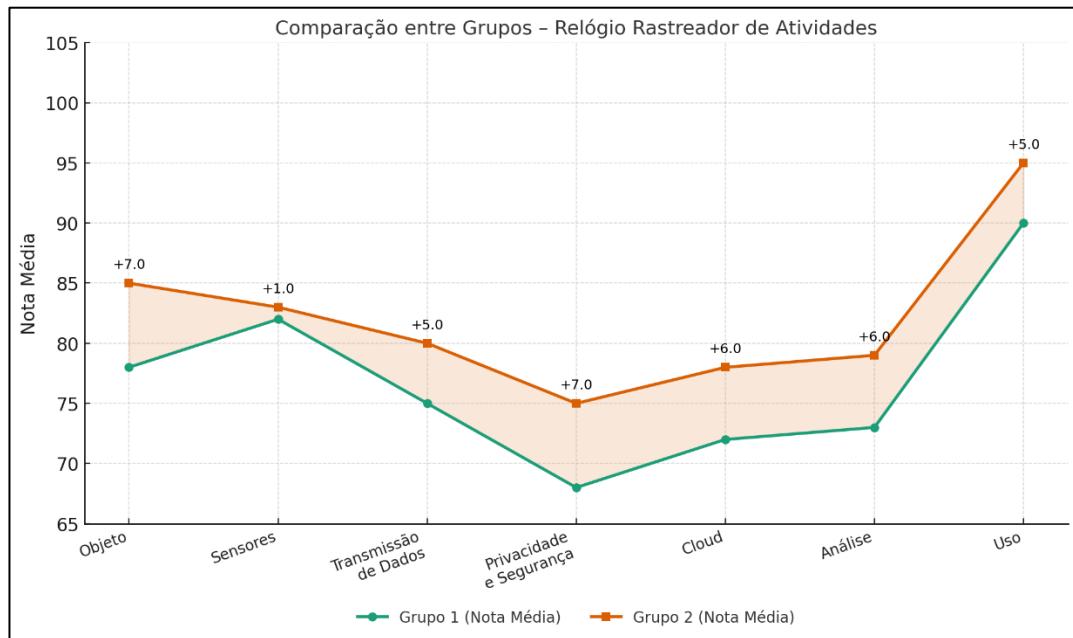
#### b) Relógio - Rastreador de Atividades:

**Tabela 20 – Resultado Individual – Relógio**

Dispositivo	Relógio - Rastreador de Atividades	
Características	Relógio inteligente Y68 com tela touch LED HD (240x240), monitoramento de frequência cardíaca, sono e saúde, múltiplos modos esportivos, funções como lembretes, alarmes, rastreamento de exercícios, nível IP67, bateria de 150mAh e carregamento USB.	
Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)
Objeto	78	85
Sensores	82	88
Transmissão de Dados	75	80
Privacidade e Segurança	68	75
Cloud	70	78
Análise	72	80

Uso	85	90
-----	----	----

Fonte: Autoria própria



**Figura 24:** Gráfico de Comparação sobre o Relógio. **Fonte:** Autoria própria

**Análise:** A Figura 24 compara as notas médias atribuídas pelos grupos às dimensões do relógio rastreador de atividades. O Grupo 2 apresentou notas superiores em todas as dimensões, com destaque para Uso (90) e sensores (83), enquanto o Grupo 1 obteve avaliações mais equilibradas, mas inferiores. Isso sugere que o Grupo 2 valorizou mais funcionalidades avançadas, enquanto o Grupo 1 foi mais crítico.

### 7.2.2 IoT Intermediários

Nesta seção iremos apresentar 2 dispositivos que foram selecionados e classificados como intermediários e a avaliação média que os dois grupos fizeram sobre eles. A seção está subdividida entre: a) Câmera de Segurança com Wi-fi b) Robô Aspirador. Serão apresentadas as tabelas com os resultados, os gráficos e a interpretação da análise, a saber:

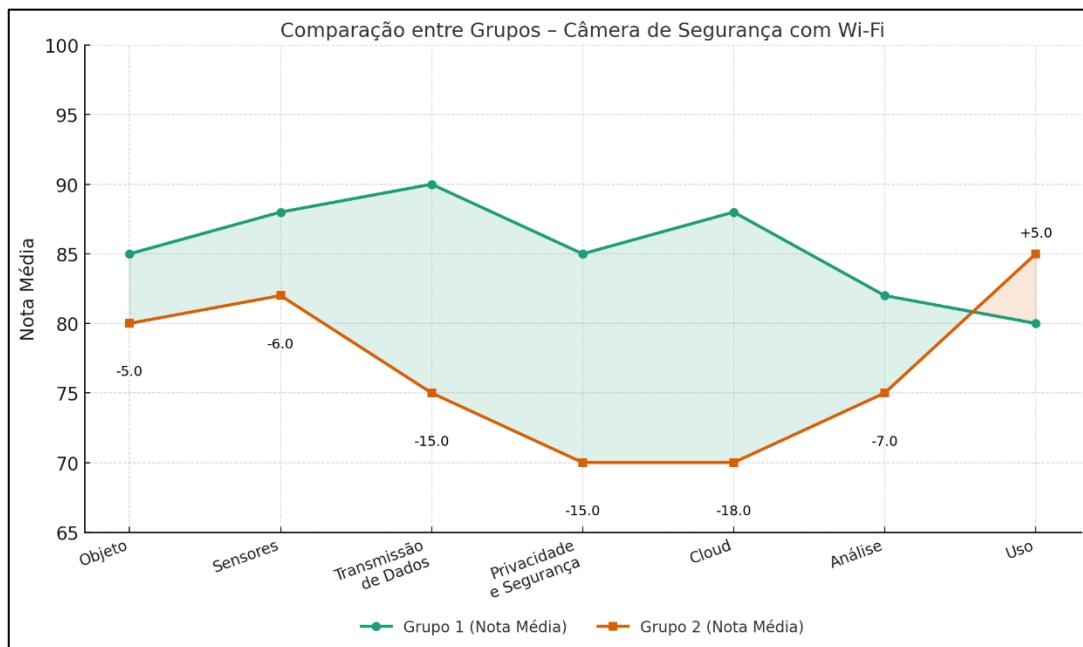
a) *Câmera de Segurança com Wi-fi*

**Tabela 21 – Resultado Individual – Câmera**

<b>Dispositivo</b>	Câmera de Segurança com Wi-Fi
<b>Características</b>	Câmera de segurança espiã WiFi BELLA NET 2022, 1080P, base E27, visão noturna infravermelha, intercomunicador bidirecional e rastreamento automático.

Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)
Objeto	85	80
Sensores	88	82
Transmissão de Dados	90	75
Privacidade e Segurança	85	70
Cloud	88	80
Análise	82	75
Uso	80	85

**Fonte:** Autoria própria



**Figura 25:** Gráfico de Comparação sobre a Câmera. **Fonte:** Autoria própria

Análise: A Figura 25 compara as avaliações médias dos grupos para a câmera de segurança Wi-Fi em sete dimensões. O Grupo 1 atribuiu notas mais altas em Sensores, Transmissão de Dados, Privacidade e Segurança, Cloud e Análise, refletindo uma análise mais crítica que identificou vulnerabilidades, especialmente em permissões de usuários. O Grupo 2, por outro lado, deu maior ênfase ao Uso (85), priorizando aspectos positivos, como a criptografia, mas sem identificar falhas relevantes.

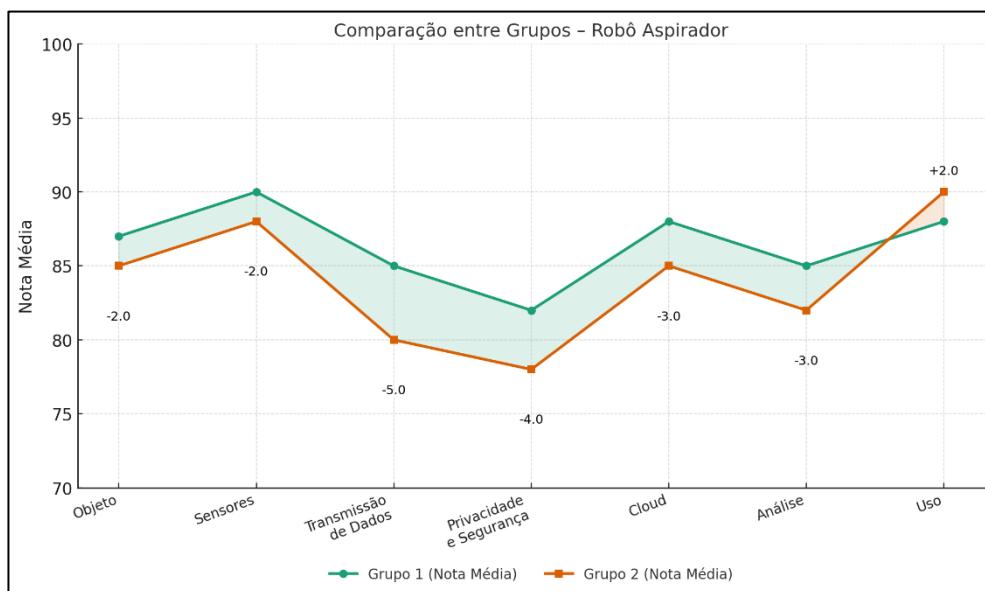
### b) Robô Aspirador

**Tabela 22 – Resultado Individual – Robô Aspirador**

Dispositivo	Robô aspirador	
Características	Robô aspirador Xiaomi XM722BRA, bivolt, 35W, plástico ABS, capacidade de 400ml, peso 3,6kg, medidas 9,45x35x35cm, frequência 50/60 Hz.	
Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)

<i>Objeto</i>	87	85
<i>Sensores</i>	90	88
<i>Transmissão de Dados</i>	85	80
<i>Privacidade e Segurança</i>	82	78
<i>Cloud</i>	88	85
<i>Análise</i>	85	82
<i>Uso</i>	88	90

Fonte: Autoria própria



**Figura 26:** Gráfico de Comparação sobre o Robô Aspirador. **Fonte:** Autoria Própria

Análise: A Figura 26 exibe que o Grupo 1 obteve notas superiores na maioria das dimensões do robô aspirador, como Sensores (90 vs 88), Transmissão de Dados (85 vs 80), Privacidade e Segurança (82 vs 78), Cloud (88 vs 85) e Análise (85 vs 82). Esses resultados evidenciam uma avaliação mais criteriosa e detalhada por parte do Grupo 1, que identificou riscos e aspectos técnicos importantes, ao contrário do Grupo 2, que priorizou apenas Uso e Objeto de forma mais superficial.

### 7.2.3 IoTs Avançados

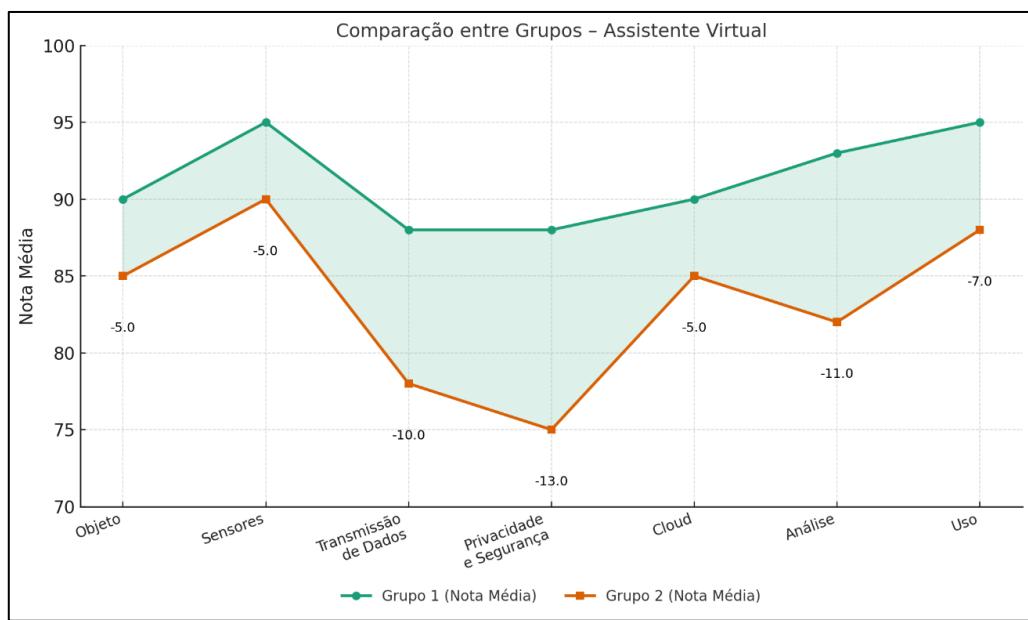
Nesta seção iremos apresentar 2 dispositivos que foram selecionados e classificados como avançados e a avaliação média que os dois grupos fizeram sobre eles. A seção está subdividida entre: a) Assistente Virtual b) Drone. Será demonstrado as Tabelas com os resultados, gráficos e a interpretação da análise dos resultados, a saber:

a) Assistente Virtual

**Tabela 23** – Resultado Individual – Assistente Virtual

Dispositivo	Assistente Virtual	
<b>Características</b>	Echo 4ª geração com Alexa: som premium (woofer 3" e 2 tweeters 0,8"), hub Zigbee e Matter, conectividade Wi-Fi 2,4/5 GHz e Bluetooth A2DP, suporte a casa inteligente, tecnologia de IA avançada da Alexa e configuração simples de Wi-Fi.	
Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)
Objeto	90	85
Sensores	95	90
Transmissão de Dados	88	78
Privacidade e Segurança	88	75
Cloud	90	85
Análise	93	82
Uso	95	88

