



**UNIVERSIDADE FEDERAL DO TOCANTINS  
CAMPUS UNIVERSITÁRIO DE PALMAS-TO  
PROGRAMA DE PÓS-GRADUAÇÃO EM  
MODELAGEM COMPUTACIONAL DE SISTEMAS  
MESTRADO PROFISSIONAL**

**LUCYANO CAMPOS MARTINS**

**SISTEMA DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO UTILIZANDO  
INTERNET DAS COISAS**

**Palmas/TO**

**2021**

LUCYANO CAMPOS MARTINS

SISTEMA DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO UTILIZANDO  
INTERNET DAS COISAS

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Modelagem Computacional de Sistemas da Universidade Federal do Tocantins como requisito parcial para obtenção do título de Mestre em Modelagem Computacional de Sistemas.

Orientador: Dr. George Lauro Ribeiro de Brito

Palmas/TO

2021

**Dados Internacionais de Catalogação na Publicação (CIP)**  
**Sistema de Bibliotecas da Universidade Federal do Tocantins**

---

M386s MARTINS, LUCYANO CAMPOS.  
SISTEMA DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO  
UTILIZANDO INTERNET DAS COISAS. / LUCYANO CAMPOS MARTINS.  
– Palmas, TO, 2021.

67 f.

Dissertação (Mestrado Acadêmico) - Universidade Federal do Tocantins  
– Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) em  
Modelagem Computacional de Sistemas, 2021.

Orientador: George Lauro Ribeiro de Brito

1. Internet das Coisas. 2. Segurança Residencial. 3. Polícia Comunitária. 4.  
Círculo Impresso. I. Título

**CDD 004**

---

TODOS OS DIREITOS RESERVADOS – A reprodução total ou parcial, de qualquer  
forma ou por qualquer meio deste documento é autorizado desde que citada a fonte.  
A violação dos direitos do autor (Lei nº 9.610/98) é crime estabelecido pelo artigo 184  
do Código Penal.

**Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os  
dados fornecidos pelo(a) autor(a).**

LUCYANO CAMPOS MARTINS

SISTEMA DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO UTILIZANDO  
INTERNET DAS COISAS

Dissertação apresentada ao Programa de Pós-Graduação Profissional em Modelagem Computacional de Sistemas da Universidade Federal do Tocantins. Foi avaliada para obtenção do título de Mestre em Modelagem Computacional de Sistemas e aprovada em sua forma final pelo Orientador e pela Banca examinadora.

Data de aprovação \_\_\_ / \_\_\_ / \_\_\_\_

Banca examinadora

---

Prof. Dr. George Lauro Ribeiro de Brito, Orientador – PPGMCS-UFT

---

Prof. Dr. Humberto Xavier Araújo, Avaliador interno – PPGMCS-UFT

---

Prof. Dr. Patrick Letouzé Moreira, Avaliador interno – PPGMCS-UFT

---

Prof. Dr. Wendell Eduardo Moura Costa, Avaliador externo – IFTO

*Dedico este trabalho à minha filha Sofia César e minha esposa Laís César, razões da minha vida, motivo pelo qual busco todos os dias ser uma pessoa melhor.*

*Eu acredito que às vezes são as pessoas que  
ninguém espera nada que fazem as coisas que  
ninguém consegue imaginar.  
(Alan Turing)*

## AGRADECIMENTOS

Há tantos agradecimentos a fazer. Gostaria de iniciar lembrando do apoio incondicional que recebi da minha família, minha esposa Laís César e minha filha Sofia César, quando decidimos mudar para Palmas em 2018. O objetivo da mudança era a realização do meu sonho em cursar o mestrado. Nesse período pairou sobre minha cabeça muitas dúvidas, mas fui incentivado com palavras de motivação.

Minha gratidão eterna ao meu orientador Dr. George Brito, que no vigésimo segundo dia, do mês de março, às dezessete horas e dezoito minutos, respondeu ao e-mail de um desconhecido que buscava oportunidade para apresentar-se, no intuito de concorrer a uma vaga para a seleção de mestrado.

Agradeço também a todos os professores do Programa de Pós-Graduação em Modelagem Computacional de Sistemas (PPGMCS) da Universidade Federal do Tocantins, em especial ao Dr. Humberto Xavier Araújo, que conduziu a disciplina de Internet das Coisas, mostrando-me um mundo novo em relação ao desenvolvimento de *software* e sistemas embarcados.

Por fim, quero agradecer *in memoriam* minha avó materna, Maria das Mercê Campos da Silva, que, mesmo não sendo formalmente alfabetizada, foi a pessoa a qual me ensinou as primeiras letras e palavras, dando início a uma caminhada de estudos que já dura mais de 25 anos.

## RESUMO

Este trabalho apresenta o desenvolvimento de uma central de segurança residencial de baixo custo, utilizando conceitos e componentes de Internet das Coisas. O dispositivo desenvolvido poderá ser utilizado para auxiliar a comunidade na segurança pública. Através da revisão de literatura, para evidenciar quais soluções foram propostas usando IoT na segurança residencial, buscou-se desenvolver um circuito impresso com os componentes necessários para auxiliar a segurança nas residências, em diversos fatores. O desenvolvimento do software embutido no dispositivo buscou seguir práticas evolutivas que permitissem adaptabilidade a diversas situações encontradas em diferentes ambientes a serem monitorados. A solução final contempla um dispositivo eletrônico com componentes de baixo custo, e um software que permite obter os dados dos sensores e alertar o morador caso ocorra alguma anormalidade. A proposta final é a instalação de uma central de segurança referenciada em residências da comunidade, para monitorar a segurança e os parâmetros dos ambientes, proporcionando maior segurança aos moradores durante o período que estiverem ausentes de seus domicílios.

**Palavras-chaves:** Segurança Residencial. Internet das Coisas. Monitoramento de Residências.

## **ABSTRACT**

This work presents the development of a low-cost residential security center, using Internet of Things concepts and components. The device developed can be used to assist the community in public safety. Through the literature review, to show which solutions were proposed using IoT in residential security, it was sought to develop a printed circuit with the necessary components to help security in homes, in several factors. The development of the software embedded in the device sought to follow evolutionary practices that allowed adaptability to different situations found in different environments to be monitored. The final solution includes an electronic device with low-cost components, and a software that allows obtaining data from the sensors and alerting the resident if any abnormality occurs. The final proposal is the installation of a security center referenced in community homes, to monitor the safety and parameters of the environments, providing greater security to residents during the period they are away from their homes.

**Keywords:** Home Security. Internet of Things. Home Monitoring.

## LISTA DE ILUSTRAÇÕES

<b>Figura 1</b> - Etapas da revisão da literatura .....	27
<b>Figura 2</b> - Microcontrolador ESP8266 .....	31
<b>Figura 3</b> - Sensor de umidade e temperatura DHT11 .....	32
<b>Figura 4</b> - Sensor de gás MQ-2.....	33
<b>Figura 5</b> - Sensor de chama 760 a 1100 nm .....	33
<b>Figura 6</b> - Transmissor RF XLC-RF-5V .....	34
<b>Figura 7</b> - Sensor magnético sem fio IPEC .....	34
<b>Figura 8</b> - Módulo GMS SIM800L EVB .....	35
<b>Figura 9</b> - Fonte carregador 12V 3A .....	35
<b>Figura 10</b> - Bateria 12V 7A para alimentação do circuito.....	36
<b>Figura 11</b> - Regulador de tensão LM2596.....	36
<b>Figura 12</b> - Prototipagem dos componentes da solução .....	37
<b>Figura 13</b> - Protótipo de circuito montado com <i>protoboard</i> e <i>jumpers</i> .....	38
<b>Figura 14</b> - Camada superior do projeto do circuito eletrônico impresso .....	39
<b>Figura 15</b> - Segunda camada do projeto do circuito eletrônico impresso .....	39
<b>Figura 16</b> - Visão superior do circuito impresso .....	40
<b>Figura 17</b> - Visão inferior do circuito impresso .....	40
<b>Figura 18</b> - Esquemático do circuito .....	41
<b>Figura 19</b> - Fluxograma geral de funcionamento do <i>software</i> .....	42
<b>Figura 20</b> - Declaração das variáveis <i>toggles</i> .....	43
<b>Figura 21</b> - Função <i>loop</i> .....	44
<b>Figura 22</b> - Função <i>setup</i> inicialização do sistema.....	44
<b>Figura 23</b> - Fluxograma de inicialização do sistema.....	45
<b>Figura 24</b> - Código função da leitura do sensor de rádio frequência.....	45
<b>Figura 25</b> - Fluxograma do funcionamento do receptor de rádio frequência.....	46
<b>Figura 26</b> - Código função da leitura de temperatura e umidade .....	46
<b>Figura 27</b> - Fluxograma de funcionamento do sensor de temperatura e umidade.....	47
<b>Figura 28</b> - Função de leitura do sensor de gás MQ2.....	47
<b>Figura 29</b> - Fluxograma de funcionamento do sensor de gás MQ2 .....	48
<b>Figura 30</b> - Função de leitura do sensor de fogo .....	48
<b>Figura 31</b> - Fluxograma de funcionamento do sensor de fogo.....	49

<b>Figura 32</b> - Página inicial do <i>ThingSpeak</i> .....	49
<b>Figura 33</b> - Configurações do canal do <i>ThingSpeak</i> .....	50
<b>Figura 34</b> - Função de envio dos dados para plataforma <i>ThingSpeak</i> .....	50
<b>Figura 35</b> - Configuração das chaves do canal do <i>ThingSpeak</i> .....	51
<b>Figura 36</b> - SMS de alerta recebido pelo celular cadastrado .....	52
<b>Figura 37</b> - Gráfico de monitoramento da temperatura plataforma <i>ThingSpeak</i> .....	53
<b>Figura 38</b> - Visualizador do valor da temperatura plataforma <i>ThingSpeak</i> .....	53
<b>Figura 39</b> - Gráfico de monitoramento da umidade na plataforma <i>ThingSpeak</i> .....	53
<b>Figura 40</b> - Visualizador do valor da umidade plataforma <i>ThingSpeak</i> .....	53
<b>Figura 41</b> - Solução montada.....	54
<b>Gráfico 1</b> - Artigos selecionados por ano de publicação .....	28
<b>Quadro 1</b> - Valor médio de equipamento similar encontrado no mercado .....	24
<b>Quadro 2</b> - Termos combinados para pesquisa nas bases de dados .....	26
<b>Quadro 3</b> - Base de dados utilizadas na pesquisa .....	26
<b>Quadro 4</b> - Especificações do microcontrolador ESP8266 .....	32
<b>Quadro 5</b> - Componentes utilizados na prototipagem .....	38
<b>Quadro 6</b> - Bibliotecas utilizadas na programação .....	43
<b>Quadro 7</b> - Especificações da solução .....	54
<b>Quadro 8</b> - Aplicação da solução .....	55