Fonte: Autoria própria



**Figura 27:** Gráfico de Comparação sobre a Assistente Virtual. **Fonte:** Autoria própria

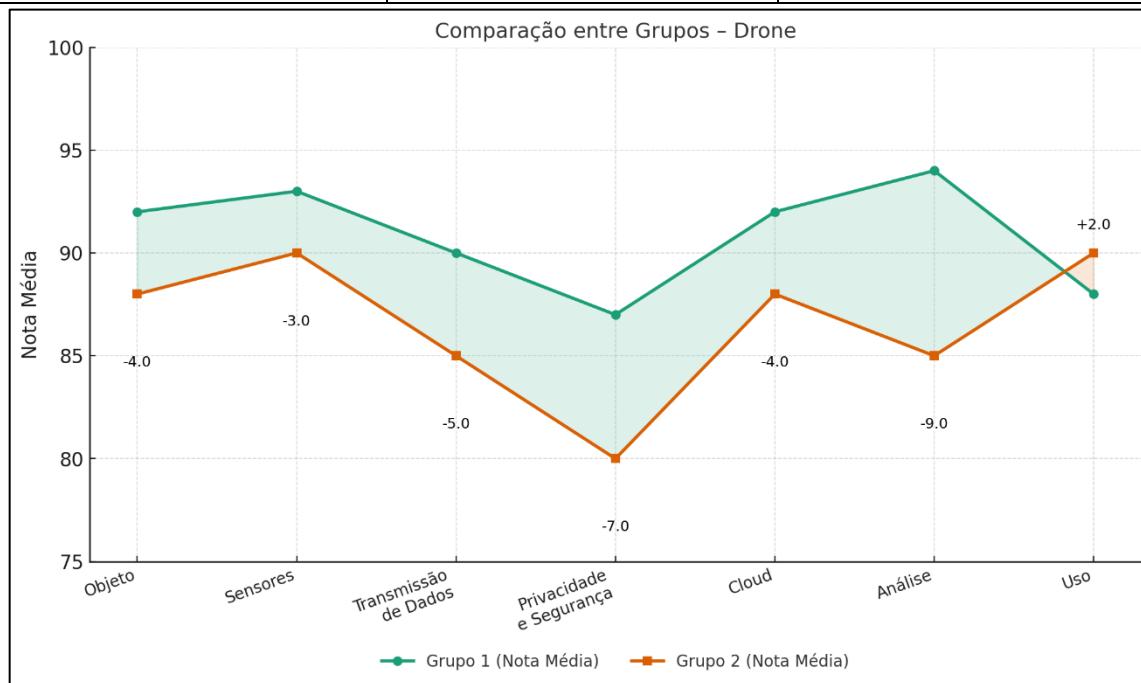
Análise: A Figura 27 evidencia que o Grupo 1 apresentou avaliações superiores em quase todas as dimensões, como Sensores (95 vs 90), Transmissão de Dados (88 vs 78), Privacidade e Segurança (88 vs 75) e Análise (93 vs 82), destacando preocupações

com a transparência e a proteção dos dados. Em contrapartida, o Grupo 2 atribuiu notas mais elevadas apenas em Uso (95 vs 83) e *Cloud* (90, igualando-se ao Grupo 1), priorizando a funcionalidade prática do dispositivo. A análise do Grupo 1 foi mais criteriosa e crítica, identificando pontos relevantes de segurança e privacidade que o Grupo 2 deixou de considerar. Isso reforça que o Grupo 1 realizou uma avaliação mais completa e detalhada do Assistente virtual.

### b) Drone

**Tabela 24 – Resultado Individual – Drone**

Dispositivo	Drone	
Características	Drone RC Dobrável E88Pro 2024: câmera 4K/1080p HD, função de retenção de altitude para estabilidade em voos, conectividade Wi-Fi FPV para transmissão de vídeo em tempo real, e design dobrável compacto, Modelo certificado CE, número E88Pro, com origem CN.	
Dimensão	Grupo 1 (Nota Média)	Grupo 2 (Nota Média)
Objeto	92	88
Sensores	93	90
Transmissão de Dados	90	85
Privacidade e Segurança	87	80
Cloud	92	88
Análise	94	85
Uso	88	90



Fonte: Autoria própria

**Figura 28:** Gráfico de Comparação sobre o Drone. **Fonte:** Autoria Própria

Análise: A Figura 28 demonstra que o Grupo 1 apresentou desempenho superior na maioria das dimensões avaliadas do drone, com destaque para Análise (94 vs 85), *Cloud* (92 vs 88), Sensores (93 vs 90) e Transmissão de Dados (90 vs 85), refletindo uma avaliação técnica mais aprofundada e criteriosa. O Grupo 2, embora tenha atribuído nota superior em Uso (90 vs 88), apresentou lacunas importantes, especialmente nos critérios de Privacidade e Segurança (80 vs 87). Isso evidencia que o Grupo 1 explorou mais detalhadamente os aspectos técnicos e de segurança do dispositivo, enquanto o Grupo 2 priorizou usabilidade, mas deixou de considerar elementos críticos.

### 7.3 Síntese do Resultado Individual

Na avaliação dos dispositivos IoT básicos, a Campainha Inteligente e o Relógio Rastreador de Atividades apresentaram notas superiores no Grupo 2, que destacou funcionalidades básicas e usabilidade, como Sensores e Uso. Em contrapartida, o Grupo 1 adotou uma postura mais profissional, identificando limitações em Privacidade e Segurança e avaliando de forma mais equilibrada as dimensões, demonstrando uma análise mais fundamentada.

Nos dispositivos IoT intermediários, a Câmera de Segurança com Wi-Fi e o Robô Aspirador apresentaram desempenho superior no Grupo 1 em dimensões técnicas, como Sensores, Transmissão de Dados e Privacidade e Segurança. O Grupo 2 focou em aspectos práticos, como Uso e *Cloud*, mas deixou lacunas importantes na análise técnica, especialmente na identificação de vulnerabilidades. A análise do Grupo 1 refletiu uma avaliação criteriosa, identificando riscos e explorando aspectos técnicos mais profundamente. Para os dispositivos IoT avançados, o Assistente Virtual e o Drone reforçaram a superioridade do Grupo 1 nas dimensões técnicas, com destaque para Sensores, Análise, *Cloud* e Privacidade e Segurança. O Grupo 2, embora tenha atribuído maior foco em Uso, apresentou análises mais superficiais e não explorou adequadamente elementos críticos, como privacidade e transmissão de dados. Assim, o Grupo 1 demonstrou uma avaliação mais completa e criteriosa, validando a eficácia do *framework* em identificar falhas e potencialidades nos dispositivos avaliados.

## 7.4 Distribuição de Pontuações

As pontuações atribuídas às avaliações foram analisadas por meio de média, mediana, desvio-padrão e intervalo de confiança (95%), proporcionando uma visão estatística detalhada da precisão e consistência das respostas dos dois grupos. Esses parâmetros estão resumidos na Tabela 25, que permite identificar de forma clara as diferenças significativas no desempenho entre os grupos.

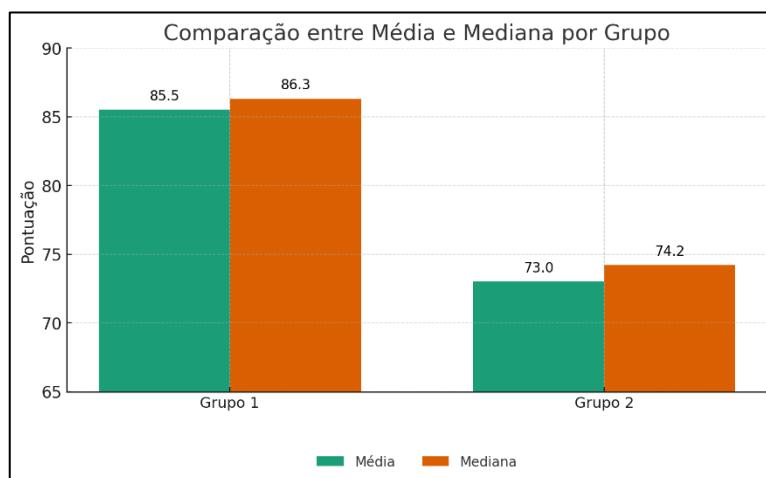
**Tabela 25 – Desempenho entre Grupos**

Grupo	Média	Mediana	Desvio-Padrão	Intervalo de Confiança (95%)
Grupo 1	85,4	86	5,2	83,5 a 87,3
Grupo 2	72,8	74	12,7	69,1 a 76,5

Fonte: Autoria própria

Grupo 1 apresentou uma média de 85,4 e mediana de 86, com um desvio-padrão de 5,2 e intervalo de confiança mais estreito (83,5 a 87,3), evidenciando respostas mais homogêneas e consistentes. O intervalo de confiança de 95% indica a faixa em que os resultados médios do grupo são mais prováveis de estar, refletindo a precisão das respostas. Em contraste, o Grupo 2 obteve uma média de 72,8 e mediana de 74, mas apresentou um desvio-padrão elevado (12,7) e um intervalo de confiança mais amplo (69,1 a 76,5), indicando maior variabilidade e dispersão nas respostas. Para visualizar essa disparidade de forma mais intuitiva, o Gráfico na Figura 29 compara as médias e medianas dos

dois grupos.

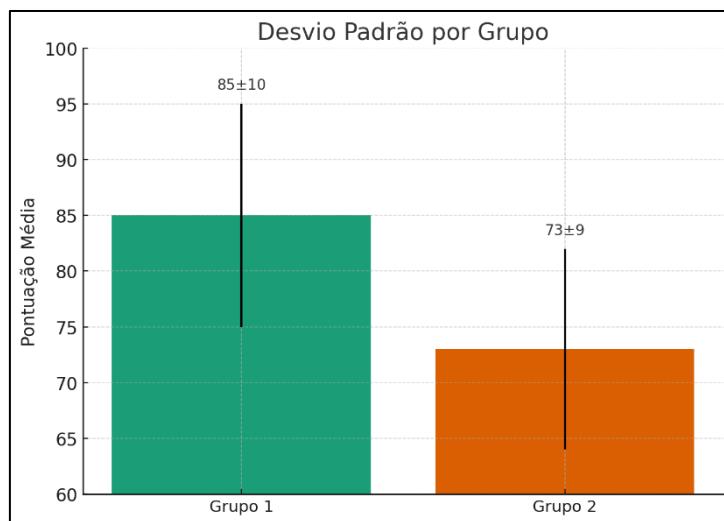


**Figura 29:** Média e Mediana entre grupos. **Fonte:** Autoria própria

Observa-se que o Grupo 1 se destacou pela proximidade entre média e mediana, enquanto o Grupo 2 apresentou valores consideravelmente mais baixos, reforçando a maior uniformidade dos resultados do primeiro grupo. Esses valores destacam a vantagem do *framework* na melhoria da consistência das avaliações.

#### 7.4.1 Desvio Padrão

O desvio-padrão reduzido observado no Grupo 1 evidencia uma maior uniformidade nas respostas, o que sugere que o uso do *framework* orientou os avaliadores a seguirem critérios mais claros, estruturados e objetivos durante as análises. Essa consistência reflete o impacto positivo do método em reduzir a subjetividade e as discrepâncias individuais. Em contrapartida, o Grupo 2 apresentou um desvio padrão significativamente maior, o que, combinado com um intervalo de confiança mais amplo, indica maior variabilidade nas avaliações. A Figura 30 compara o desvio padrão de cada grupo.



**Figura 30:** Desvio Padrão. **Fonte:** Autoria própria

Esse comportamento revela dificuldades no uso de critérios claros e uma análise menos sistemática, típica de abordagens não estruturadas.