## **LISTA DE TABELAS**

<b>Tabela 1</b> - Relação entre pessoas e dispositivos conectados ao longo dos anos.....	21
<b>Tabela 2</b> - Resultado das buscas avançadas nas bases de dados.....	28
<b>Tabela 3</b> - Microcontroladores apresentados nos trabalhos da revisão .....	30
<b>Tabela 4</b> - Comparação de funcionalidades e valores entre soluções de segurança.....	55

## LISTA DE ABREVIATURAS E SIGLAS

CCTV	Televisão em Circuito Fechado
IoT	<i>Internet Of Things</i> – Internet das Coisas
LCD	Liquid Crystal Display – Display de Cristal Líquido
LED	Light-Emitting Diode – Diodo Emissor De Luz
PM-TO	Polícia Militar do Tocantins
POP	Procedimento Operacional Padrão
PPGMCS	Programa de Pós-Graduação em Modelagem Computacional de Sistemas
RAM	Random Access Memory – Memória de Acesso Aleatório
RCS	Redes de Segurança Comunitária
RFID	Identificação por Radiofrequência
UFT	Universidade Federal do Tocantins

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>15</b>
<b>1.1 Delimitação do escopo .....</b>	<b>16</b>
<b>1.2 Justificativa .....</b>	<b>16</b>
<b>1.3 Objetivo geral.....</b>	<b>17</b>
<b>1.4 Objetivos específicos.....</b>	<b>18</b>
<b>1.5 Metodologia.....</b>	<b>18</b>
<b>1.6 Organização da dissertação .....</b>	<b>18</b>
<b>2 REFERENCIAL TEÓRICO .....</b>	<b>20</b>
<b>2.1 Características da pesquisa.....</b>	<b>20</b>
<b>2.2 Internet das Coisas .....</b>	<b>21</b>
<b>2.3 Segurança comunitária .....</b>	<b>21</b>
<b>2.4 Segurança residencial.....</b>	<b>22</b>
<b>2.5 Dispositivos de segurança residencial .....</b>	<b>23</b>
<b>2.6 Pesquisa bibliográfica.....</b>	<b>24</b>
<b>3 ESPECIFICAÇÃO DO SISTEMA PARA SEGURANÇA RESIDENCIAL.....</b>	<b>31</b>
<b>3.1 Componentes utilizados .....</b>	<b>31</b>
3.1.1 Microcontrolador ESP8266 .....	31
3.1.2 Sensor de umidade e temperatura DHT11.....	32
3.1.3 Sensor de gás e fumaça MQ-2.....	33
3.1.4 Sensor de chama fogo 760 a 1100 nm.....	33
3.1.5 Transmissor RF XLC-RF-5V .....	34
3.1.6 Sensor magnético sem fio IPEC .....	34
3.1.7 Módulo GMS SIM800L EVB .....	35
3.1.8 Sistema de alimentação .....	35
<b>4 MODELAGEM DO SISTEMA.....</b>	<b>37</b>
<b>4.1 Prototipação e montagem dos componentes .....</b>	<b>37</b>
<b>4.2 Desenvolvimento do circuito elétrico .....</b>	<b>39</b>
<b>4.3 Programação do microcontrolador.....</b>	<b>41</b>
4.3.1 Bibliotecas utilizadas.....	43
4.3.2 Feature Toggles .....	43
4.3.3 Inicialização do sistema.....	44

4.3.4 Funcionamento do receptor rádio frequência 433 mhz e sensor de abertura magnético sem fios .....	45
4.3.5 Funcionamento do sensor de temperatura e umidade.....	46
4.3.6 Funcionamento do sensor de gás .....	47
4.3.7 Funcionamento do sensor de fogo .....	48
4.3.8 Integração <i>ThingSpeak</i> .....	49
<b>5 RESULTADOS E ANÁLISE.....</b>	<b>52</b>
<b>5.1 Dados e interfaces da solução .....</b>	<b>52</b>
<b>5.2 Central de segurança residencial .....</b>	<b>54</b>
<b>5.3 Custo da solução .....</b>	<b>55</b>
<b>6 CONCLUSÃO.....</b>	<b>56</b>
<b>6.1 Trabalhos futuros .....</b>	<b>57</b>
<b>7 CONTRIBUIÇÕES E TRABALHOS PUBLICADOS .....</b>	<b>58</b>
<b>REFERÊNCIAS .....</b>	<b>60</b>
<b>APÊNDICE A - ESTUDOS INCLUÍDOS NA REVISÃO DA LITERATURA .....</b>	<b>62</b>
<b>APÊNDICE B - CUSTO DA SOLUÇÃO EM NOVEMBRO 2021 .....</b>	<b>65</b>

## 1 INTRODUÇÃO

O surgimento de dispositivos eletrônicos conectados à internet permitiu a criação de soluções para problemas do cotidiano, como abertura/destravamento de portas, controle de autorização de acesso, gerenciamento de entrada, dentre outros. Tais soluções são respaldadas em componentes eletrônicos de baixo custo, cada vez mais acessíveis, em razão da facilidade dos mecanismos de compras virtuais.

A segurança de residências é um aspecto que preocupa cada vez mais o cidadão, pois o número de furtos cresce dia após dia, como é possível perceber no noticiário. O auxílio à segurança doméstica vai além do monitoramento de acesso não autorizado. Outra questão importante para os moradores é saber quando cada evento desses ocorre. Diante desses requisitos, a maior parte das soluções presentes no mercado não apresenta a possibilidade de monitoramento e alerta para todas essas situações.

Na mesma proporção, o surgimento de dispositivos para Casas Inteligentes, em inglês, *Smart Home*, vem aumentando na última década, juntamente do crescimento e da adoção do conceito de Internet das Coisas, *Internet of Things* (IoT). Segundo Santos et al. (2016), Internet das Coisas significa a capacidade, embutida em eletrônicos, de coletar, armazenar, processar e transmitir informações por meio da internet, utilizando sensores e dispositivos interconectados.

Já é possível encontrar soluções comerciais completas para Casas Inteligentes, que monitora diversos tipos de eletrônicos, mesmo aqueles que não estão conectados. Isto se deve ao desenvolvimento de sensores diversificados com capacidade de leitura de parâmetros necessários para manter um ambiente residencial seguro. Essas soluções, presentes no mercado, custam centenas ou mesmo milhares de reais, pois acumulam valor de marca e margem de lucro para grandes empresas e prestadores de serviço.

Os dispositivos conectados à internet podem gerar alternativas para resoluções de circunstâncias do dia a dia, além de influenciar a diminuição de custos para soluções já existentes. A exemplo de soluções de baixo custo, temos os microcontroladores ligados a sensores dos mais diversos tipos.

Nessa perspectiva, diante do crescente aumento de tecnologias baseadas em Internet das Coisas e da expansão das conexões móveis, as soluções que utilizam internet podem ser atrativas para resolução de problemas da indústria e até mesmo demandas residenciais. Sendo assim, a proposta deste trabalho é desenvolver uma central de segurança residencial de baixo custo, que possa alertar o proprietário e/ou morador, por meio de sensores, sobre a ocorrência de alguma anormalidade em suas residências no que diz respeito a abertura indevida de portas

ou janelas, ou de parâmetros ambientais, como: gás de cozinha (butano C<sub>4</sub>H<sub>10</sub>) em excesso no ar, detecção de incêndio, variação abrupta de umidade e temperatura ambiente.

Detectada a ocorrência, o sistema terá capacidade de armazenar os parâmetros e enviá-los para o celular do responsável pela residência, por meio de mensagem SMS em caso de gatilhos configurados, seja por variação do limite mínimo ou máximo de cada valor, ou por agenda configurada para sincronia temporal.

### **1.1 Delimitação do escopo**

Esta dissertação apresenta o desenvolvimento de um dispositivo para segurança residencial capaz de monitorar a abertura de portas e janelas por meio de sensores sem fio. Inclui-se no sistema de monitoramento, os parâmetros: ambientes de temperatura e umidade, a presença de gás inflamável no ar, e a ocorrência de fogo.

### **1.2 Justificativa**

A justificativa para o desenvolvimento desse projeto está alinhada às propostas das redes de Polícia Comunitária de Palmas – TO, que visam aproximar a atuação do policiamento às necessidades da sociedade. As discussões sobre os furtos às residências e quais ações a comunidade juntamente da polícia poderiam tomar para combater esse problema, foram fatores que desencadearam ideias de ferramentas que pudessem auxiliar na segurança das residências e no trabalho dos policiais.

As políticas de segurança estabelecidas pela Polícia Militar do Tocantins (TOCANTINS, 2017) regulamentam as atividades da mesma, juntamente das Redes de Segurança Comunitária (RCS), no âmbito do Comando de Policiamento da Capital. O objetivo da RSC é contribuir com os comandos das unidades para, em redes integradas, demonstrar alternativas viáveis de capacitação da instituição para assistência ao cidadão. Essas alternativas ajudam na tomada de decisões para aproximação da polícia à comunidade, a fim de garantir o trabalho já realizado, de forma técnica, uniforme e padronizada.

O processo histórico das redes comunitárias, de acordo com as diretrizes de número 001-2017, de novembro de 2017, da Polícia Militar do Tocantins, teve origem em 2014 quando os blocos da capital do estado do Tocantins decidiram se reunir, em parceria com o Ministério Público, para que pudessem analisar, priorizar, decidir e atuar em situações de crimes.

No ano de 2013 foi implementado o Procedimento Operacional Padrão (POP), no qual qualifica a polícia para as ações da Polícia Comunitária, implementando visitas de solidariedade ao cidadão, monitoramento e reuniões mensais da comunidade. Com base no uso dessa ferramenta, a rede passou a incluir mais serviços militares, administrativos e operacionais em visitas proativas. Nos anos de 2015 e 2016, foram realizadas Reuniões Participativas de Segurança Comunitária com a presença dos presidentes e líderes comunitários, membros do RCS dos residentes.

Em 2014 a Polícia Militar (PM) utilizou a tecnologia para envolver a comunidade na busca de soluções perante crimes contra o patrimônio. O objetivo das redes de segurança comunitária é incentivar a comunidade a formar as redes de serviços comunitárias em parceria com a PM – TO. Logo, a polícia oferece à comunidade cursos, capacitações, reuniões, palestras e eventos direcionados à segurança pública. Cabe à polícia, também, divulgar ações preventivas e responder aos índices criminais, reduzindo, assim, taxas de furtos nas áreas atendidas pela PM do Tocantins (2017).

Apesar dos esforços, por parte dos grupos e das redes de segurança comunitária, ainda persistia o problema de não ter o alerta em tempo real de arrombamentos das residências. A comunidade conseguia acionar os agentes de segurança, em caso de invasão de sua residência, mas apenas algum tempo após o crime ter sido realizado. Isso se deve ao fato de que a maior parte da população trabalha fora, o que deixa o domicílio sem a presença de ocupantes durante esse período. Além disso, o alto custo das soluções de mercado para segurança e alerta de invasão de residência viabilizou a elaboração desse projeto, uma vez que também é papel da universidade propor soluções para os problemas da sociedade.

Os furtos à residência têm sido problema constante no país inteiro. Pode-se inferir que, diante dessa realidade, a tecnologia de Internet das Coisas pode ajudar a sociedade, juntamente do setor de segurança público e privado, dentre eles a Polícia Militar, na luta contra a violência, oferecendo oportunidades para o desenvolvimento de serviços de qualidade.

### **1.3 Objetivo geral**

Desenvolver a modelagem de um circuito utilizando componentes de Internet das Coisas para a criação de uma central de segurança residencial de baixo custo, aplicada à prevenção de furtos residenciais e que monitore parâmetros sensíveis à segurança do ambiente.

## 1.4 Objetivos específicos

1. Identificar na literatura soluções baseadas em Internet das Coisas para segurança residencial;
2. Estabelecer comparativos entre as principais soluções: microcontroladores e sensores para segurança residencial;
3. Desenvolver e registrar o *software* e o circuito impresso para a solução central de segurança residencial integrado aos componentes selecionados.

## 1.5 Metodologia

Como metodologia para o desenvolvimento desta pesquisa, buscou-se apoio na pesquisa explicativa, cujo método pretende justificar os fatores que levaram à realização do fenômeno estudado. Neste caso, a pesquisa trata do desenvolvimento de uma central de segurança de baixo custo baseada em Internet das Coisas.

Após definição da metodologia, realizou-se uma revisão da literatura com objetivo de encontrar soluções semelhantes já propostas, com o intuito de aprender com estas e conduzir uma especificação assertiva da proposta a ser criada.

Abordou-se ainda sobre os materiais e métodos usados na condução da pesquisa utilizada no desenvolvimento do protótipo. Foram apresentadas as especificações de todos os componentes de *hardware* usados, e a programação do microcontrolador. Depois de definido o protótipo, demonstrou-se os testes preliminares.

## 1.6 Organização da dissertação

Este trabalho está organizado em **seis capítulos** demonstrados, a seguir, juntamente de sua descrição.

**Capítulo I** – A introdução contém o início da contextualização a respeito do tema. Em seguida, são apresentados os seguintes tópicos: a delimitação, a justificativa, os objetivos gerais e os objetivos específicos. A metodologia é apresentada em um subcapítulo, no qual constam as características da pesquisa, o referencial teórico e uma breve contextualização sobre: Internet das Coisas, segurança comunitária, segurança residencial e dispositivos de segurança residencial.

**Capítulo II** – No referencial utilizou-se artigos, livros e publicações escolhidas para construir a base da proposta do trabalho.

**Capítulo III** – É apresentado o referencial teórico junto da revisão da literatura, evidenciando os trabalhos selecionados com base no protocolo de revisão.

**Capítulo IV** – Contém a modelagem do sistema, com esquema de ligação dos componentes e os detalhes sobre desenvolvimento e lógica do *software* e circuito impresso.

**Capítulo V** – Demonstrou-se os resultados e as análises dos dados da solução desenvolvida.

**Capítulo VI** – Neste capítulo são descritas a conclusão, as contribuições e as perspectivas do trabalho.

## 2 REFERENCIAL TEÓRICO

Os estudos sobre Internet das Coisas, ou Computação Ubíqua, já vem sendo discutidos há pelo menos duas décadas. Segundo Galegale et al. (2016), apud ASHTON, 2009, o termo Internet das Coisas, ou *Internet of Things* (IoT), em inglês, foi apresentado primeiramente por Kevin Ashton da MIT Auto Centre<sup>1</sup>, em uma apresentação sobre Identificação por Radiofrequência (RFID). Com isso é possível perceber que os estudos e discussões sobre dispositivos conectados já vem ocorrendo há muito tempo no meio científico.

Para Stevan (2018), outras tecnologias de comunicação foram impulsionadas mediante a invenção da telefonia, a exemplo: a telemetria, as máquinas monitoradas, as automações e os sistemas supervisionados; dando vazão a criação de cada vez mais dispositivos com capacidade de coletar e armazenar informações por meio de sensores.

Já Oliveira (2017) descreve que classificar algo como Internet das Coisas não é somente comandar dispositivos por meio do *smarthphone*, mas embutir inteligência, ou mesmo capacidade de decidir com base em leituras de sensores que leiam parâmetros do ambiente que estão conectados.

### 2.1 Características da pesquisa

Desenvolveu-se uma pesquisa da literatura sobre o uso da Internet das Coisas em segurança residencial, com o objetivo de compreender quais aspectos envolvem a segurança de uma residência. A linha de pesquisa sobre Internet das Coisas já vem sendo amplamente discutida no cenário acadêmico, com variadas aplicações, em especial soluções que busquem o aumento de eficiência e diminuição de custo por meio de componentes simples e customizados.

Para Sampaio; Mancini (2007), na revisão da literatura são utilizadas fontes de dados sobre temas específicos permitindo à pesquisa encontrar evidências de forma mais direta, uma vez que o objetivo da busca é definido. Diante disso, foi elaborado um criterioso protocolo de revisão, com etapas bem descritas e claras, de forma a permitir sua reprodução e supervisão por pares. O objetivo da revisão é conhecer os trabalhos relevantes ao tema proposto e, por meio deles, escolher caminhos viáveis para o uso das técnicas e tecnologias empregadas em cada

---

<sup>1</sup> Grupo de pesquisa sobre radiofrequência e tecnologias de identificação de detecção, composto por sete universidades em vários países diferentes.

solução. Esses fatores, possibilitam adequação à realidade proposta para a solução final, considerando a complexidade da implementação e do custo.

## 2.2 Internet das Coisas

Com o avanço da tecnologia e com a expansão da conectividade de internet, foi possível perceber o surgimento, cada vez mais significativo, de dispositivos conectados. Esses dispositivos apresentam capacidade de conexão, e processam e armazenam informações, podendo, assim, serem úteis em tarefas do dia a dia.

Muito se discute sobre a definição e o conceito de Internet das Coisas. Para o autor Stevan (2018) é possível imaginar que qualquer “coisa” possa prover informações na internet e se comunicar com outras que nela estejam conectadas, considerando que qualquer dispositivo ligado à internet pode ser identificado por meio de endereços universais.

Conforme definido por Santos et al. (2016), a Internet das Coisas é uma extensão da internet atual, a qual proporciona aos objetos do cotidiano (quaisquer que sejam), capacidade computacional e de comunicação para se conectarem à internet. Para Evans (2011), a *IoT*, algumas vezes, também, referida como a Internet dos Objetos, mudará tudo, inclusive nós mesmos. Isso pode parecer uma declaração arrojada, mas se considera nessa afirmação o impacto que a Internet já teve na educação, na comunicação, nos negócios, na ciência, no governo e na humanidade.

**Tabela 1** - Relação entre pessoas e dispositivos conectados ao longo dos anos

	2003	2010	2015	2020 (previsão)
<b>População mundial</b>	6,3 bilhões	6,8 bilhões	7,2 bilhões	7,6 bilhões
<b>Dispositivos conectados</b>	0,5 bilhões	12 bilhões	25 bilhões	50 bilhões
<b>Dispositivos por pessoa</b>	0,8	1,84	3,47	6,58

Fonte: Stevan (2018). Adaptada de Evans (2011).

## 2.3 Segurança comunitária

Segundo a Constituição Federal (BRASIL, 1988), no seu Capítulo III, artigo 144, a segurança pública é um dever do Estado e um direito e responsabilidade de todos. O direito a segurança pública garante a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, por intermédio dos seguintes órgãos: polícia federal; polícia rodoviária federal; polícia ferroviária federal; polícias civis; polícias militares e corpos de bombeiros militares.

Diante disso, podemos visualizar o papel fundamental entre os agentes do estado e a sociedade civil, uma vez que a carta magna do Brasil estabelece a união entre direito e responsabilidade. Outro ponto importante a ser ressaltado diz respeito à preservação do patrimônio em geral, tendo em vista que não há distinção sobre os âmbitos público ou privado.

A respeito do surgimento das primeiras discussões sobre Polícia Comunitária, Bohn (2014) descreve que, no período de redemocratização do Brasil, com a Constituição de 1988, as instituições responsáveis pela segurança pública foram incumbidas de se reformarem para atender as novas demandas da sociedade no que se refere a cidadania.

Para Matrak Filho (2010), a construção de boas polícias é possível se existirem doutrinas e ferramentas com orientações precisas, clarividentes e elaboradas com empenho. Na concepção deste autor, é por meio dessas doutrinas e ferramentas que o agente encontra orientação de como agir, solucionar seus problemas e legitimar suas ações.

Novamente Bohn (2014) descreve que a adoção da implantação de polícia comunitária tem sido adotada por vários países, com objetivo de modificar as relações entre polícia e sociedade, buscando a aproximação e o bom relacionamento entre ambos.

Observa-se com base em todas as discussões sobre segurança e polícia comunitária que o objetivo intrínseco é unir e aproximar os agentes de segurança pública da sociedade, retirando rótulos e preconceitos a respeito do serviço prestado pela polícia à população. Outro aspecto interessante é a colocação de estratégias de policiamento preventivo, uma vez que a segurança pública é dever de todos.

## **2.4 Segurança residencial**

Pode-se utilizar diversas definições para destacar a importância da segurança residencial, tendo em vista que o próprio conceito de residência, casa e lar, remete, em diversas vezes, lugar de moradia ou lugar seguro, sejam eles permanentes ou temporários.

Para Batrinu (2018, p. 106), temos interesse em saber como está a nossa casa quando estamos ausentes. Essa preocupação está ligada à segurança, tendo em vista os elementos críticos presentes, como: gás, fogo ou água. Por isso é importante saber quando algo errado estiver ocorrendo para minimizar danos potenciais.

Segundo Surantha; Wicaksono (2018), residência é um local em que são armazenadas riquezas, portanto, a segurança se torna uma das considerações obrigatórias para impedir eventos indesejáveis ocasionados por acidentes. Considerando esses fatos e o avanço da tecnologia e dos paradigmas sobre segurança envolvendo residências, Nadafa et al. (2020)

ressaltam, ser evidente que as habilidades dos ladrões também aumentaram, portanto, é um grande desafio projetar um sistema infalível. Usualmente, as pessoas usam câmeras de segurança para proteger suas casas. As câmeras registram as atividades que ocorrem e armazenam no dispositivo de armazenamento.