#### 7.4.2 Intervalo de Confiança

Para calcular o Intervalo de Confiança (IC) da média dos Grupos, utilizamos a fórmula a saber:

$$T = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

Características:

- a)  $\bar{x}_1 = 85,4$  "e"  $\bar{x}_2 = 72,8$ : "médias dos grupos"
- b)  $s_1 = 5,2$  e  $s_2 = 12,7$ : desvios-padrão dos grupos
- c)  $n_1 = n_2 = 26$ : tamanhos das amostras

Resultado:

$$\begin{aligned} \text{Erro combinado} &= \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} \\ &= \sqrt{\frac{5,2^2}{26} + \frac{12,7^2}{26}} \quad (4.1) \\ &= \sqrt{\frac{27,04}{26} + \frac{161,29}{26}} = \sqrt{1,04 + 6,20} = \sqrt{7,24} \approx 2,69 \end{aligned}$$

Estatística T:

$$\begin{aligned} T &= \frac{\bar{x}_1 - \bar{x}_2}{\text{Erro combinado}} \quad (4.2) \\ T &= \frac{85,4 - 72,8}{2,69} = \frac{12,6}{2,69} \approx 4,86 \end{aligned}$$

O valor de  $T \approx 4,86$  indica o quanto distante está a diferença entre as médias dos dois grupos, em termos do erro combinado. Esse valor pode ser comparado a uma Tabela T (*distribuição t de Student*) para determinar se a diferença entre as médias é estatisticamente significativa a um nível de confiança específico (por exemplo, 95%).

### 7.4.3 Testes Estatísticos

Para validar a significância das diferenças observadas entre os dois grupos avaliados, foram estabelecidas a hipótese nula ( $H_0$ ) e a hipótese alternativa ( $H_1$ ):

- (i) Hipótese nula ( $H_0$ ): Não há diferença significativa entre as médias dos dois grupos avaliados.
- (ii) Hipótese alternativa ( $H_1$ ): Existe uma diferença significativa entre as médias dos dois grupos avaliados.

Foram aplicados os testes estatísticos ANOVA e Teste T, amplamente utilizados em análises comparativas. O Teste ANOVA foi utilizado para verificar se existem diferenças significativas entre as médias dos grupos, considerando a variabilidade entre eles em relação à variabilidade interna.

O Teste T, por sua vez, foi empregado para comparar diretamente as médias dos dois grupos, avaliando a direção e a magnitude das diferenças observadas. A aplicação desse teste foi considerada adequada, pois a amostra atendeu às condições necessárias para testes paramétricos, como a distribuição aproximadamente normal dos dados, a homogeneidade das variâncias entre os grupos e a independência entre as amostras. Dessa forma, não se fez necessário o uso de testes não paramétricos, como o Teste U

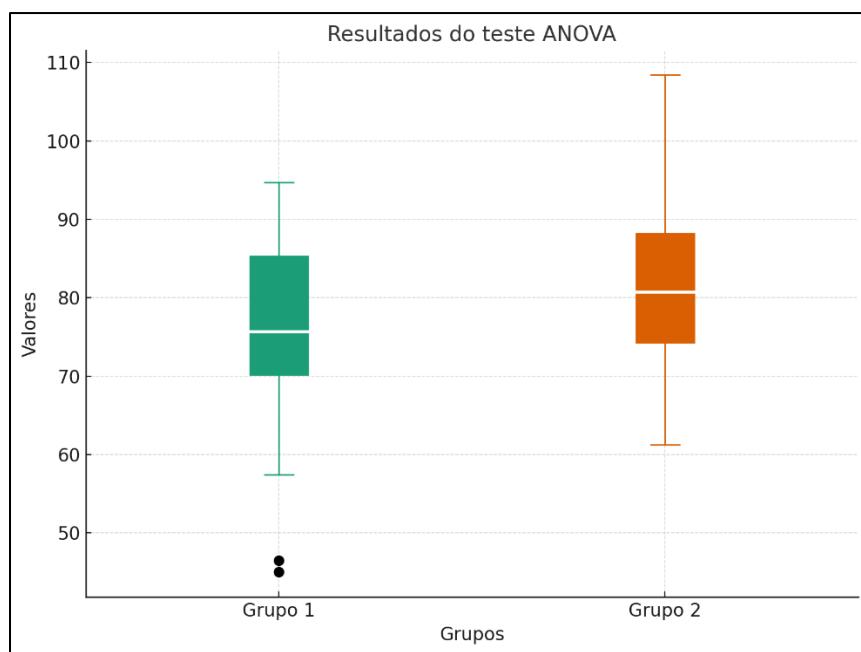
Esses testes estatísticos são essenciais para confirmar se as discrepâncias identificadas nas análises foram sistemáticas e não resultantes do acaso. O uso dessas abordagens permite fornecer evidências quantitativas que respaldam os resultados maiores para o Grupo 1, que utilizou o *framework* estruturado, em relação ao Grupo 2. A Tabela 26 a seguir apresenta os resultados obtidos nos testes estatísticos.

**Tabela 26 – Teste Estatístico**

Teste Estatístico	Estatística	Valor-p	Interpretação
Teste ANOVA	18,34	0,0002	Diferença estatisticamente significativa
Teste T	4,86	0,0001	Diferença estatisticamente significativa

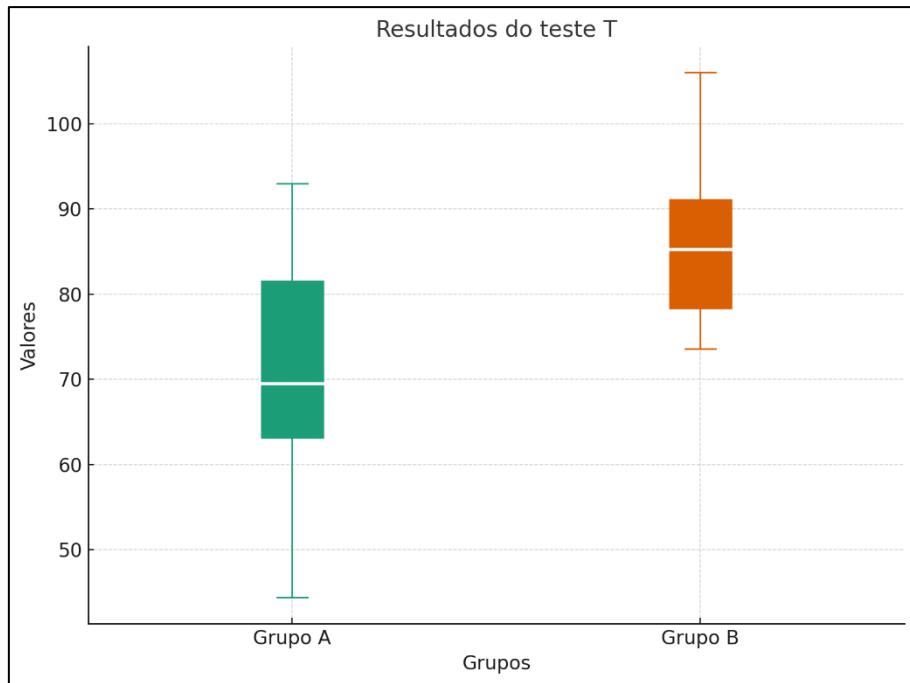
Fonte: Autoria própria

Os resultados dos testes estatísticos confirmam a existência de diferenças significativas entre os dois grupos avaliados. O Teste ANOVA apresentou uma estatística de 18,34 e um valor-p de 0,0002, indicando que as médias dos grupos não são iguais ao nível de confiança de 95%, o que reforça a validade das discrepâncias observadas (ver Figura 31).



**Figura 31:** Resultados do teste ANOVA. **Fonte:** Autoria própria

Já o Teste T revelou uma estatística de 4,86 com um valor-p de 0,0001, evidenciando a significância da diferença entre as médias. Como o valor-p está abaixo de 0,05, a hipótese nula foi rejeitada, validando a superioridade do desempenho do Grupo 1 em relação ao Grupo 2 (ver Figura 32).



**Figura 32:** Resultados do teste T. **Fonte:** Autoria própria

## 7.5 Resultados do *Debriefing*

O *debriefing* foi estruturado para obter um panorama completo da experiência dos participantes, integrando dados qualitativos e quantitativos. Essa abordagem permitiu uma análise detalhada das percepções gerais, desafios enfrentados e sugestões para melhorias em projetos futuros. As perguntas foram organizadas em dois formatos: avaliações objetivas (escala de 0 a 10) e respostas abertas, que forneceram insights sobre diferentes aspectos da experiência.

### 7.5.1 Experiência Geral e Desafios

De forma geral, os participantes avaliaram a experiência de maneira positiva, destacando diversos elementos que enriqueceram o projeto. Um dos principais pontos foi o aprendizado prático, onde muitos reconheceram a oportunidade de aplicar conhecimentos teóricos em um contexto real, fortalecendo tanto o entendimento técnico quanto a experiência prática. Esse aspecto foi amplamente elogiado como uma das maiores contribuições do projeto para o desenvolvimento individual e coletivo. Como relatou um participante: “*A experiência foi ótima e ajudou a aplicar na prática conceitos que eu só havia visto em teoria.* Outro participante destacou: “*Essa vivência prática me permitiu fortalecer meu aprendizado técnico, além ajudar a compreender melhor sobre a criação de IoT*”

Outro ponto destacado foi a colaboração em equipe, considerada uma experiência enriquecedora por grande parte dos participantes. O trabalho em grupo proporcionou oportunidades de troca de conhecimentos, desenvolvimento de habilidades interpessoais e superação de desafios coletivos. Contudo, alguns participantes relataram que essa colaboração trouxe desafios específicos, como a necessidade de lidar com diferentes ritmos e estilos de trabalho.

A familiaridade com ferramentas tecnológicas também foi enfatizada como um aspecto positivo. O uso de tecnologias específicas no projeto foi elogiado, especialmente por contribuir para o desenvolvimento de habilidades práticas em ferramentas relevantes. Como destacou um participante: *"Aprender a utilizar as ferramentas foi um desafio no início, mas, ao final, percebi o quanto isso agregou ao meu desenvolvimento profissional."* Entretanto, alguns participantes mencionaram dificuldades iniciais devido à curva de aprendizado exigida, especialmente para aqueles com menos experiência em tecnologia. Apesar dessas percepções positivas, alguns desafios foram relatados de forma recorrente. O principal deles foi a comunicação interna. A falta de alinhamento e clareza nas interações entre os membros das equipes foi apontada como uma dificuldade significativa, impactando o andamento do trabalho em alguns momentos."

Outro desafio notado foi o gerenciamento de tempo. Diversos participantes relataram dificuldades em equilibrar as demandas do projeto com outras responsabilidades acadêmicas e pessoais, o que resultou em atrasos ou em uma execução menos eficiente em algumas etapas. Por fim, o uso das ferramentas disponíveis, embora reconhecido como útil, também apresentou desafios. Alguns participantes indicaram a necessidade de suporte adicional ou treinamento para explorar o potencial completo dessas ferramentas. Isso reforça a importância de preparar os participantes de forma mais estruturada antes do início do projeto. A Tabela 27 apresenta uma síntese sobre a experiência geral e desafios.

**Tabela 27** – Síntese sobre a Experiencia Geral e Desafios

Aspecto Avaliado	Pontos Positivos	Desafios Identificados	Principais Comentários
<i>Aprendizado Prático</i>	Oportunidade de aplicar conhecimentos teóricos em um contexto real.	Adaptação inicial ao ambiente prático e à complexidade dos cenários propostos	"Foi incrível ver como os conceitos teóricos realmente se aplicam em cenários reais."
<i>Colaboração em Equipe</i>	Troca de conhecimentos e desenvolvimento de habilidades interpessoais.	Diferenças de ritmo e estilos de trabalho dificultaram a interação em alguns casos.	"Foi difícil conciliar os diferentes ritmos e estilos de trabalho da equipe."
<i>Familiaridade com Ferramentas</i>	Uso de tecnologias específicas contribuiu para o desenvolvimento de habilidades.	Dificuldades iniciais devido à curva de aprendizado, especialmente para participantes menos experientes.	"No início foi complicado entender algumas ferramentas, especialmente para quem era menos experiente."
<i>Comunicação Interna</i>	O uso de reuniões e canais digitais proporcionou organização.	Falta de alinhamento e clareza nas interações impactaram o andamento do trabalho.	"Às vezes, a falta de clareza prejudicava o andamento das avaliações."

Fonte: Autoria própria

### 7.5.2 Resultados Quantitativos

Os resultados quantitativos, obtidos a partir de perguntas avaliadas em escala de 0 a 10, permitiram identificar tendências claras nos seguintes aspectos:

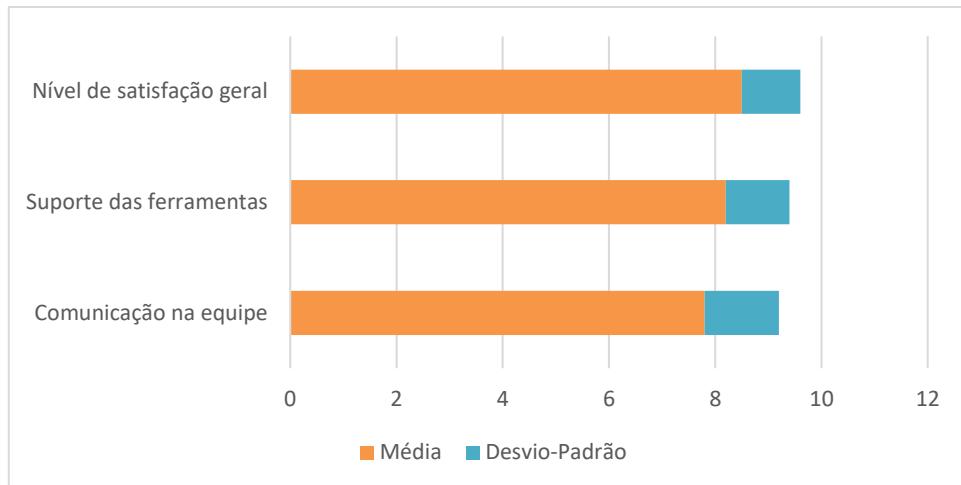
- (i) Comunicação na equipe.
- (ii) Suporte das ferramentas utilizadas.
- (iii) Nível de satisfação geral com o projeto.

Os dados coletados foram analisados em termos de média e desvio-padrão, com os resultados resumidos na Tabela 28 e na Figura 33.

**Tabela 28** – Resultados Quantitativos

Aspecto Avaliado	Média	Desvio-Padrão
Comunicação na equipe	7,8	1,4
Suporte das ferramentas	8,2	1,2
Nível de satisfação geral	8,5	1,1

Fonte: Autoria Própria

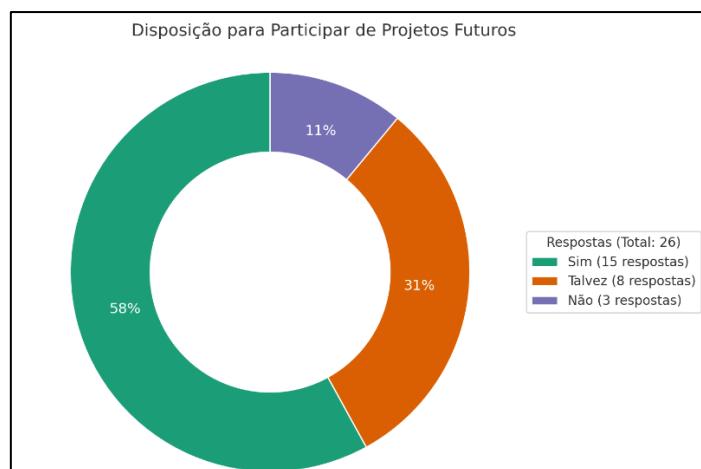


**Figura 33:** Aspectos Quantitativos *Debriefing*. **Fonte:** Autoria própria

Os resultados mostram que o suporte das ferramentas e a satisfação geral destacaram-se como os aspectos mais bem avaliados pelos participantes, apresentando médias de 8,2 e 8,5, respectivamente, o que evidencia uma percepção positiva quanto à utilidade e eficiência das tecnologias utilizadas, bem como ao impacto geral do projeto. Por outro lado, a comunicação interna apresentou a maior variabilidade nos resultados, com um desvio-padrão de 1,4, refletindo uma experiência heterogênea entre os participantes, possivelmente devido a diferenças nos níveis de alinhamento e interação entre as equipes.

### 7.5.3 Recomendação para Projetos Futuros

A disposição dos participantes em repetir experiências semelhantes foi avaliada com base em uma pergunta direta, cujo resultados são apresentados na Figura 34.



**Figura 34:** Participação em Projetos Futuros. **Fonte:** Autoria própria

Os dados indicam que 57,7% dos participantes manifestaram interesse em participar novamente de iniciativas semelhantes, demonstrando uma percepção majoritariamente positiva do projeto. Outros 30,8% manifestaram interesse condicionado, destacando a necessidade de melhorias específicas para aumentar o engajamento e a satisfação nessas iniciativas futuras. Por outro lado, apenas 11,5% dos participantes afirmaram que não participariam novamente, o que sinaliza oportunidades de aprendizado e ajustes na organização e execução de futuros projetos para atender melhor às expectativas dos envolvidos.

#### **7.5.4 Insights Qualitativos e Sugestões de Melhoria**

As respostas abertas trouxeram insights e sugestões para o aprimoramento em projetos futuros. Um dos pontos destacados foi a necessidade de melhorar a comunicação interna, investindo em práticas e ferramentas que facilitem o alinhamento e a colaboração entre os membros das equipes, promovendo um ambiente mais integrado e produtivo. Outra sugestão destacada foi o treinamento inicial. Disponibilizar guias práticos e workshops antes do início do projeto pode ajudar os participantes a utilizarem as ferramentas de forma mais eficiente, reduzindo dificuldades iniciais e potencializando os resultados.

Também foi apontada a importância de um planejamento de prazos mais equilibrado, com cronogramas que considerem as demandas do projeto de maneira mais realista. Essa abordagem pode ajudar na organização das etapas e garantir uma execução mais tranquila, beneficiando o desempenho geral.

#### **7.6 Validação do *Framework***

O *framework QualIoT* apresentou eficácia em promover análises criteriosas e detalhadas de dispositivos IoT no estudo realizado, proporcionando resultados superiores em comparação com abordagens sem suporte metodológico estruturado. A comparação entre o Grupo 1 (que utilizou o *framework*) e o Grupo 2 (que utilizou dimensões isoladas) revelou que o uso do *framework* garantiu avaliações mais precisas e consistentes, particularmente em dimensões críticas como Privacidade e Segurança,

Transmissão de Dados e Análise Avançada. Essa superioridade se refletiu tanto nos resultados quantitativos quanto nos insights qualitativos obtidos durante o estudo.

Os resultados quantitativos destacaram que o Grupo 1 apresentou médias superiores em praticamente todas as dimensões avaliadas. Por exemplo, na dimensão de Privacidade e Segurança, o Grupo 1 atribuiu uma média de 90 a dispositivos avançados, enquanto o Grupo 2 avaliou com uma média de 75, evidenciando diferenças significativas. O desvio-padrão reduzido do Grupo 1 (5,2) também indicou maior homogeneidade e rigor nas respostas, ao contrário do Grupo 2, que apresentou maior variabilidade (desvio-padrão de 12,7). Essa consistência do Grupo 1 sugere a capacidade do *framework* de orientar os avaliadores em critérios mais claros e objetivos, reduzindo a subjetividade nas análises.

Do ponto de vista qualitativo, os participantes que utilizaram o *framework* relataram maior facilidade em identificar limitações técnicas e vulnerabilidades nos dispositivos IoT. Por exemplo, o Grupo 1 foi capaz de apontar falhas específicas em dispositivos avançados, como assistentes virtuais, relacionadas à transparência na coleta de dados e confiabilidade em comandos críticos. Esses aspectos foram subestimados pelo Grupo 2, que priorizou aspectos mais superficiais, como usabilidade e design, sem explorar dimensões técnicas mais complexas.

Os testes estatísticos reforçaram a validade das diferenças observadas entre os grupos. O Teste ANOVA (valor-p de 0,0002) e o Teste T (valor-p de 0,0001) confirmaram que as discrepâncias entre as médias dos dois grupos eram estatisticamente significativas. Esses resultados respaldam a eficácia do *framework* porque as discrepâncias significativas entre os grupos, identificadas pelos testes estatísticos (valor-p < 0,05), indicam que as análises realizadas foram capazes de diferenciar claramente os cenários avaliados. Isso reforça a capacidade do *framework* em capturar diferenças relevantes entre os grupos, promovendo maior precisão e confiabilidade nos resultados.

Além disso, a análise do intervalo de confiança destacou que o Grupo 1 manteve maior precisão nas avaliações, com uma faixa mais estreita de variação (83,5 a 87,3), enquanto o Grupo 2 apresentou maior dispersão (69,1 a 76,5), evidenciando menor consistência. Ou seja, justificando a existência de um *framework* capaz de padronizar os resultados das análises.

Os resultados por categoria de IoT também apontam para a superioridade do *framework*. Para dispositivos básicos, como campainhas inteligentes, o Grupo 1 avaliou com maior equilíbrio as dimensões de Privacidade e Segurança e Transmissão de Dados, enquanto o Grupo 2 superestimou funcionalidades básicas. Nos dispositivos intermediários, como câmeras de segurança, o Grupo 1 destacou vulnerabilidades no gerenciamento de permissões, enquanto o Grupo 2 focou em aspectos gerais, deixando de explorar critérios técnicos fundamentais. Já nos dispositivos avançados, como drones e assistentes virtuais, o Grupo 1 novamente demonstrou ser mais criterioso, apontando aspectos como robustez em segurança e escalabilidade, enquanto o Grupo 2 priorizou elementos de uso, sem identificar falhas críticas.

Por fim, o *debriefing* corroborou os resultados quantitativos, evidenciando que os avaliadores do Grupo 1 reconheceram a importância do *framework* na organização das análises e na identificação de limitações técnicas que passaram despercebidas pelo Grupo 2. Além disso, os participantes sugeriram melhorias relacionadas à comunicação interna e ao treinamento inicial para maximizar a eficiência do *framework*. A partir dessas evidências, conclui-se que, para grupo estudado, o *framework QualIoT* não apenas promoveu análises mais completas e consistentes, mas também demonstrou seu potencial para elevar a qualidade das avaliações em sistemas IoT, podendo contribuindo para o avanço científico e tecnológico engenharia de requisitos.

## 7.7 Comparação com *Frameworks*

A revisão da literatura realizada na Seção 3.3.1 demonstrou que *frameworks* existentes para avaliação de maturidade em IoT apresentam limitações importantes na cobertura de critérios essenciais para a engenharia de requisitos e para a qualidade dos sistemas IoT. Esses *frameworks*, apesar de relevantes em seus contextos, geralmente abordam aspectos específicos (como segurança ou gestão de risco), deixando lacunas em áreas como usabilidade, qualidade de dados, engenharia de requisitos e validação prática.

A aplicação do *QualIoT* no estudo de caso permitiu comprovar empiricamente que o *framework* proposto não apenas cobre essas dimensões de forma completa, mas também oferece um suporte prático e integrado para a avaliação da maturidade dos requisitos em

sistemas IoT. Para reforçar essa evidência, esta seção apresenta uma análise visual da cobertura prática dos *frameworks* analisados, considerando os seguintes critérios:

QD – Qualidade de Dados

S – Segurança

U – Usabilidade

ER – Engenharia de Requisitos

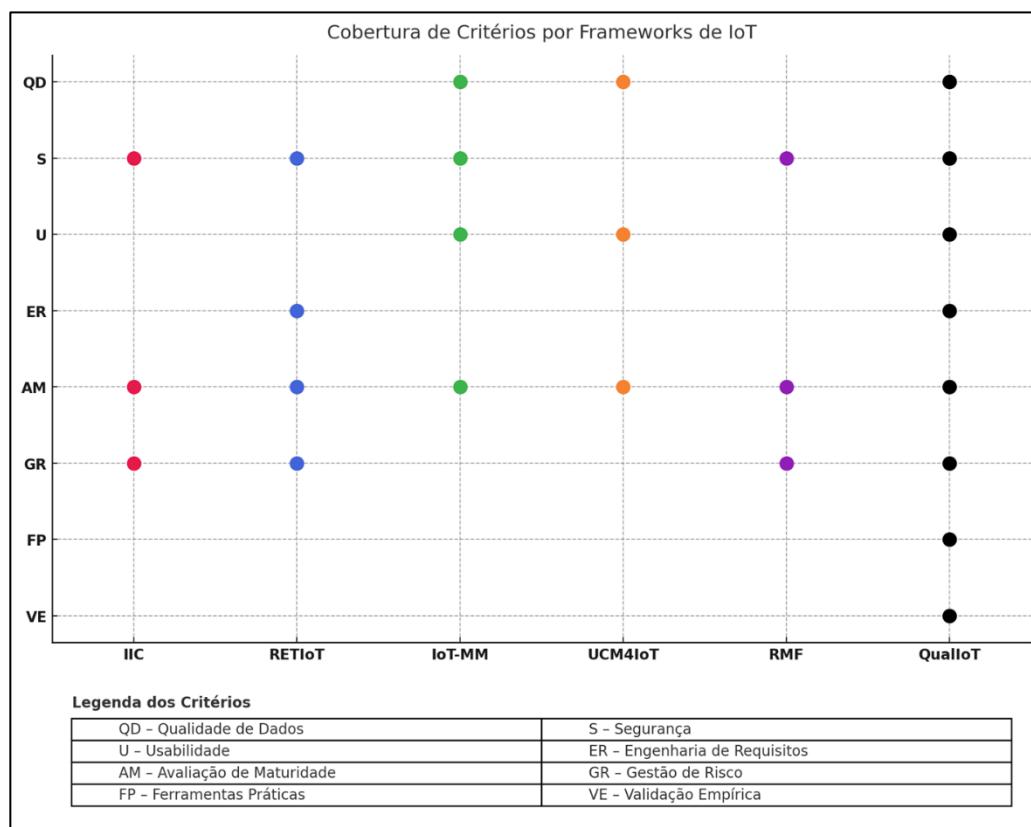
AM – Avaliação de Maturidade

GR – Gestão de Risco

FP – Ferramentas Práticas

VE – Validação Empírica

A Figura 35 apresenta um gráfico comparativo, construído com base na análise dos *frameworks* da Seção 3.3.1, complementada pelos resultados práticos observados com a aplicação do *QualIoT* no estudo de caso. Cada eixo do gráfico representa um dos critérios avaliados, permitindo visualizar a abrangência de cada *framework*.