Ainda se tratando das diversas peculiaridades que envolve a segurança residencial, observa-se que, segundo Aldawira et al. (2019), portas e janelas são os primeiros recursos de defesa para manter a segurança física da casa. Se elas podem ser abertas facilmente, algum ladrão poderá entrar e roubar o conteúdo da casa, sem maiores dificuldades.

Diante de todas as discussões, pode-se estabelecer especificações bases para a segurança dos ambientes residenciais, a manutenção controlada do acesso, o monitoramento de parâmetros considerados de risco: temperatura ambiente, fogo e gás, e o mais importante, ser alertado em tempo real, caso o *status* ou os parâmetros estejam fora do padrão. Desta forma, o morador conseguirá tomar decisões que evitem furtos e situações de risco, como: alagamentos, incêndio e/ou vazamento de gás.

## **2.5 Dispositivos de segurança residencial**

No panorama tradicional dos dispositivos para segurança residencial existentes no mercado, apontou-se diversos problemas. Para Patel et al. (2019) é importante entender que nem todos os casos referentes à segurança residencial exigem um sistema de vigilância volumoso, caro, sofisticado e pesado, o que pode gerar tráfego excessivo no consumo de internet. A maioria dos sistemas de segurança e vigilância existentes consiste em televisão em circuito fechado, em inglês, *Closed-Circuit Television* (CCTV). As câmeras, embora sofisticadas, exigem supervisão humana para obter recursos em tempo real, para não mencionar o alto consumo de energia.

Para Paul et al. (2016), sistemas de segurança residenciais possuem três grandes dificuldades: alto custo da propriedade, inflexibilidade e gerenciamento ruim. Observa-se com base nessa colocação a justificativa do alto preço desse tipo de solução, atrelado à margem de lucro das empresas que os produzem. Observa-se, ainda, que uma solução genérica para atender um grande público traz consigo uma série de outros problemas. Para exemplificar, tem-se a inflexibilidade, já mencionada, sendo um entrave para possibilidade de adaptação aos diversos cenários.

As soluções existentes no mercado, de propriedade das marcas consolidadas, oferecem soluções fechadas. Geralmente são oferecidos modelos ou pacotes com número limitado de

sensores, e ainda, tipo de alerta não conectado, por exemplo, alertas sonoros ou de ligação por linha fixa. Essas soluções limitam-se ao monitoramento de sensores de porta aberta e presença, propiciando a deficiência para realmente manter um ambiente residencial seguro.

Diante de toda deficiência apresentada, foi realizada uma pesquisa nos principais sites de vendas, a fim de fazer um levantamento de preço e funcionalidades dessas soluções, uma vez que, um dos objetivos desta pesquisa é a comparação entre as soluções de mercado com o protótipo desenvolvido como resultado do projeto.

Realizou-se pesquisa numa loja *on-line*, de venda de produtos para segurança residencial, com intuito de estabelecer parâmetros de preços desse tipo de solução. Para comparativo de valores foi desenvolvido, no **Quadro 1**, uma lista dos itens característicos: tipo de solução, tipos de sensores e monitoramento, mecanismo de alerta e valor.

**Quadro 1** - Valor médio de equipamento similar encontrado no mercado

Solução	Sensores	Tipo Alerta	Valor	Observações
Kit de Segurança Inteligente KaBuM! Smart 500	Sensor de abertura e presença sem fio.	Alerta sonoro e aplicativo	R\$ 279,00	Ações de alerta fixa, não é possível configurar alertas, interações somente por comando em teclado físico.
Sistema De Segurança Residencial Sem Fio Alarme C/ 6 Sensor	Sensor de abertura com e sem fio e sensor de presença com fio.	Alerta sonoro por sirene.	R\$ 604,99	Alerta somente sonoro, monitoramento apenas de sensores de abertura e presença.
Sistema Segurança Residencial Amt 2018e Iva 3070x Intelbras	Sensor de presença infravermelho com e sem fio.	Alerta por meio de plataforma própria do fabricante por aplicativo.	R\$ 2.215,48	Utiliza sirene para alerta sonoro, teclado para interação e programação.
Kit Alarme Central Intelbras Segurança Residencial Comercial	Sensor de presença infravermelho com fio e sensor de abertura sem fio.	Alerta sonoro por sirene.	R\$ 628,25	Alerta somente sonoro por sirene, não há nenhum tipo de conectividade.

Fonte: Consulta realizada em julho 2020.

## 2.6 Pesquisa bibliográfica

Com objetivo de buscar na literatura existente trabalhos que pudessem contribuir com o desenvolvimento da pesquisa, elaborou-se uma revisão da literatura nas bases de dados disponíveis *on-line*, utilizando criterioso protocolo de revisão e análise dos trabalhos. Foi evidenciado que as tecnologias de Internet das Coisas vêm sendo amplamente utilizadas para resolução de problemas do cotidiano da sociedade moderna, sendo esses problemas relativos a monitoramento e automatização com auxílio de sensores e atuadores.

Elaborou-se um protocolo de revisão conforme sugerido por Letouze et al. (2016), cuja etapa de estabelecimento de um protocolo para a revisão é o momento no qual definimos desde a viabilidade da realização da proposta ao refinamento das características dos próximos passos. Portanto, o protocolo deste trabalho tem as seguintes diretrizes:

- **Definição dos termos de busca:** associou-se termos relevantes do objetivo central da pesquisa com as palavras-chave Internet das Coisas, do inglês, *internet of things* e *low cost*, combinados com os termos chaves: *home security*, *door sensor* e *window sensor*.
- **Crítérios de inclusão e exclusão:** selecionou-se trabalhos relevantes que tenham sido publicados há no máximo 5 anos, de 2015 a 2020, com objetivo de evitar a utilização tecnologias obsoletas.
- **Levantamento de estudos aptos a serem incluídos na revisão:** leitura e avaliação do título e resumo/abstract dos trabalhos pré-selecionados, para inclusão ou descarte.
- **Avaliação da qualidade:** comparação entre os resultados dos trabalhos selecionados ponderação das soluções propostas, considerando que o trabalho para ser selecionado precisaria ter a especificação dos componentes utilizados.

Segundo Sampaio; Mancini (2007), são necessárias boas perguntas a serem respondidas, na revisão da literatura, portanto, definiu-se as seguintes: quais microcontroladores e componentes baseados em Internet das Coisas são usados em soluções para segurança residencial e quais soluções para armazenamento e alerta das informações obtidas? Dentre estes, quais são os de menor custo?.

Os termos foram elaborados para que pudessem relacionar os trabalhos com a temática de Internet das Coisas, baixo custo, segurança residencial e sensores de abertura de portas e janelas, todos esses termos ligados pelo operador lógico “E”, proporcionando a combinação da expressão principal com as características específicas que se fez necessária para o trabalho.

A combinação de termos secundários com o termo principal, que é Internet das Coisas, ficou da seguinte maneira conforme **Quadro 2**.

**Quadro 2** - Termos combinados para pesquisa nas bases de dados

<b>Termo principal</b>	<b>Operador</b>	<b>Termo secundário</b>	<b>Termo terciário</b>
<i>"internet of things"</i>	AND	<i>"home security"</i>	<i>"low cost"</i>
<i>"internet of things"</i>	AND	<i>"home alert sensor"</i>	<i>"low cost"</i>
<i>"internet of things"</i>	AND	<i>"door sensor"</i>	<i>"low cost"</i>
<i>"internet of things"</i>	AND	<i>"window sensor"</i>	<i>"low cost"</i>

Fonte: Elaborado pelo autor (2021).

Para Letouze et al. (2016), os critérios de inclusão e exclusão são definidos quando se desenvolve o protocolo da revisão sistemática e deles se determina quais estudos primários serão usados na mesma. Os critérios para inclusão na pesquisa bibliográfica são: língua que o trabalho foi escrito, sendo estabelecido também como condição de exclusão trabalhos não escritos em inglês e que não fossem artigos de periódicos.

Critérios de inclusão conforme a lista a seguir:

- Artigos publicados em periódicos;
- Trabalhos escritos em língua inglesa;
- Publicações de janeiro de 2015 a junho 2020.

Critérios de exclusão conforme a lista a seguir:

- Trabalhos que não fossem artigos;
- Não fossem publicados em periódicos;
- Artigo que não fosse escrito em inglês;
- Trabalhos anteriores a janeiro de 2015.

A definição das bases de dados utilizada para a pesquisa deu-se conforme sugestões definidas por Letouze et al. (2016). Considerou-se as bases de dados disponíveis por meio da internet, que possibilitassem a pesquisa avançada e acesso livre. As referidas bases de dados e os seus respectivos endereços para acesso estão demonstrados no **Quadro 3**.

**Quadro 3** - Base de dados utilizadas na pesquisa

<b>Base de dados</b>	<b>Endereço</b>
Google Acadêmico	<a href="https://scholar.google.com">https://scholar.google.com</a>
Science Direct – Elsevier	<a href="https://www.sciencedirect.com/">https://www.sciencedirect.com/</a>
ACM – Digital Library	<a href="https://dl.acm.org/">https://dl.acm.org/</a>
Portal de Periódicos da CAPES – <i>Café</i>	<a href="http://www.periodicos.capes.gov.br/">http://www.periodicos.capes.gov.br/</a>
IEEE Xplorer	<a href="https://ieeexplore.ieee.org/">https://ieeexplore.ieee.org/</a>

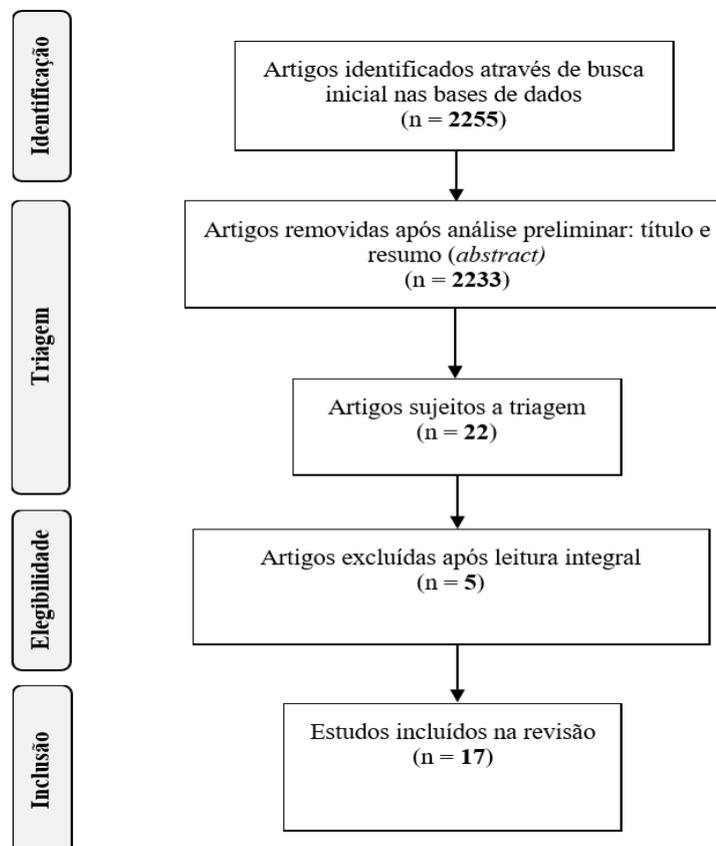
Fonte: Elaborado pelo autor (2021).

A fase de identificação consiste nos resultados primários obtidos nas bases de dados selecionadas, o resultado desse procedimento foi um total de 2255 artigos. Após a identificação, aplicou-se a análise prévia que consiste na leitura do título e resumo/*abstract*. Esse procedimento permitiu a primeira análise dos trabalhos pré-selecionados, identificando os que têm ou não relação com o tema proposto.

Na fase de triagem, aplicou-se os critérios de exclusão e inclusão, com objetivo de refinar o resultado da primeira busca. O resultado dessa fase foi o descarte de 2233 artigos, pois, não foram encontrados nos títulos ou resumos/abstracts elementos em correlação com o que se buscava.

Para analisar se o trabalho estaria apto a compor a base literária da pesquisa, buscou-se aprofundar mais na leitura e análise, contemplando as sessões: introdução, materiais e métodos, dos 22 artigos selecionados. Nessa etapa, 5 foram excluídos. Por fim, selecionou-se 17 artigos que tratam dos temas Internet das Coisas e Segurança Residencial, os quais apontam soluções e demonstram experimentos com os componentes utilizados. O fluxo de trabalho com as etapas da revisão foi demonstrado na **Figura 1**, juntamente das quantidades de trabalhos.

**Figura 1** - Etapas da revisão da literatura.



Fonte: Elaborada pelo autor (2021).

Na **Tabela 2** é demonstrada a quantidade de trabalhos em cada fase de seleção. A segunda coluna traz os resultados brutos utilizando os termos de buscas e critérios definidos anteriormente e aplicado a cada buscador das bases de dados. A terceira coluna demonstra os trabalhos pré-selecionados após a leitura do título e o resumo ou abstract. A última coluna, “selecionados”, quantifica os trabalhos selecionados depois das etapas de avaliação de objetivo e demonstração do resultado, estes incluídos na revisão.

**Tabela 2** - Resultado das buscas avançadas nas bases de dados

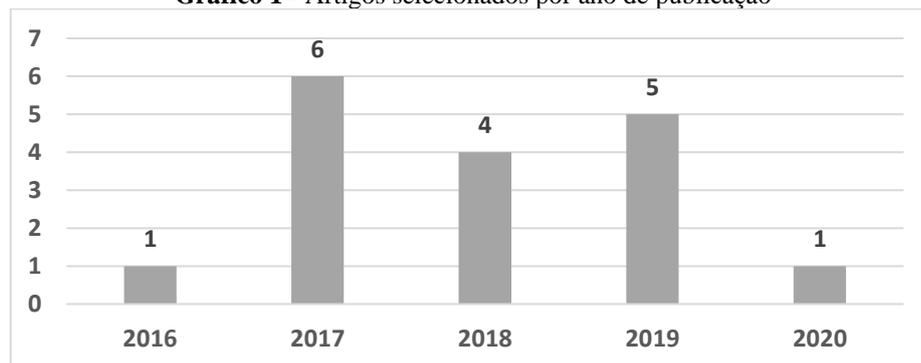
Base de dados	Resultado	Pré-selecionado	Selecionados
Google Acadêmico	2210	13	9
Science Direct – Elsevier	13	5	4
ACM – Digital Library	23	1	1
IEEE Xplorer	9	3	3
TOTAL	2255	22	17

Fonte: Elaborada pelo autor (2021).

Observou-se que o resultado do Google Acadêmico, retornou diversos trabalhos de outras bases, incluindo aquelas que fazem parte da lista desta revisão. Sendo assim, foi preciso desconsiderar esses resultados para evitar duplicidade de trabalhos pré-selecionados. Desse modo, pode-se observar a grande quantidade de resultados da busca preliminar e a quantidade menor de trabalhos selecionados desta base específica.

O **Gráfico 1** demonstra a quantidade de artigos selecionados em cada ano. Nele pode ser observado que apesar de a busca ter sido feita entre 2015 e 2020, trabalhos anteriores a 2017 não satisfizeram os critérios de inclusão.

**Gráfico 1** - Artigos selecionados por ano de publicação



Fonte: Elaborado pelo autor (2021).

No projeto de Aldawira et al. (2019) é utilizado o microcontrolador da empresa *Espressif Systems*, o ESP32, pois o mesmo possui dois núcleos, um para executar funções *wi-fi* e o outro para executar o programa carregado. O ESP32 também possui um módulo *wi-fi* e *bluetooth* e

36 *GPIO*<sup>2</sup>, possui uma memória bastante grande e consome pouca energia, além de possuir um sensor de toque interno, o que o torna adequado para uso em projetos de desenvolvimento de sistemas de segurança de portas.

Já Patel et al. (2019) utiliza *Raspberry Pi* na versão 3B+ (plus), pois tem a necessidade de processar imagens para reconhecimento, utilizando *Raspberry Pi Camera*. O protótipo do sistema consiste em um pequeno computador (*Raspberry Pi Modelo 3B +*), uma câmera (*Raspberry Pi Camera Module v2*), um serviço em nuvem – *Amazon Web Services (AWS)*, um sensor de proximidade (sensor infravermelho), um comutador (para imitar uma campainha), uma lâmpada *LED* (para imitar a porta), uma tela *LCD* e um aplicativo Android.

Surantha; Wicaksono (2018) utilizam *Raspberry Pi 3*, porque esta placa pode realizar processamento de imagem consumindo pouca energia com computador e *laptop*. Também é utilizado *Arduíno UNO* para integrar todos os dispositivos eletrônicos em um ambiente.

Na proposta de Nadafa et al. (2020) também foi utilizado *Raspberry Pi 3*, justificado pelos desafios de processamento e reconhecimento de imagem. Conforme colocado pelos autores, o maior desafio foi trabalhar com sistemas embarcados, que necessita de um conhecimento adequado do *hardware*. *Raspberry Pi* é um dispositivo com baixa capacidade de processamento e armazenamento, a versão mais recente do *Raspberry* possui apenas 1 GB de RAM. Portanto, projetar o modelo proposto com um dispositivo de processamento tão baixo é um grande desafio. Outro desafio é fornecer a máxima precisão possível na detecção de invasões humanas.

Um aspecto importante no desenvolvimento de sistemas baseados em Internet das Coisas é o microcontrolador, o qual é responsável pela união de todos os componentes envolvidos na solução. Para a escolha do microcontrolador é importante levar-se em consideração o custo total da solução, nesse aspecto, observou-se que as soluções propostas nos trabalhos escolhidas mudaram de acordo com o ano de cada trabalho, característica justificada pelo avanço das tecnologias embarcadas. Além do mais, a aplicação da proposta torna-se fator preponderante ao decidir por um microcontrolador mais robusto, ou mais simples.

Foi organizado uma tabela com todos os modelos de microcontroladores utilizados nos trabalhos selecionados, agrupado por modelo próximo, não distinguindo as diferentes versões, por exemplo, o microcontrolador *Raspberry Pi*, que existe diversas versões: *A+*, *B*, *Pi 2*, *Pi*

---

<sup>2</sup> GOIP – Portas de entrada e/ou saída programáveis utilizadas para comunicação com sensores e outros dispositivos.

*Zero, Pi 3, Pi 3 model B+* etc. Após esse agrupamento foi feito o levantamento de quantas vezes ocorria cada um dos diferentes dispositivos, conforme tabela a seguir:

**Tabela 3** - Microcontroladores apresentados nos trabalhos da revisão

<b>Microcontrolador</b>	<b>Menções</b>
Raspberry Pi	7
Beaglebone	1
TI-CC3200	1
Arduíno Mega	4
ESP8266	4
Arduíno UNO	3

Fonte: Elaborada pelo autor (2021).

A síntese dos trabalhos pesquisados mostrou que uma solução para segurança residencial precisa ir além de garantir o alerta de acesso não autorizado, as soluções apresentadas variam da escolha de componente conforme a necessidade de cada cenário, porém alguns itens são fundamentais ao longo da maior parte das pesquisas: o registro das ações e envio de alerta em situações adversas. Com isso, ressalta-se a estes dois devem estar presentes no trabalho da central de segurança residencial de baixo custo desenvolvido por essa proposta.

### 3 ESPECIFICAÇÃO DO SISTEMA PARA SEGURANÇA RESIDENCIAL

A percepção do uso de Internet das Coisas na elaboração de protótipos para resolução de problemas do cotidiano torna-se quase que automática, considerando a crescente popularidade dessas tecnologias. Pensando na praticidade do uso e acesso, este trabalho teve o cuidado de selecionar os melhores componentes que se adequassem ao tema, com a proposta de baixo custo. Nesse sentido, será demonstrado, de forma específica, os componentes e o passo a passo para montagem de uma central de segurança residencial de baixo custo.

#### 3.1 Componentes utilizados

Todos os componentes utilizados na solução estão disponíveis no mercado por preços acessíveis. Os componentes classificados como essenciais são aqueles que estão diretamente ligados ao funcionamento geral da solução, e opções, sensores que podem ou não fazer parte da lista de componentes da solução final. Desta maneira, permite-se que a solução seja customizada para cada caso específico, proporcionando assim um custo final ideal para cada caso.

##### 3.1.1 Microcontrolador ESP8266

O microcontrolador ESP8266, da empresa *Espressif Systems*, possui processador *Tensilica L106 32-bit* e módulo *wi-fi* integrado. Este é ideal para os projetos que necessitam de conectividade, pois dispensa o uso de *hardware* externo.

**Figura 2** - Microcontrolador ESP8266



Fonte: Espressif (2015).