**Figura 35:** Comparação de *frameworks*. **Fonte:** Autoria própria

A análise visual reforça que o *QualIoT* é o único *framework* que atinge cobertura total em todas as dimensões avaliadas. Em contrapartida, os demais frameworks apresentam lacunas relevantes:

- (i) Segurança (S) e Gestão de Risco (GR) são bem tratadas em frameworks como o *IoT Security Maturity Model* e o *IoT Risk & Maturity Framework*, mas esses modelos não contemplam adequadamente usabilidade, engenharia de requisitos e qualidade de dados.
- (ii) Usabilidade (U) e Qualidade de Dados (QD), que são fundamentais para garantir soluções IoT centradas no usuário e com informações confiáveis, são consistentemente negligenciadas nos *frameworks* analisados.
- (iii) Engenharia de Requisitos (ER) — uma dimensão central para garantir o alinhamento entre requisitos e solução IoT — é abordada apenas parcialmente ou ausente em todos os *frameworks*, com exceção do *QualIoT*.
- (iv) Ferramentas Práticas (FP) e Validação Empírica (VE) são critérios essenciais para viabilizar a aplicação dos *frameworks* em ambientes reais. Aqui novamente o *QualIoT* se destaca por ter sido aplicado em estudo de caso com análise quantitativa e qualitativa dos resultados.

A análise visual complementa a comparação qualitativa realizada anteriormente, evidenciando que o *QualIoT* oferece uma abordagem fundamentada, integrada e validada para avaliação da maturidade dos requisitos em sistemas IoT. Essa abrangência diferencia o *QualIoT* e reforça seu potencial para apoiar a melhoria contínua em sistemas IoT.

## 7.8 Conclusão do Capítulo.

Neste capítulo, foram analisados os resultados obtidos com a aplicação do *framework* *QualIoT*, permitindo avaliações quantitativas e qualitativas dos dispositivos IoT. A comparação entre os grupos demonstrou que o uso do *framework* contribuiu para análises mais técnicas, consistentes e equilibradas, enquanto o grupo sem apoio estruturado teve maior dificuldade em identificar critérios e vulnerabilidades específicas.

Esses resultados evidenciam a importância de abordagens sistemáticas na avaliação de sistemas IoT, promovendo maior precisão e redução da subjetividade. A

aplicação do *QualIoT* também revelou áreas críticas de melhoria, como segurança, privacidade e transmissão de dados, fornecendo subsídios práticos para avanços futuros.

De forma geral, os dados reforçam o valor do uso de metodologias organizadas como o *QualIoT* no contexto da engenharia de requisitos, contribuindo para avaliações mais confiáveis e alinhadas às demandas do mercado. As evidências apresentadas servem como base para futuras pesquisas e para o desenvolvimento de soluções mais maduras e seguras em ambientes tecnológicos complexos.

O próximo capítulo aprofunda as implicações práticas desses achados, destacando as contribuições da pesquisa para a área de IoT e apontando caminhos para trabalhos futuros.

## **8. Conclusão**

Este capítulo final aborda os aspectos relacionados à avaliação de soluções IoT, destacando os desafios de subjetividade na atribuição de pontuações e a importância de critérios abrangentes e atualizáveis. Além disso, apresenta as limitações da pesquisa, as considerações finais e os próximos passos para continuidade dos trabalhos.

### **8.1 Limitações da Pesquisa**

A atribuição de pontuações em avaliações de soluções IoT pode ser influenciada por interpretações individuais, especialmente quando os critérios adotados não são suficientemente claros ou padronizados. Avaliadores distintos podem atribuir pesos diferentes a determinados aspectos, o que impacta diretamente a consistência dos resultados.

Além disso, a lista de critérios utilizados para calcular a pontuação pode não ser exaustiva, deixando de considerar outros aspectos relevantes. Os sistemas IoT são complexos e multifacetados, e critérios importantes, como interoperabilidade com outros sistemas ou facilidade de manutenção, podem não estar incluídos na avaliação inicial.

Para garantir uma análise mais completa e precisa, é fundamental revisar e atualizar periodicamente as dimensões, os critérios de avaliação e as perguntas norteadoras, incorporando novos aspectos conforme necessário.

Uma das principais limitações do estudo de caso está relacionada à restrição da amostra e ao contexto específico de aplicação. Os participantes foram selecionados exclusivamente entre estudantes do curso de Sistemas de Informação, com idade e formação homogêneas. Embora isso tenha garantido um nível técnico consistente entre os grupos, restringiu a generalização dos resultados para outros perfis, como profissionais experientes ou indivíduos com menos familiaridade com tecnologias IoT.

A pesquisa foi realizada em um ambiente controlado de laboratório, o que pode não refletir integralmente os desafios enfrentados em cenários reais de aplicação, como limitações de infraestrutura, recursos financeiros e restrições operacionais frequentemente encontradas em projetos IoT no mercado.

Outro ponto a destacar refere-se às limitações metodológicas inerentes ao experimento. A divisão dos grupos e a utilização do *framework* completo *versus* dimensões isoladas podem ter gerado viés cognitivo, uma vez que os participantes do Grupo 2, sem acesso às perguntas norteadoras, enfrentaram maior esforço subjetivo na avaliação. Isso pode ter influenciado as discrepâncias observadas nos resultados.

A dependência de dados autorrelatados e da observação direta pode introduzir vieses interpretativos, ainda que tenham sido adotadas estratégias para minimizar esses impactos.

Embora o *QualIoT* tenha sido aplicado a um conjunto específico de dispositivos no estudo de caso, seu modelo é flexível e pode ser adaptado a diferentes domínios da IoT, como ambientes hospitalares, industriais ou domésticos. A personalização pode ocorrer pela seleção de dimensões mais relevantes a cada cenário ou pela reformulação das perguntas norteadoras, mantendo a estrutura do *framework*, mas ajustando seu foco conforme o contexto de uso.

Por fim, a classificação de uma solução para mensurar requisitos IoT pode mudar ao longo do tempo, à medida que novas tecnologias e funcionalidades são desenvolvidas. O campo da IoT está em constante evolução, com inovações frequentes que podem melhorar significativamente o desempenho e as capacidades das soluções existentes. Avanços em inteligência artificial, segurança cibernética e redes de comunicação podem alterar a avaliação, elevando seu nível de maturidade. Portanto, é importante que as avaliações sejam revisadas regularmente para refletir essas mudanças tecnológicas, garantindo que as classificações permaneçam relevantes e precisas. Essa abordagem dinâmica assegura que as soluções IoT continuem a atender às necessidades e expectativas, mantendo-se competitivas no mercado.

## 8.2 Considerações Finais

O presente estudo propõe um *framework* para a validação de requisitos em sistemas IoT, visando atender à crescente demanda por soluções confiáveis e seguras nesse contexto. A motivação para este trabalho reside na complexidade crescente dos sistemas IoT, nos altos custos associados a falhas e nos riscos à segurança e privacidade.

Por meio de uma revisão da literatura e da análise de casos reais, identificamos a necessidade de um método sistemático para a validação de requisitos em sistemas IoT. O *framework* proposto aborda essa necessidade ao fornecer um conjunto de técnicas e ferramentas que permitem a identificação, análise e verificação de requisitos de forma eficiente e eficaz.

Assim, o *QualIoT* cumpre uma dupla função: além de promover qualidade na estruturação dos requisitos, oferece suporte direto à avaliação da maturidade das soluções, permitindo um diagnóstico prático e orientado à evolução contínua dos dispositivos IoT.

A principal contribuição deste trabalho foi o desenvolvimento de uma metodologia que auxilia os desenvolvedores de sistemas IoT a garantir a qualidade e a confiabilidade de seus produtos. Ao seguir os passos propostos no *framework*, é possível minimizar os riscos de falhas, otimizar o processo de desenvolvimento e atender às expectativas dos usuários.

## Referências

AAQIB, M.; ALI, A.; CHEN, L.; et al. IoT trust and reputation: a survey and taxonomy. *J Cloud Computing*, v. 12, p. 42, 2023. doi: 10.1186/s13677-023-00416-8.

ALABA, F. A.; OTHMAN, M.; HASHEM, I. A. T.; AL-OTAIBI, F. Internet of Things security: A survey. *Journal of Network and Computer Applications*, v. 88, p. 10-28, 2017. doi: 10.1016/j.jnca.2017.04.002.

ALI, M. I.; ONO, N.; KAYSAR, M.; et al. Real-Time Data Analytics and Event Detection for IoT-Enabled Communication Systems. *SSRN Electronic Journal*, 2017. doi: 10.2139/ssrn.3199128.

ALMEIDA, E. M.; PERES, L. M.; L'ERARIO, A. An Approach to Use Comic Strips To Support IoT Systems Requirements Engineering. In: *IEEE FRONTIERS IN EDUCATION CONFERENCE (FIE)*, 2022, Uppsala. IEEE, 2022. p. 1-6. doi: 10.1109/FIE56618.2022.9962579.

AMEYED, D.; JAAFAR, F.; PETRILLO, et al. Quality and Security Frameworks for IoT-Architecture Models Evaluation. *SN Computing Science*, v. 4, p. 394, 2023. doi: 10.1007/s42979-023-01815-z.

ARMBRUST, M.; et al. A View of Cloud Computing. *Communications of the ACM*, v. 53, n. 4, p. 50–58, 2010. doi: 10.1145/1721654.1721672.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. *Computer Networks*, v. 54, n. 15, p. 2787-2805, 2010. doi: 10.1016/j.comnet.2010.05.010.

BANERJEE, T.; SHETH, A. IoT Quality Control for Data and Application Needs. *IEEE Intelligent Systems*, v. 32, n. 2, p. 68-73, mar./abr. 2017. doi: 10.1109/MIS.2017.35.

BOTTA, A.; DONATO, W. de; PERSICO, V.; PESCAPÉ, A. Integration of Cloud Computing and Internet of Things: A Survey. *Future Generation Computer Systems*, v. 56, p. 684-700, 2016. doi: 10.1016/j.future.2015.09.021.

BRYMAN, A. *Social Research Methods*. 5. ed. Oxford: Oxford University Press, 2016.

COSTA, B.; PIRES, P. F.; DELICATO, F. C. Specifying Functional Requirements and QoS Parameters for IoT Systems. In: *IEEE INTERNATIONAL CONFERENCE ON DEPENDABLE, AUTONOMIC AND SECURE COMPUTING (DASC)*, 2017,

Orlando. IEEE, 2017. p. 407-414. doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.83.

CRESWELL, J. W. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4. ed. Thousand Oaks, CA: Sage, 2014.

DENZIN, N. K. The Sage Handbook of Qualitative Research. Thousand Oaks, CA: Sage Publications, 2012.

DIJKMAN, R. M.; SPRENKELS, B.; PEETERS, T.; JANSSEN, A. Business models for the Internet of Things. International Journal of Information Management, v. 35, n. 6, p. 672–678, 2015. doi: 10.1016/j.ijinfomgt.2015.07.008.

FENTON, N. E.; PFLEEGER, S. L. Software Metrics: A Rigorous and Practical Approach. Boston: PWS Publishing Co., 1998.

FORTINO, G.; TRUNFIO, P.; GRAVINA, R.; et al. Internet of Things for Smart Environments: Technologies and Applications. Springer, 2018.

GE, M.; BANGUI, H.; BUHNOVA, B. Big Data for Internet of Things: A Survey. Future Generation Computer Systems, v. 87, p. 601-614, 2018. doi: 10.1016/j.future.2018.04.053.

GLINZ, M. M. Glinz, "On Non-Functional Requirements," 15th IEEE International Requirements Engineering Conference (RE 2007), Delhi, India, 2007, pp. 21-26, doi: 10.1109/RE.2007.45.

GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, v. 29, n. 7, p. 1645-1660, 2013. doi: 10.1016/j.future.2013.01.010.

HWANG, C. L.; YOON, K. Multiple Attribute Decision Making: Methods and Applications. Springer, 1981.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 25030:2019. Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) Quality requirements Framework.

KALEEM, S.; AHMAD, S.; BABAR, M.; AKRE V.; RAIAN A.; ULLAH F.; "A Review on Requirements Engineering for Internet of Things (IoT) Applications," 2019

Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 2019, pp. 269-275, doi: 10.1109/ITT48889.2019.9075078.

KARKOUCH, Aimad; MOUSANNIF, Hajar; AL MOATASSIME, Hassan; NOEL, Thomas. Data quality in internet of things: A state-of-the-art survey. *Journal of Network and Computer Applications*, v. 73, p. 57–81, 2016. ISSN 1084-8045. DOI: <https://doi.org/10.1016/j.jnca.2016.08.002>.

KARLSSON, J.; WOHLIN, C.; REGNELL, B. An evaluation of methods for prioritizing software requirements. *Information and Software Technology*, v. 39, p. 939-947, 1998. doi: 10.1016/S0950-5849(97)00053-0.

KITCHENHAM, B. Procedures for performing systematic reviews. Keele, UK: Keele University, 2004. doi: 10.1.1.122.3308.

LEHMAN, M. M.; BELADY, L. A. *Program Evolution: Processes of Software Change*. Academic Press, 1985.

LI, S.; XU, L. D.; ZHAO, S. The internet of things: a survey. *Information Systems Frontiers*, v. 17, p. 243–259, 2015. doi: 10.1007/s10796-014-9492-7.

LIKERT, R. A Technique for the Measurement of Attitudes. *Archives of Psychology*, v. 140, p. 1-55, 1932.

LINCOLN, Y. S.; GUBA, E. G. *Naturalistic Inquiry*. Sage Publications, 1985.

MAXWELL, J. A. *Qualitative Research Design: An Interactive Approach*. 3. ed. Thousand Oaks, CA: Sage, 2013.

MINANI, J. B.; SABIR, F.; MOHA, N.; GUÉHÉNEUC, Y.-G. A Systematic Review of IoT Systems Testing: Objectives, Approaches, Tools, and Challenges. *IEEE Transactions on Software Engineering*, v. 50, n. 4, p. 785-815, abr. 2024. doi: 10.1109/TSE.2024.3363611.

MIORANDI, D.; SICARI, S.; DE PELLEGRINI, F.; CHLAMTAC, I. Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, v. 10, n. 7, p. 1497–1516, 2012. doi: 10.1016/j.adhoc.2012.02.016.

NAKAJIMA, T.; KOMIYAMA, T. Applying Quality Requirements Framework to an IoT System and its Evaluation. In: INTERNATIONAL CONFERENCE ON QUALITY REQUIREMENTS FRAMEWORK, 2019. p. 28-36.

NIELSEN, J. Usability Engineering. San Francisco: Morgan Kaufmann Publishers Inc., 1994.

NOORZADEH, A.; AMINI, A. Comparison of Requirements Engineering Methods for IoT-based Systems: A Systematic Mapping Study. In: INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND ROBOTICS (QICAR), 10., 2024, Qazvin. IEEE, 2024. p. 74-79. doi: 10.1109/QICAR61538.2024.10496655.

PATTON, M. Q. Qualitative Research and Evaluation Methods. 4. ed. Thousand Oaks, CA: Sage, 2015.

PAUL, P. V.; SARASWATHI, R. The Internet of Things — A comprehensive survey. In: INTERNATIONAL CONFERENCE ON COMPUTATION OF POWER, ENERGY INFORMATION AND COMMUNICATION (ICCP-EIC), 2017, Melmaruvathur. IEEE, 2017. p. 421-426. doi: 10.1109/ICCP-EIC.2017.8290405.

PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. Context aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, v. 16, n. 1, p. 414-454, 2014. doi: 10.1109/SURV.2013.042313.00197.

PEREZ-CASTILLO, R.; et al. Data Quality Best Practices in IoT Environments. In: INTERNATIONAL CONFERENCE ON THE QUALITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (QUATIC), 2018, Coimbra. Anais [...]. IEEE, 2018. p. 272-275. doi: 10.1109/QUATIC.2018.00048.

PLAGERAS, A. P.; PSANNIS, K. E.; STERGIOU, C.; WANG, H.; GUPTA, B. B. Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. Future Generation Computer Systems, v. 82, p. 349-357, 2018. doi: 10.1016/j.future.2017.09.082.

PRESSMAN, R. S.; MAXIM, B. Software Engineering: A Practitioner's Approach. New York: McGraw-Hill Education, 2014.

ROMAN, R.; NAJERA, P.; LOPEZ, J. Securing the Internet of Things. IEEE Computer, v. 44, n. 9, p. 51-58, 2011. doi: 10.1109/MC.2011.291.

SAATY, T. L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. New York: McGraw-Hill, 1980.

SANDELOWSKI, M. Sample Size in Qualitative Research. *Research in Nursing & Health*, v. 18, n. 2, p. 179-183, abr. 1995. doi: 10.1002/nur.4770180211.

SCHNEIER, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company, 2015.

SHAH, J. L.; BHAT, H. F.; KHAN, A. I. Integration of Cloud and IoT for smart e-healthcare. In: *Healthcare Paradigms in the Internet of Things Ecosystem*. Academic Press, 2021. p. 101-136. doi: 10.1016/B978-0-12-819664-9.00006-5.

STERGIOU, C.; PSANNIS, K. E.; KIM, B.-G.; GUPTA, B. Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, v. 78, p. 964-975, 2018. doi: 10.1016/j.future.2016.11.031.

TROCHIM, W. M. K. *Research Methods Knowledge Base*. 2. ed. Cincinnati: Atomic Dog Publishing, 2006.

TYAGI, H.; KUMAR, R. Cloud Computing for IoT. In: *Internet of Things (IoT)*. Springer, 2020. p. 13-26. doi: 10.1007/978-3-030-37468-6\_2.

WYATT, L.; HELAL, A.; AHMED, E.; KHALED, K. Health-IoT: Requirements for a Healthy Ecosystem. In: *SPLITECH 2022*. IEEE, 2022. doi: 10.23919/SpliTech55088.2022.9854349.

YIN, R. K. *Case Study Research and Applications: Design and Methods*. 6. ed. Thousand Oaks, CA: Sage, 2018.

ZAMAN, M.; PURYEAR, N.; ABDELWAHED, S.; ZOHRABI, N. A Review of IoT-Based Smart City Development and Management. *Journal of Smart Cities*, v. 7, p. 1462-1500, 2024. doi: 10.3390/smartcities7030061.

ZANELLA, A.; BUI, N.; CASTELLANI, A.; VANGELISTA, L.; ZORZI, M. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, v. 1, n. 1, p. 22-32, 2014. doi: 10.1109/JIOT.2014.2306328.

# APÊNDICE I

Artigo de Revisão de Literatura publicado no XX Workshop de Computação da UNIFACCAMP

## Análise sobre Engenharia de Requisitos e Qualidade de Software para Sistemas IoT: Uma Revisão Sistemática da Literatura

Luis Fernando dos Santos Pires<sup>1</sup>,

<sup>1</sup>Universidade Campo Limpo Paulista (UNIFACCAMP)  
Campo Limpo Paulista – SP – Brazil

[luis.spires@outlook.com](mailto:luis.spires@outlook.com)

**Abstract.** *The Internet of Things (IoT) is a technology that transforms human interaction with the digital environment by connecting everyday devices to the global network. However, the diversity and complexity of IoT devices also present significant challenges. In this context, this study conducted a systematic literature review, focusing on the analysis of requirements engineering and software quality in IoT systems, aiming to discover dimensions for improving these devices. The findings of this review reveal concern in metrics, requirements elicitation in IoT, and the measurement of the quality of these systems.*

**Resumo.** *A Internet das Coisas (IoT) é uma tecnologia que transforma a interação humana com o ambiente digital ao conectar dispositivos cotidianos à rede global. No entanto, a diversidade e complexidade dos dispositivos IoT também apresentam desafios significativos. Nesse contexto, este estudo realizou uma revisão sistemática da literatura, focando na análise da engenharia de requisitos e qualidade de software em sistemas IoT visando descobrir dimensões para melhoria destes dispositivos. Os achados dessa revisão revelam a preocupação nas métricas, elicitação de requisitos em IoT e na mensuração da qualidade destes sistemas.*

### Introdução

A Internet das Coisas (IoT) está transformando o cotidiano ao conectar o mundo físico ao virtual. Segundo Aaqib, M. et al. (2023), a IoT é uma das tecnologias de crescimento mais rápido, com mais de um bilhão de dispositivos previstos até 2030. B. Costa et al. (2016) afirmam que a IoT visa melhorar a qualidade de vida e otimizar processos industriais. L. Médini et al. (2017) destacam que a IoT impacta todos os aspectos da vida, mas traz desafios que precisam ser superados para seu uso responsável e eficiente. P. P. Ray et al. (2018) enfatizam a importância de garantir a qualidade das soluções IoT. A. Noorzadeh et al. (2024) apontam a complexidade da engenharia de requisitos (ER) para sistemas IoT devido às suas características inerentes. A. P. Plageras et al. (2018) ressaltam que, sem qualidade, os dados da IoT perdem valor. S. Kaleem et al. (2019) destacam a necessidade de focar no ciclo de vida de desenvolvimento de software (SDLC) para garantir a qualidade necessária. Este estudo tem como principal objetivo responder à seguinte questão de pesquisa: “Como a engenharia de requisitos e a qualidade de software podem promover melhorias em sistemas IoT?”. Além de analisar e classificar os estudos de acordo com as abordagens técnicas empregadas, este artigo também discute os fundamentos em IoT e seu impacto na sociedade. O objetivo principal é identificar técnicas, teorias, aspectos positivos e limitações relacionados à qualidade da IoT. Os pontos fortes e contribuições dos estudos são identificados, bem como suas limitações metodológicas e de generalização. Além disso, o objetivo é destacar os

Publicado em: 2024 – ISSN: 2447-4703 – Anais do XX WCF 2024 – Página: 1

Link de acesso: [https://www.cc.faccamp.br/anaisdowcf/edicao\\_atual/wcf2024/1/](https://www.cc.faccamp.br/anaisdowcf/edicao_atual/wcf2024/1/)

## APÊNDICE II

Artigo Estendido da Revisão de Literatura publicado na Revista FT – Qualis B2



ISSN 1678-0817 Qualis B2

### ANÁLISE SOBRE ENGENHARIA DE REQUISITOS E QUALIDADE DE SOFTWARE PARA SISTEMAS IOT: UMA REVISÃO SISTEMÁTICA DA LITERATURA

[Engenharia da Computação, Volume 29 - Edição 142/JAN 2025 / 27/01/2025](#)

REGISTRO DOI: 10.69849/revistaft/th102501271116

Luis Fernando dos Santos Pires<sup>1</sup>

#### Resumo

A Internet das Coisas (IoT) é uma tecnologia que transforma a interação humana com o ambiente digital ao conectar dispositivos cotidianos à rede global. Essa integração cria possibilidades para comunicação entre pessoas e empresas. No entanto, a diversidade e complexidade dos dispositivos IoT também apresentam desafios significativos. Para garantir a qualidade, interoperabilidade, segurança e eficiência operacional, é essencial estabelecer requisitos claros e objetivos. Nesse contexto, este estudo realizou uma revisão sistemática da literatura, focando na análise da engenharia de requisitos e qualidade de software em sistemas IoT visando descobrir dimensões para melhoria destes dispositivos. Foram analisados 27 estudos selecionados por suas metodologias, incluindo abordagens de engenharia de requisitos, qualidade de software e bases teóricas sólidas. Esses estudos contemplam perspectivas de crescimento da IoT no cenário mundial. Os achados dessa revisão revelam a

Publicado em 27/01/2025 - ISSN: 1678-0817 - Volume 29 - Edição 142- Págs 16

Registro DOI: <https://www.doi.org/.69849/revistaft/th102501271116>

## APÊNDICE III

### Autorização para pesquisa nas Faculdades Integradas Rio Branco



#### TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Eu, Prof. Dr. José Maria de Souza Junior, Diretor das Faculdades Integradas Rio Branco, declaro que estou ciente e autorizo o pesquisador **Luis Fernando dos Santos Pires** a desenvolver a pesquisa intitulada "*Um Framework para Mensuração da Maturidade de Requisitos de Sistemas em IoT*", nos trabalhos desenvolvidos nas disciplinas do curso de Bacharelado em Sistemas de Informação, conjuntamente com os professores responsáveis pela disciplina. Esta pesquisa pretende validar um framework para a mensuração da maturidade dos requisitos em sistemas de Internet das Coisas (IoT), visando analisar a qualidade dos requisitos levantados e o impacto do framework na melhoria da eficácia dos sistemas IoT.