Outros detalhes do ESP8266 no quadro a seguir:

**Quadro 4** - Especificações do microcontrolador ESP8266

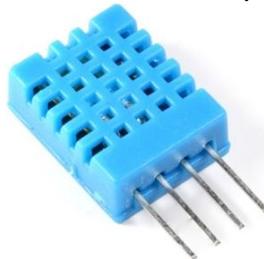
<i>Wi-Fi</i>	Protocolos: 802.11 b/g/n (HT20). Faixa de frequência: 2.4 GHz ~ 2.5 GHz (2400 MHz ~ 2483.5 MHz). Poder de transmissão: 802.11 b: +20 dBm 802.11 g: +17 dBm 802.11 n: +14 dBm. Sensibilidade de recebimento: 802.11 b: -91 dBm (11 Mbps) 802.11 g: -75 dBm (54 Mbps) 802.11 n: -72 dBm (MCS7). Antena: PCB Trace, External, IPEX Connector, Ceramic Chip
<i>Hardware</i>	CPU: Tensilica L106 32-bit processor. Interface de periféricos: UART/SDIO/SPI/I2C/I2S/IR Remote Control GPIO/ADC/PWM/LED Light & Button. Voltagem de operação: 2.5 V ~ 3.6 V Corrente de Operação: valor médio 80 mA. Faixa de temperatura de operação: -40 °C ~ 125 °C Dimensões: 5 mm x 5 mm
<i>Software</i>	Modo <i>wi-fi</i> : Station/SoftAP/SoftAP+Station Segurança: WPA/WPA2 Criptografia: WEP/TKIP/AES Atualização da <i>firmware</i> : UART Download / OTA (via network) Desenvolvimento de <i>software</i> : Suporta desenvolvimento de servidor na nuvem / <i>Firmware e SDK</i> com programação rápida no chip; Protocolos de rede: Ipv4, TCP/UDP/HTTP

Fonte: Adaptado de Espressif (2015).

### 3.1.2 Sensor de umidade e temperatura DHT11

O sensor de umidade e temperatura DHT11 da fabricante *Aosong*<sup>3</sup>, utiliza componente medidor de umidade e um componente NTC para medir temperatura, ambos ligados a um controlador de 8 bits.

**Figura 3** - Sensor de umidade e temperatura DHT11



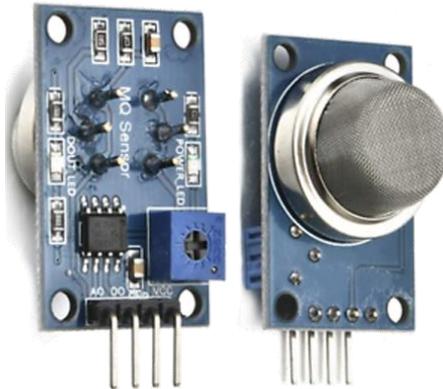
Fonte: Adaptado de Aosong (2019).

<sup>3</sup> Aosong. Disponível em: <https://ww.aosong.com>. Acesso em: 5 de dez. 2021.

### 3.1.3 Sensor de gás e fumaça MQ-2

O sensor de gás MQ-2 é capaz de detectar, no ar, a presença de gases combustíveis e fumaça, sendo ideal para uso próximo em cozinhas com fogão alimentado por gás GLP. O sensor possui um regulador para ajustar o nível de sensibilidade, adaptando-se a diversas situações encontradas nos ambientes distintos.

**Figura 4** - Sensor de gás MQ-2



Fonte: Adaptado de Flying (2019).

### 3.1.4 Sensor de chama fogo 760 a 1100 nm

Para detecção de chamas e outras fontes do calor, utilizou-se o sensor de fogo 760 a 1100 nm, que funciona com a identificação das ondas de calor a partir do comprimento do ario da chama emitida. É possível realizar o ajuste no potenciômetro acoplado ao componente, o qual é importante devido a quantidade de luminosidade que pode incidir no local monitorado. Desta maneira, elimina-se o acionamento falso do sensor.

**Figura 5** - Sensor de chama 760 a 1100 nm



Fonte: Arquivos do autor (2021).

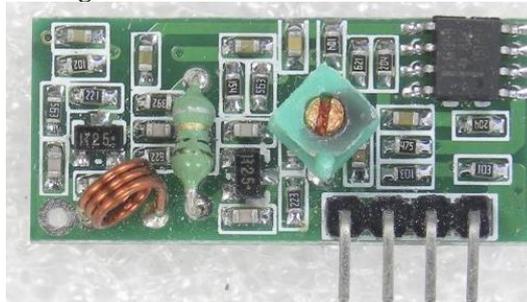
### 3.1.5 Transmissor RF XLC-RF-5V

Para integração com sensores de abertura e presença sem fio, que utilizem frequência de curto alcance na faixa de 433 Mhz com protocolo HT6P20, utiliza-se o transmissor de rádio frequência XLC-RF-5V.

Ressalta-se que no mercado existem outros tipos de sensores de abertura e presença sem fio, porém todos com protocolo proprietário, ou seja, que depende de *hardware* específico para funcionamento.

O protocolo HT6P20 é aberto, e pode ser decodificado por qualquer transmissor de rádio frequência que opere na faixa de 433 mhz, sendo assim, esse foi incluído no projeto.

**Figura 6** - Transmissor RF XLC-RF-5V



Fonte: Adaptada de Murta (2018).

### 3.1.6 Sensor magnético sem fio IPEC

Foi utilizada para monitoramento de aberturas não autorizada o sensor magnético IPEC. Este sensor opera na frequência 433 mhz e protocolo HTP20 compatível com o receptor de rádio frequência apresentado anteriormente.

**Figura 7** - Sensor magnético sem fio IPEC.



Fonte: Arquivos do autor (2021).

### 3.1.7 Módulo GMS SIM800L EVB

O módulo SIM800L é um comunicador que utiliza tecnologia GSM e GPRS para realizar ligações e enviar SMS, com ele também é possível conectar à rede de dados móvel. Este módulo faz o papel de um telefone celular, permitindo a integração com o microcontrolador por meio dos recursos das operadoras de telefonia móvel.

**Figura 8** - Módulo GMS SIM800L EVB.



Fonte: Adaptada de Wireless Solutions (2013).

### 3.1.8 Sistema de alimentação

Para fornecimento da corrente elétrica contínua, foi utilizado um acumulador (bateria) de 12V com 7A para alimentação principal do circuito, ligada à rede de energia elétrica por meio de uma fonte carregadora 12V 3A. A corrente é regulada para tensão de 5V pelo componente LM2596. O microcontrolador é alimentado pela entrada VIN de 5V, os demais componentes externos ao microcontrolador são alimentados pela corrente de saída do regulador de tensão.

**Figura 9** - Fonte carregador 12V 3<sup>a</sup>.



Fonte: Arquivos do autor (2021).

**Figura 10** - Bateria 12V 7A para alimentação do circuito.



Fonte: Adaptada de Barasch (2020).

**Figura 11** - Regulador de tensão LM2596.



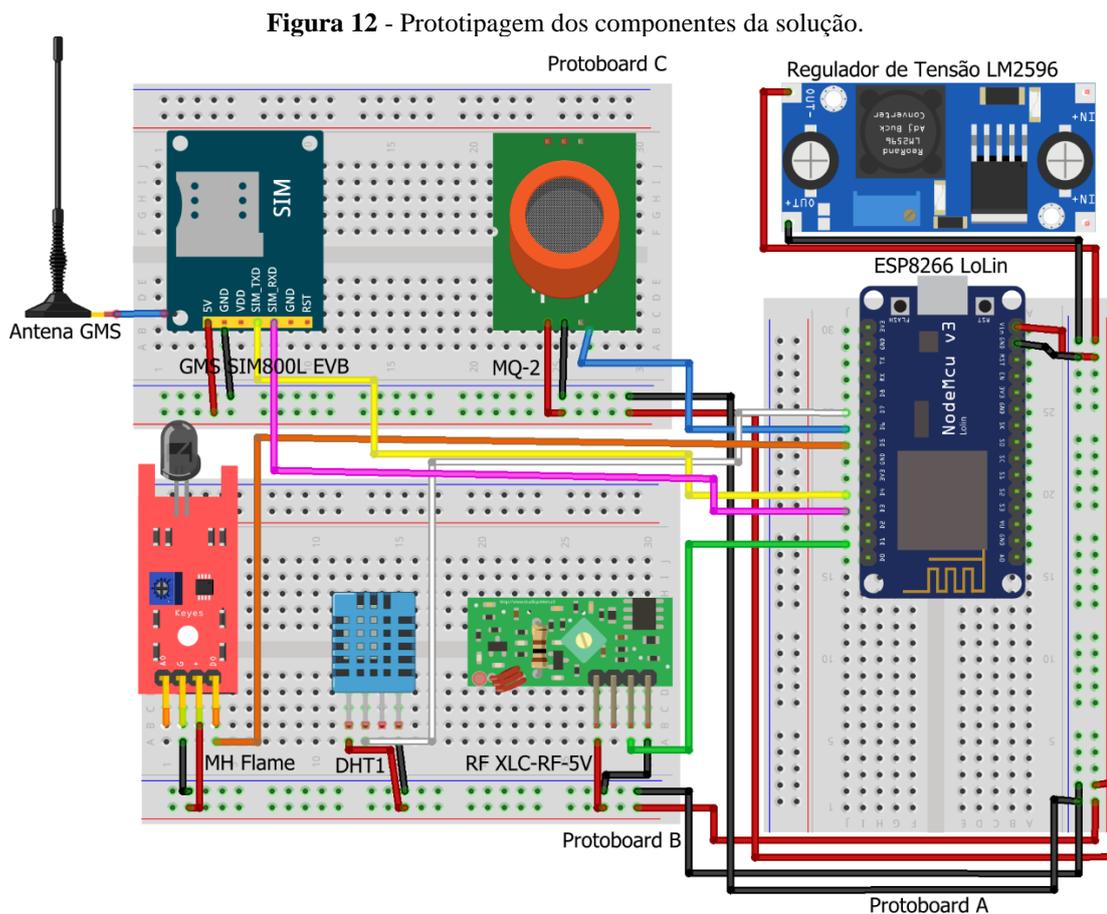
Fonte: Adaptada de Instruments (2020).

## 4 MODELAGEM DO SISTEMA

Neste capítulo será apresentada a modelagem do sistema com as fases de prototipagem e montagem do circuito utilizando *proto-board*. Em seguida é apresentado o projeto do circuito elétrico com esquemático e descritivo das conexões. Por fim, são descritos os fluxogramas de funcionamento do *software* detalhando toda lógica programada.

### 4.1 Prototipação e montagem dos componentes

Para chegar à versão final da solução foi realizada a montagem dos componentes utilizando *proto-board* e *jumps*, o que facilitou a testagem do funcionamento do circuito. Na **Figura 12** é apresentado o esquema de prototipagem dos componentes interligados.



Fonte: Elaborada pelo autor (2021).