A participação dos alunos e demais professores é voluntária e se dará por meio de questionários presenciais e discussões relacionadas ao impacto do framework em comparação com métodos tradicionais de avaliação de requisitos. Os riscos decorrentes da participação dos alunos e professores são conhecidos e todas as ações necessárias para minimizar e mitigar esses riscos serão tomadas. Toda e qualquer responsabilidade ética e científica decorrente desta pesquisa é de responsabilidade exclusiva do pesquisador.

Estou ciente que, mesmo após consentir, posso desistir de continuar participando da pesquisa a qualquer momento, sem nenhum tipo de ônus ou prejuízo ao curso ou à faculdade. Os resultados da pesquisa serão analisados e publicados, sendo todas as identidades preservadas e guardadas em sigilo. Para qualquer outra informação, o(a) Sr(a) pode entrar em contato com o pesquisador responsável no **Centro Universitário Campo Limpo Paulista (FACCAMP)**, pelo telefone **11 94970-3282**.

Se o(a) Sr(a) se sentir suficientemente esclarecido(a) sobre essa pesquisa, objetivo, procedimentos e eventuais riscos e benefícios, convido-o(a) a assinar este Termo, elaborado em duas vias, sendo que uma ficará com o(a) Sr(a) e a outra com o pesquisador.

Se o(a) Sr(a) se sentir suficientemente esclarecido sobre essa pesquisa, objetivo, procedimentos e eventuais riscos e benefícios, convido-o(a) a assinar este Termo, elaborado em duas vias, sendo que uma ficará com o(a) Sr(a) e a outra com o pesquisador.

Cotia, 23 de outubro de 2024.

JOSE MARIA DE  
SOUZA  
JUNIOR:32610417810

Assinado de forma digital por  
JOSE MARIA DE SOUZA  
JUNIOR:32610417810  
Dados: 2024.10.21 22:23:16  
-03'00'

Assinatura do Diretor das Faculdades

Luis Fernando dos Santos Pires  
(Responsável pela pesquisa)

#### Identificação:

Nome: José Maria de Souza Junior

RG: 33.59.83.00-5

CPF: 326.104.178/10

Telefone: 1198350-4327

Endereço: Rod. Raposo Tavares – KM 24, Granja Viana, Cotia – São Paulo/SP, CEP:06709-105

#### Para questões associadas com esse estudo:

Entrar em contato com Luis Fernando dos Santos Pires – Telefone (11194970-3282)

## APÊNDICE IV

TCLE submetido e aprovado pelo CEP da Universidade Santo Amaro (UNISA)

1



### Termo de Consentimento Livre e Esclarecido - TCLE

**PROTOCOLO:** Um Framework para Mensuração da Maturidade de Requisitos de Sistemas em IoT

Estes esclarecimentos estão sendo apresentados para solicitar sua participação livre e voluntária no projeto **Um Framework para Mensuração da Maturidade de Requisitos de Sistemas em IoT**, do Programa de **Mestrado Profissional em Ciências da Computação** do Centro Universitário Campo Limpo Paulista - **UNIFACCAMP**, que será realizado pelo pesquisador **Luis Fernando dos Santos Pires** como Trabalho de Conclusão de Curso sob orientação do **Prof Dr. Rodrigo Bonacin**.

A **Internet das Coisas (IoT)** tem transformado a forma como interagimos com dispositivos e sistemas inteligentes. No entanto, um dos desafios desse crescimento tecnológico é garantir que os requisitos de software e hardware sejam bem definidos e avaliados para que os sistemas sejam seguros, confiáveis e eficientes. A ausência de um método estruturado para mensurar a maturidade dos requisitos pode resultar em falhas operacionais, insegurança dos dados e retrabalho no desenvolvimento dos sistemas.

Essa pesquisa tem o objetivo de preencher essa lacuna por meio do desenvolvimento e validação de um framework específico para mensurar a maturidade dos requisitos em sistemas IoT. A realização deste estudo permitirá identificar pontos críticos no processo de engenharia de requisitos e aprimorar metodologias de desenvolvimento, beneficiando tanto desenvolvedores quanto usuários finais. A participação dos alunos no estudo é fundamental para avaliar a aplicabilidade e eficácia do framework, permitindo verificar como ele pode ser utilizado para otimizar a especificação de requisitos e reduzir falhas em projetos IoT.

O objetivo principal desta pesquisa é **desenvolver e validar um framework para mensuração da maturidade dos requisitos em sistemas IoT**, possibilitando avaliar a qualidade dos requisitos e garantir maior segurança e confiabilidade no desenvolvimento desses sistemas. Para alcançar esse objetivo, serão aplicadas técnicas de análise comparativa entre abordagens tradicionais de engenharia de requisitos e a metodologia proposta no framework.

Serão propostas melhorias e ajustes na ferramenta desenvolvida, a partir dos resultados obtidos com os participantes da pesquisa. Os testes serão conduzidos com alunos do **3º e 4º semestre do curso de Sistemas de Informação das Faculdades Integradas Rio Branco**, que contribuirão para a validação do framework por meio de experimentos práticos e avaliações qualitativas e quantitativas.

---

Luis Fernando dos Santos Pires - Rua Henrique Schurig, 495 – Jd. Fernandes, São Paulo, SP – CEP: 03580-060, Fone: 11 94970-3282; Prof. Dr. Rodrigo Bonacin, - Rua Guatemaia, 167 - Jardim América, Campo Limpo Paulista - SP, CEP: 13231-230, Fone(s): (11) 4812-9400 (Secretaria de Pós-graduação) ou 19 98136-2352.

Comitê de Ética em Pesquisa – Unisa - Rua Prof. Enéas de Siqueira Neto, 340 cep: 04829-300 São Paulo – SP, Fone: (11) 2141-8687 - [www.unisa.br](http://www.unisa.br)

Esta pesquisa segue rigorosamente os princípios éticos que norteiam estudos envolvendo seres humanos, conforme as diretrizes do **Comitê de Ética em Pesquisa (CEP)** e a **Resolução 466/12 do Conselho Nacional de Saúde (CNS)**. Esses princípios incluem **autonomia**, assegurando que cada participante tem o direito de decidir voluntariamente sobre sua participação, sem qualquer tipo de coerção ou prejuízo em caso de desistência; **beneficência**, garantindo que a pesquisa traga avanços científicos e acadêmicos sem causar danos aos envolvidos; **não maleficência**, assegurando que todos os riscos sejam minimizados ao máximo e que os participantes não sejam expostos a situações prejudiciais; e **justiça**, garantindo que todos os envolvidos tenham acesso às informações da pesquisa e que os benefícios do estudo sejam distribuídos de forma equitativa.

A transparência e o respeito aos participantes são compromissos fundamentais desta pesquisa, e qualquer dúvida ou necessidade de esclarecimento poderá ser prontamente atendida pela equipe responsável.

É garantido o acesso, em qualquer etapa do estudo, aos profissionais responsáveis pela pesquisa para **esclarecimento de eventuais dúvidas ou informações** sobre os resultados parciais das pesquisas, quando em estudos abertos, ou de resultados que sejam do conhecimento dos pesquisadores. O pesquisador responsável é **Luis Fernando dos Santos Pires** que pode ser encontrado no endereço: Rua Henrique Schurig, 495 – Jd. Fernandes, São Paulo, SP – CEP: 03580-060, Telefone (s)11 94970-3282, ou Prof. Dr. Rodrigo Bonacin, que pode ser encontrado no endereço: Rua Guatemala, 167 - Jardim América, Campo Limpo Paulista - SP, CEP:13231-230 Telefone (s): (11) 4812-9400 (Secretaria de Pós-graduação) ou 19 98136-2352.

Se você tiver alguma consideração ou dúvida sobre a ética da pesquisa, entre em contato com o Comitê de Ética em Pesquisa (CEP-UNISA) – Rua Prof. Enéas de Siqueira Neto, 340, Jardim das Imbuínas, SP – Tel.: 2141-8687.

É garantida sua liberdade da retirada de consentimento a qualquer momento e deixar de participar do estudo, sem qualquer prejuízo à continuidade de qualquer benefício que você tenha obtido junto à Instituição, antes, durante ou após o período deste estudo. As informações obtidas pelos pesquisadores serão analisadas em conjunto com as de outros participantes, **não sendo divulgada a identificação** de nenhum deles. Não há **despesas pessoais** para o participante em qualquer fase do estudo, incluindo exames e consultas. Também não há **compensação financeira** relacionada à sua participação. Se existir qualquer despesa adicional, ela será absorvida pelo orçamento da pesquisa.

---

Luis Fernando dos Santos Pires - Rua Henrique Schurig, 495 – Jd. Fernandes, São Paulo, SP – CEP: 03580-060, Fone: 11 94970-3282; Prof. Dr. Rodrigo Bonacin, - Rua Guatemala, 167 - Jardim América, Campo Limpo Paulista - SP, CEP: 13231-230, Fone(s): (11) 4812-9400 (Secretaria de Pós-graduação) ou 19 98136-2352.

Comitê de Ética em Pesquisa – Unisa - Rua Prof. Enéas de Siqueira Neto, 340 cep: 04829-300 São Paulo – SP, Fone: (11) 2141-8687 - www.unisa.br

A pesquisa será realizada de forma **presencial e consistirá em sessões práticas** de avaliação de requisitos em sistemas IoT, nas quais os participantes serão divididos em dois grupos. O primeiro grupo utilizará o framework proposto para a análise de requisitos, enquanto o segundo grupo realizará a mesma atividade sem o auxílio da ferramenta, utilizando apenas o conhecimento adquirido em sala de aula. Os participantes responderão **questionários individuais**, nos quais deverão avaliar a clareza e a eficácia do framework, além de descrever sua experiência ao aplicar a ferramenta. Ao final do estudo, será realizada uma **discussão em grupo**, permitindo a troca de opiniões sobre a experiência com os métodos utilizados e uma reflexão sobre a aplicabilidade do framework no contexto de desenvolvimento de sistemas IoT.

Todas as informações coletadas serão tratadas de forma sigilosa, garantindo que os dados individuais dos participantes não sejam divulgados. Caso seja necessário realizar gravações de áudio ou vídeo para fins de análise acadêmica, os participantes serão previamente informados e poderão optar por não participar desse registro. O armazenamento dos dados seguirá as diretrizes da **Lei Geral de Proteção de Dados (LGPD - Lei 13.709/18)**, assegurando que os registros coletados serão utilizados exclusivamente para fins acadêmicos e científicos. A participação na pesquisa é voluntária, e os alunos poderão se retirar do estudo a qualquer momento, sem necessidade de justificativa e sem prejuízo acadêmico.

Esta pesquisa **não apresenta riscos significativos** aos participantes. No entanto, algumas atividades podem gerar pequenos desconfortos, como o tempo dedicado ao preenchimento de questionários ou a necessidade de refletir sobre experiências prévias na especificação de requisitos. Para minimizar possíveis desconfortos, garantimos que **nenhuma resposta será obrigatória**, e os participantes poderão **interromper sua participação a qualquer momento** sem qualquer penalização. Além disso, não há qualquer custo financeiro envolvido na participação no estudo.

Os participantes poderão se beneficiar da pesquisa de forma indireta, pois terão a oportunidade de **aprimorar seus conhecimentos** sobre engenharia de requisitos aplicada a sistemas IoT, além de aprenderem novas metodologias que poderão ser úteis em sua atuação profissional. Os participantes também terão acesso antecipado aos resultados do estudo, que poderão auxiliar na melhoria de práticas de desenvolvimento de software e na aplicação de técnicas inovadoras de engenharia de requisitos. O estudo visa, ainda, contribuir com a comunidade acadêmica e a indústria ao propor um método estruturado para avaliação de requisitos IoT, permitindo maior eficiência e confiabilidade no desenvolvimento de sistemas inteligentes.

---

Luis Fernando dos Santos Pires - Rua Henrique Schurig, 495 – Jd. Fernandes, São Paulo, SP – CEP: 03580-060, Fone: 11 94970-3282; Prof. Dr. Rodrigo Bonacin, - Rua Guatemala, 167 - Jardim América, Campo Limpo Paulista - SP, CEP: 13231-230, Fone(s): (11) 4812-9400 (Secretaria de Pós-graduação) ou 19 98136-2352.

Comitê de Ética em Pesquisa – Unisa - Rua Prof. Enéas de Siqueira Neto, 340 cep: 04829-300 São Paulo – SP, Fone: (11) 2141-8687 - [www.unisa.br](http://www.unisa.br)

Em caso de dano pessoal, diretamente relacionado aos procedimentos deste estudo (nexo causal comprovado), a qualquer tempo, fica **assegurado ao participante o respeito a seus direitos legais**, bem como procurar obter **indenizações** por danos eventuais.

**Uma via deste Termo de Consentimento ficará em seu poder.**

São Paulo, 18/02/2025

\_\_\_\_\_  
 (pesquisadores)

Se você concordar em participar desta pesquisa assine no espaço determinado abaixo e coloque seu nome e o nº de seu documento de identificação.

Nome: (do participante): .....  
 Doc. Identificação: .....  
 Ass: .....

Declaro (amos) que obtive (mos) de forma apropriada e voluntária o Consentimento Livre e Esclarecido deste participante (ou do representante legal deste participante) para a participação neste estudo, conforme preconiza a Resolução CNS 466, de 12 de dezembro de 2012, IV.3 a 6.

\_\_\_\_\_  
 Assinatura do pesquisador responsável pelo estudo  
 Data: 18/02/2025

Luis Fernando dos Santos Pires - Rua Henrique Schurig, 495 – Jd. Fernandes, São Paulo, SP – CEP: 03580-060, Fone: 11 94970-3282; Prof. Dr. Rodrigo Bonacini, - Rua Guatemala, 167 - Jardim América, Campo Limpo Paulista - SP, CEP: 13231-230, Fone(s): (11) 4812-9400 (Secretaria de Pós-graduação) ou 19 98136-2352.

Comitê de Ética em Pesquisa – Unisa - Rua Prof. Enéas de Siqueira Neto, 340 cep: 04829-300 São Paulo – SP,  
 Fone: (11) 2141-8687 - www.unisa.br

## Aprovação:

### – DADOS DA VERSÃO DO PROJETO DE PESQUISA

**Título da Pesquisa:** Um Framework para Mensuração da Maturidade de Requisitos de Sistemas em IoT

**Pesquisador Responsável:** Luis Fernando dos Santos Pires

Área Temática:

Versão: 2

CAAE: 85919124.1.0000.0081

Submetido em: 19/02/2025

Instituição Proponente: Faculdade Campo Limpo Paulista/Instituto de Ensino Campo Limpo Paulista - FACCAM

Situação da Versão do Projeto: **Aprovado**

Localização atual da Versão do Projeto: Pesquisador Responsável

Patrocinador Principal: Financiamento Próprio



Comprovante de Recepção: PB\_COMPROVANTE\_RECEPCAO\_2446370

## APÊNDICE V

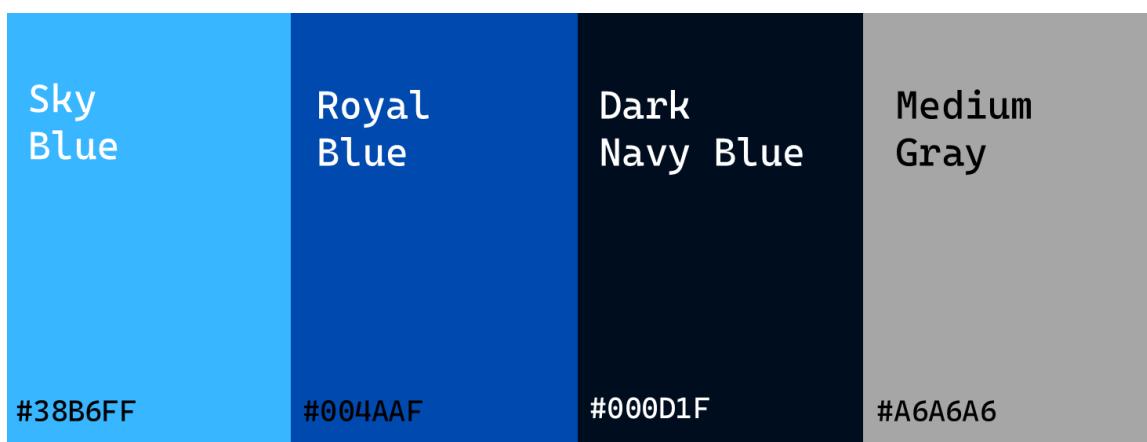
### Representação da Identidade Visual

A identidade visual do *QualIoT* foi projetada para comunicar os pilares fundamentais do *framework*: inovação, confiabilidade e conectividade. O elemento gráfico que simboliza a transmissão de dados, representado por ondas de conectividade acima do termo "IoT", reforça a proposta de interoperabilidade, um componente importante no desenvolvimento de sistemas IoT, conforme a seguir, o logotipo proposto a nosso software (Figura 36):



**Figura 36:** Logotipo *QualIoT* (Fonte: Autoria Própria)

A paleta de cores predominante, composta por tons de azul, foi escolhida para evocar confiança, precisão e segurança, aspectos importantes na implementação e validação de requisitos em sistemas IoT. O design minimalista e objetivo reflete a visão técnica e funcional do *framework*, ao mesmo tempo em que proporciona uma identidade visual atual e facilmente reconhecível no contexto acadêmico e profissional, a seguir a paleta de cores de nosso software (Figura 37):



**Figura 37:** Paleta de Cores (Fonte: Autoria Própria)

## APÊNDICE VI

### Nome e Identidade do *framework* QualIoT

O nome *QualIoT* foi concebido como uma fusão das palavras "Qualidade" e "Internet of Things" (IoT), refletindo diretamente o propósito central do *framework*: prover uma metodologia sistemática e mensurável para avaliar a maturidade de requisitos em sistemas IoT. Essa nomenclatura foi estrategicamente escolhida para destacar a proposta de valor do *framework*, que alia a excelência técnica à aplicabilidade prática no contexto da Internet das Coisas.

A escolha do termo "*QualIoT*" foi fundamentada em sua capacidade de traduzir, de forma objetiva e técnica, a conexão entre requisitos de qualidade e os complexos desafios que caracterizam o desenvolvimento de soluções IoT. Além disso, sua estrutura linguística simplificada promove uma fácil assimilação em ambientes técnicos e acadêmicos, alinhando-se à necessidade de comunicação clara e eficiente entre stakeholders.

Visando obter uma solução única e aderente, foi feita uma pesquisa no site do governo brasileiro na sessão do INPI, e confirmado que o nome de nosso *framework* se encontra disponível para a utilização, conforme registro a seguir (Figura 38):

The screenshot shows the official website of the Instituto Nacional da Propriedade Industrial (INPI) under the Ministry of Economy. The top navigation bar includes links for 'BRASIL', 'Acesso à informação', 'Participe', 'Serviços', 'Legislação', and 'Canais'. The main header features the INPI logo and the text 'Instituto Nacional da Propriedade Industrial - Ministério da Economia'. Below the header, there's a search bar with the placeholder 'Consulta à Base de Dados do INPI'. Underneath the search bar, there are links for '» Consultar por: Pesquisa Básica | Marca | Titular | Cód. Figura ]' and '[ Início | Ajuda? ].' The main content area displays the results of a search for the trademark 'QualIoT'. The heading 'RESULTADO DA PESQUISA (27/11/2024 às 08:55:54)' is followed by the text 'Marca: QualIoT' and a note: '- Nenhum resultado foi encontrado para a sua pesquisa. Para efetuar outra pesquisa, pressione o botão de VOLTAR.' Below this, there is an 'AVISO' message: 'Depois de fazer uma busca no banco de dados do INPI, ainda que os resultados possam parecer satisfatórios, não se deve concluir que a marca poderá ser registrada. O INPI no momento do exame do pedido de registro realizará nova busca que será submetida ao exame técnico que decidirá a respeito da registrabilidade do sinal.' At the bottom of the results page, it says 'Dados atualizados até 26/11/2024 - Nº da Revista:'.

**Figura 38:** Consulta INPI (**Fonte:** Governo Federal)

## ANEXO I

Certificado de Premiação de melhor artigo no XX Workshop de Computação



### **CERTIFICADO**

**C**ertificamos que o artigo “**Análise sobre Engenharia de Requisitos e Qualidade de Software para Sistemas IoT: Uma Revisão Sistemática da Literatura**” de autoria de Luis Fernando dos Santos Pires foi o melhor artigo do XX Workshop de Computação organizado pelo Centro Universitário Campo Limpo Paulista – UNIFACCAMP.

Campo Limpo Paulista/SP, 30 de outubro de 2024.



---

**Ana Maria Monteiro**  
Comitê de Organização

Razão Social: Instituto de Ensino Campo Limpo Paulista Ltda. CNPJ 02.252.746/0001-18  
Rua Guatemala, 167, Jd. América - Campo Limpo Pta/ SP | CEP: 13231-230  
[www.unifaccamp.edu.br](http://www.unifaccamp.edu.br) | (11) 4812-9400

## ANEXO II

Certificado da Publicação em Revista



## ANEXO III

### Folha de Rosto para Pesquisa Envolvendo Seres Humanos

 MINISTÉRIO DA SAÚDE - Conselho Nacional de Saúde - Comissão Nacional de Ética em Pesquisa – CONEP <b>FOLHA DE ROSTO PARA PESQUISA ENVOLVENDO SERES HUMANOS</b>		
1. Projeto de Pesquisa: Avaliação da Maturidade de Requisitos em Sistemas IoT		
2. Número de Participantes da Pesquisa: 26		
3. Área Temática:		
4. Área do Conhecimento: Grande Área 1. Ciências Exatas e da Terra		
<b>PESQUISADOR</b>		
5. Nome: Luis Fernando dos Santos Pires		
6. CPF: 361.850.968-54	7. Endereço (Rua, n.º): Rua Henrique Schuring JARDIM FERNANDES 495 SAO PAULO SAO PAULO 03580060	
8. Nacionalidade: BRASILEIRO	9. Telefone: 11949703282	10. Outro Telefone: 11. Email: luis.spires@outlook.com
Termo de Compromisso: Declaro que conheço e cumprirei os requisitos da Resolução CNS 466/12 e suas complementares. Comprometo-me a utilizar os materiais e dados coletados exclusivamente para os fins previstos no protocolo e a publicar os resultados sejam eles favoráveis ou não. Aceito as responsabilidades pela condução científica do projeto acima. Tenho ciência que essa folha será anexada ao projeto devidamente assinada por todos os responsáveis e fará parte integrante da documentação do mesmo.		
Data: 23 / 10 / 2024		 Assinatura
<b>INSTITUIÇÃO PROPONENTE</b>		
12. Nome: Faculdade Campo Limpo Paulista/Instituto de Ensino Campo Limpo Paulista - FACCAM	13. CNPJ: 02.252.746/0001-18	14. Unidade/Órgão:
15. Telefone: (11) 4812-9400	16. Outro Telefone:	
Termo de Compromisso (do responsável pela instituição): Declaro que conheço e cumprirei os requisitos da Resolução CNS 466/12 e suas Complementares e como esta instituição tem condições para o desenvolvimento deste projeto, autorizo sua execução.		
Responsável: Rodrigo Bonacin	CPF: 938.249.209/72	
Cargo/Função: Coordenador	 Assinatura	
Data: 23 / 10 / 2024		
<b>PATROCINADOR PRINCIPAL</b>		
Não se aplica.		

## ANEXO IV

### Certificado de Registro de Software - INPI

		<p style="text-align: center;"> <b>REPÚBLICA FEDERATIVA DO BRASIL</b> MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL DIRETORIA DE PATENTES, PROGRAMAS DE COMPUTADOR E TOPOGRAFIAS DE CIRCUITOS</p> <p style="text-align: center;"><b>Certificado de Registro de Programa de Computador</b></p> <p style="text-align: center;">Processo Nº: <b>BR512025001309-4</b></p> <p>O Instituto Nacional da Propriedade Industrial expede o presente certificado de registro de programa de computador, válido por 50 anos a partir de 1º de janeiro subsequente à data de 24/03/2024, em conformidade com o §2º, art. 2º da Lei 9.609, de 19 de Fevereiro de 1998.</p> <p><b>Título:</b> Qualiot</p> <p><b>Data de publicação:</b> 24/03/2024</p> <p><b>Data de criação:</b> 24/03/2024</p> <p><b>Titular(es):</b> LUIS FERNANDO DOS SANTOS PIRES</p> <p><b>Autor(es):</b> RODRIGO BONACIN; LUIS FERNANDO DOS SANTOS PIRES; VITOR DE SOUZA BARRETO; GUSTAVO HELY FERREIRA DA SILVA; RYAN LOURENÇO TEIXEIRA DA SILVA; CAUÃ NUNES PIRES</p> <p><b>Linguagem:</b> JAVA SCRIPT</p> <p><b>Campo de aplicação:</b> AD-06</p> <p><b>Tipo de programa:</b> AP-01; AV-01</p> <p><b>Algoritmo hash:</b> SHA-224</p> <p><b>Resumo digital hash:</b> 83cfa036570a78487d0efa36763b1342a9c7aab4dfd26642bbfb0501</p> <p><b>Expedido em:</b> 08/04/2025</p> <p style="text-align: center;"><b>Aprovado por:</b> Joelson Gomes Pequeno Chefe Substituto da DIPTO - PORTARIA/INPI/DIRPA Nº 02, DE 10 DE FEVEREIRO DE 2021</p>
--	--	--