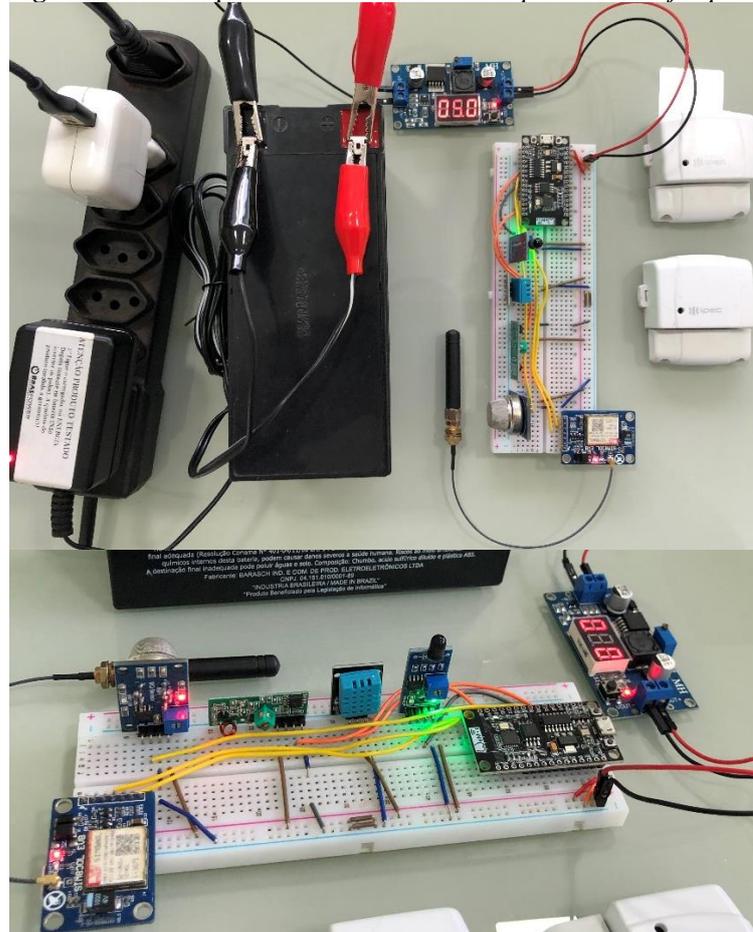
**Quadro 5** - Componentes utilizados na prototipagem.

Número	Componente
1	Bateria 12V 7A
2	Fonte carregador 12V 3000mA
3	<i>Jumps</i>
4	<i>Protoboard</i>
5	Microcontrolador ESP8266
6	Sensor de gás e fumaça MQ-2
7	Regulador de tensão LM2596
8	Sensor de temperatura e umidade DHT11
9	Módulo GSM SIM800L
10	Receptor Rádio Frequência XLC-RF-5V
11	Antena GSM
12	Sensor de chama 760 a 1100 nm
13	Sensor de abertura Magnético sem fio IPEC

Fonte: Elaborado pelo autor (2021).

Na **Figura 13** é apresentado o protótipo em teste de bancada com todos os componentes ligados. Após chegar a essa versão final do protótipo, desenvolveu-se o projeto do circuito impresso, demonstrado no subcapítulo 4.2.

**Figura 13** - Protótipo de circuito montado com *protoboard* e *jumps*.

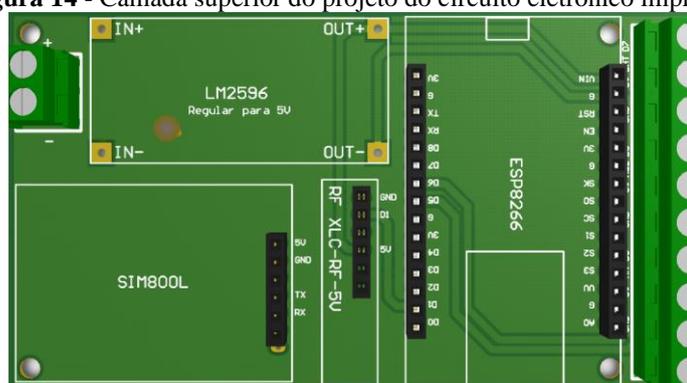


Fonte: Arquivos do autor (2021).

## 4.2 Desenvolvimento do circuito impresso

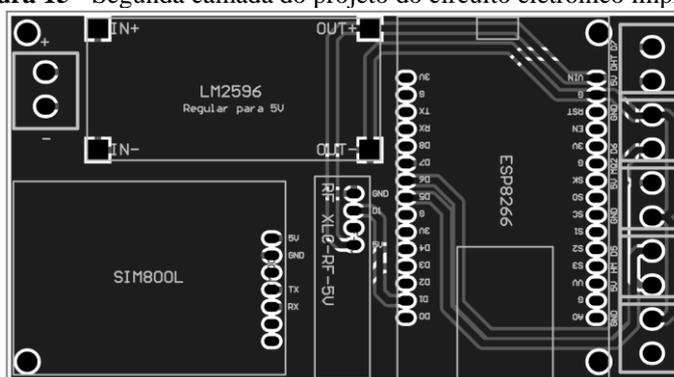
O circuito impresso da solução foi projetado para ter os componentes: regulador de tensão LM2596, RF XLM-5V e SIM800L fixo na placa impressa; e os outros componentes externos: soquetes para conexão externas, que necessitam ser colocados em algum ambiente específico, conforme **Figura 14 e 15**. No Anexo C é apresentado o esquema do circuito impresso detalhando as portas e conexões dos componentes.

**Figura 14** - Camada superior do projeto do circuito eletrônico impresso.



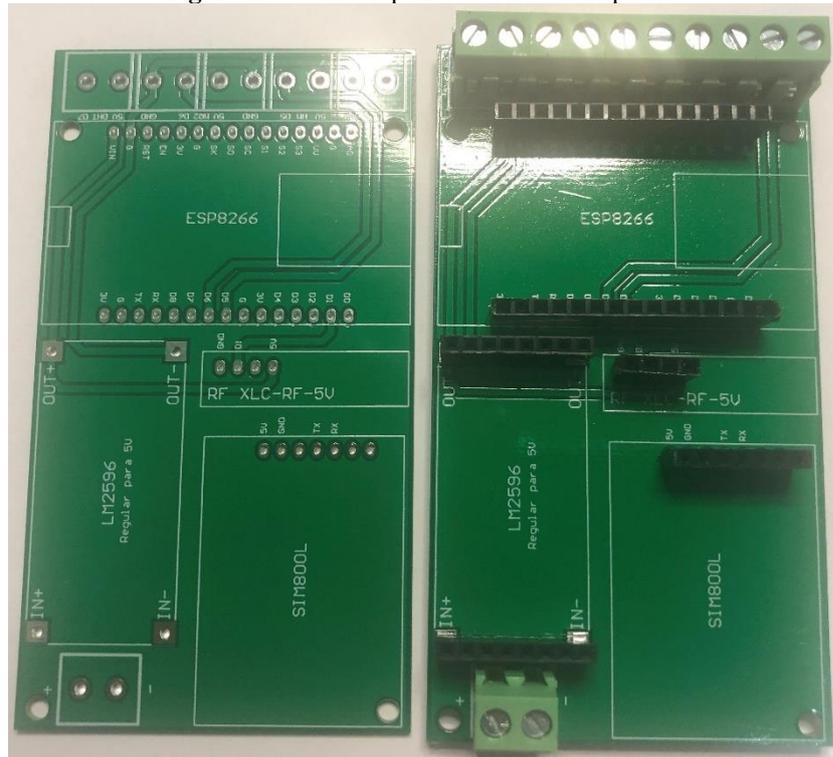
Fonte: Elaborada pelo autor (2021).

**Figura 15** - Segunda camada do projeto do circuito eletrônico impresso.



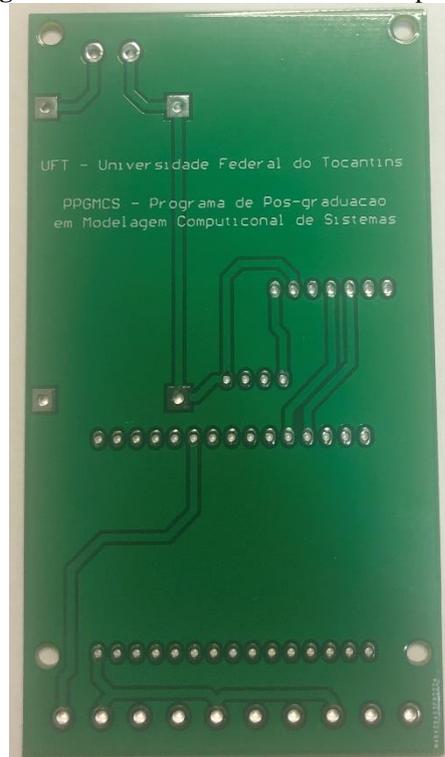
Fonte: Elaborada pelo autor (2021).

**Figura 16** - Visão superior do circuito impresso.



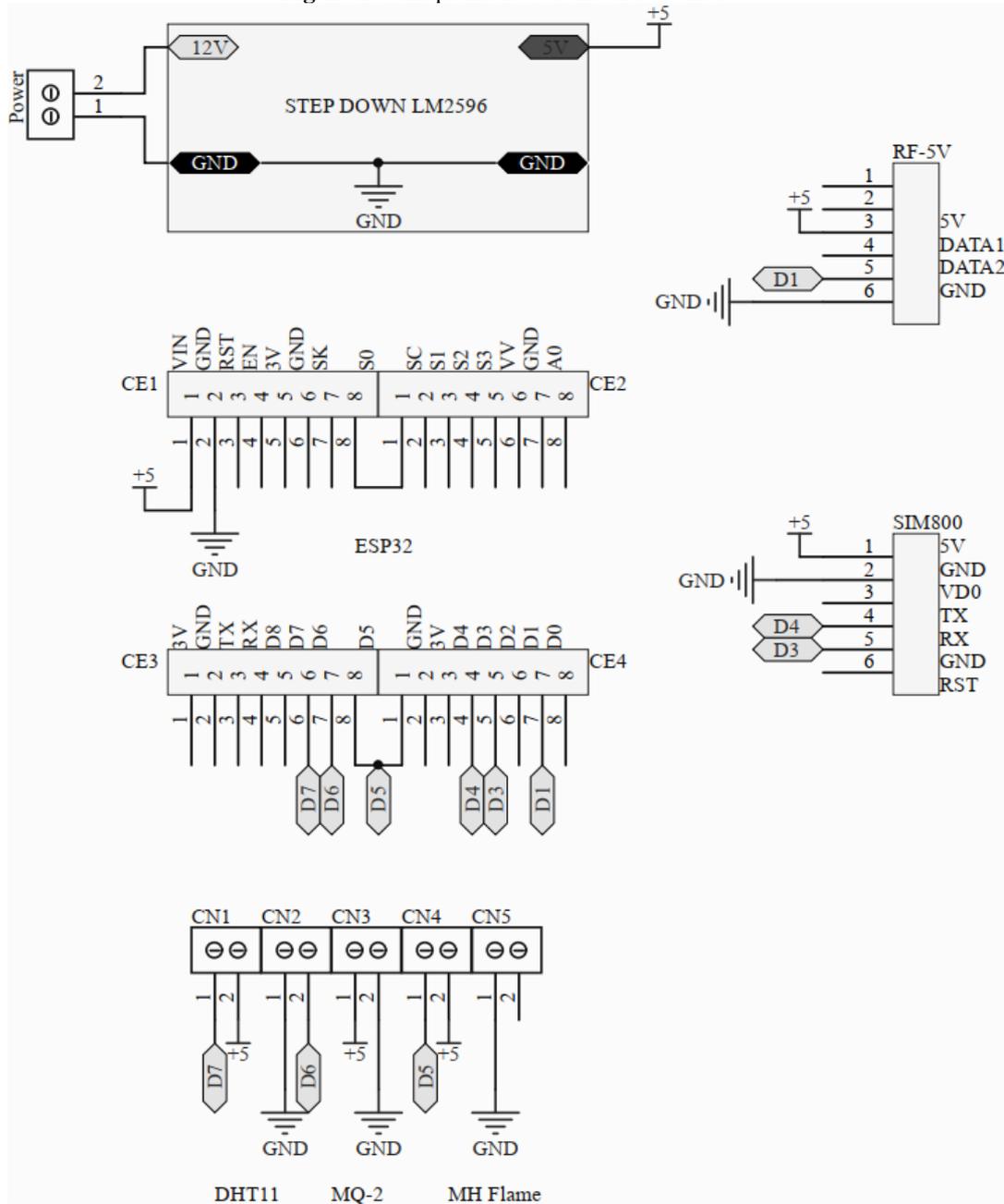
Fonte: Arquivos do autor (2021).

**Figura 17** - Visão inferior do circuito impresso.



Fonte: Arquivos do autor (2021).

**Figura 18** - Esquemático do circuito elétrico.



Fonte: Elaborada pelo autor (2021).

### 4.3 Programação do microcontrolador

A programação do microcontrolador ESP8266 deu-se por meio da *IDE*<sup>4</sup> Arduino, que utiliza linguagem C/C++. A comunicação entre o computador, a *IDE* e o microcontrolador é

<sup>4</sup> *Integrated Development Environment* – Ambiente de Desenvolvimento Integrado.

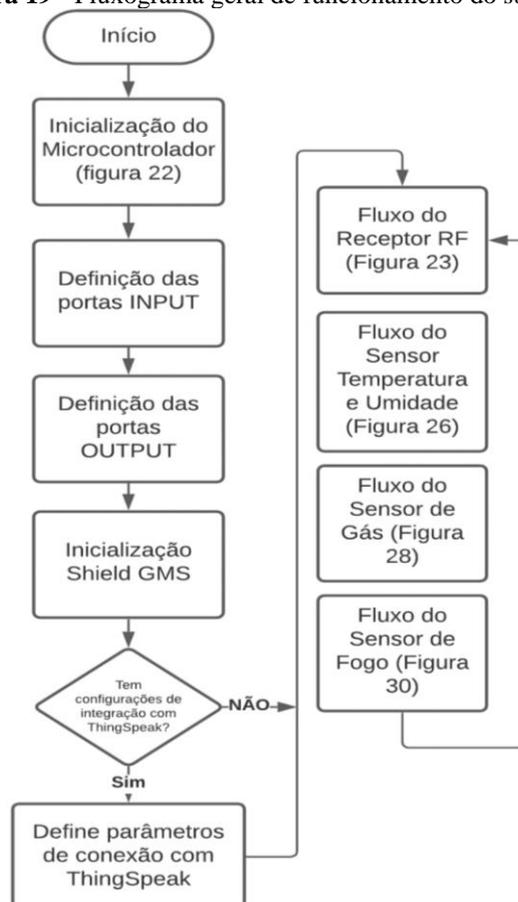
realizada por meio de comunicação serial pela porta *USB*<sup>5</sup>. Segundo Stevan (2018), o *software* Arduino é, primordialmente, uma ferramenta de edição de linguagem de alto nível.

O fluxograma da **Figura 19** descreve o funcionamento geral do *software* desenvolvido para o circuito. O primeiro passo é a inicialização do microcontrolador, após as definições de portas para entrada e saída (*INPUT/OUTPUT*). Em seguida é realizada a inicialização da *shield* *GMS*. Logo após, é verificado se existem configurações para a integração com a plataforma *ThingSpeak*, (explicado no subcapítulo 4.3.8), com o propósito de realizar a conexão com a plataforma e deixar o dispositivo pronto para enviar as informações.

Ao finalizar as configurações iniciais, o fluxo do sistema passa para a função *loop* que executa em repetição as instruções de leituras dos sensores, na seguinte sequência:

1. Receptor de rádio frequência (sensores de abertura sem fio);
2. Sensor de temperatura e umidade (DHT11);
3. Sensor de gás;
4. Sensor de fogo.

**Figura 19** - Fluxograma geral de funcionamento do *software*.



Fonte: Elaborada pelo autor (2021).

<sup>5</sup> *Universal Serial Bus* – Porta serial universal.

### 4.3.1 Bibliotecas utilizadas

Para o desenvolvimento da solução foram empregadas bibliotecas que facilitam a complexidade da utilização de alguns componentes. As bibliotecas incluídas na solução estão representadas no quadro a seguir:

**Quadro 6** - Bibliotecas utilizadas na programação.

Biblioteca	Desenvolvedor	Descrição
SoftwareSerial.h	Arduino	Utilizada comunicação serial entre microcontrolador e dispositivos externos, exemplo: módulo GMS e computador.
ESP8266WiFi.h	Espressif Systems	Funções para uso do módulo <i>wi-fi</i> ESP8266.
WiFiClient.h	Arduino	Biblioteca com funções de conexão IP.
ESP8266WebServer.h	Espressif Systems	Fornecer funções para iniciar servidor web no ESP8266.
DHT.h	Adafruit	Leitura dos parâmetros do sensor de temperatura e umidade DHT11.
ESPAsyncTCP	Me-No-Dev	Fornecer conexão tcp de forma assíncrona.
ESPAsyncWebServer		Servidor <i>web</i> assíncrono.

Fonte: Elaborada pelo autor (2021).

### 4.3.2 Feature Toggles

Todas as funcionalidades do sistema são controladas por meios de *toggles* (interruptores) organizados no início do código fonte, conforme **Figura 20**:

**Figura 20** - Declaração das variáveis *toggles*.

```

40 /* Feature Toggle
41    Set true to enable feature or false to disable.
42 */
43 bool toggleSendsSMS = true;
44 bool toggleWifiConnection = true;
45 bool toggleFireSensor = true;
46 bool toggleHumidityAndTempertureSensor = true;
47 bool toggleGasSensor = true;
48 bool toggleRFSensor = true;
49 bool toggleThingSpeak = true;

```

Fonte: Elaborada pelo autor (2021).

A aplicação das variáveis *toggles*, dessa maneira, fica sequenciada na função *loop*, responsável por executar as funções, repetidamente, enquanto o microcontrolador estiver ligado, conforme **Figura 21**. Ressalta-se que todas as outras funcionalidades estão organizadas em métodos separados, facilitando a manutenção e o entendimento do código.

**Figura 21** - Função *loop*.

```

163 void loop() {
164   if (toggleRFSensor) {
165     readRFSensors();
166   }
167
168   if (toggleGasSensor) {
169     readGasSensor();
170   }
171
172   if (toggleFireSensor) {
173     readFireSensor();
174   }
175
176   if (toggleHumidityAndTempertureSensor) {
177     readTemperatureAndHumity();
178   }
179 }

```

Fonte: Elaborada pelo autor (2021).

### 4.3.3 Inicialização do sistema

A inicialização do sistema realizada pela função *setup*, também sofre influência das variáveis *toggles*, garantindo a não inicialização dos recursos desligados, conforme mostrado na **Figura 17** e no fluxograma da **Figura 18**.

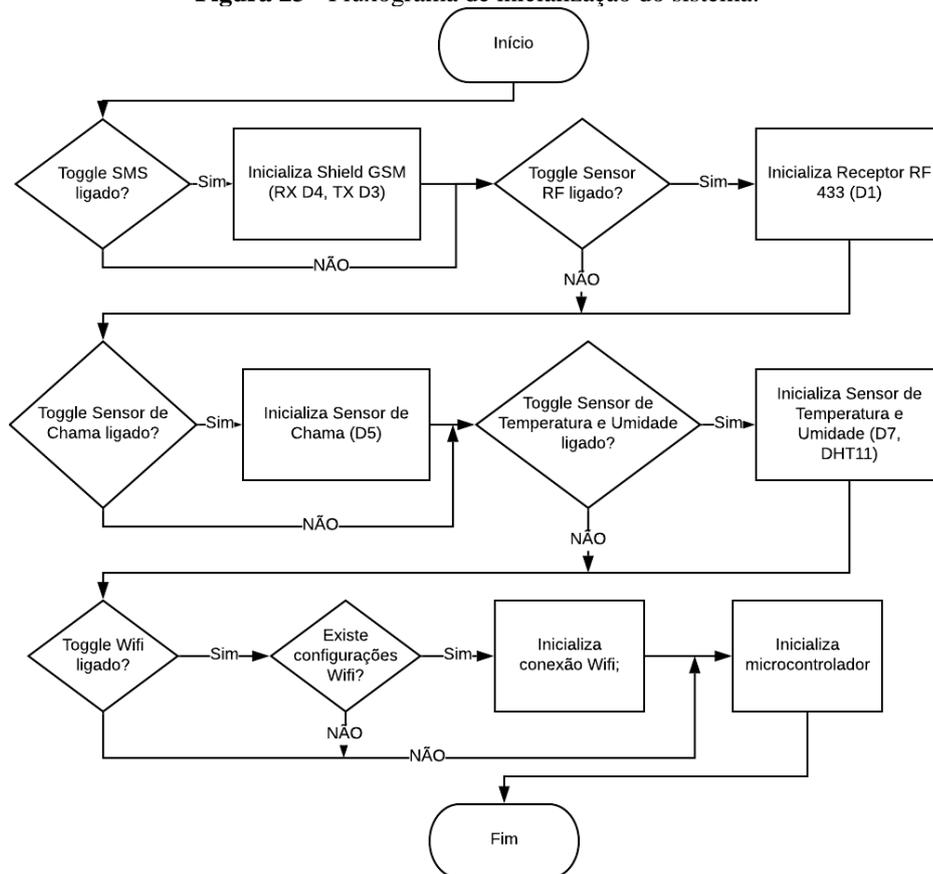
**Figura 22** - Função *setup* inicialização do sistema.

```

111 void setup() {
112   Serial.begin(9600);
113
114   if (toggleSendsSMS) {
115     SIM.begin(9600);
116     delay(1000);
117   }
118
119   if (toggleRFSensor) {
120     pinMode(pinRF, INPUT);
121   }
122
123   if (toggleFireSensor) {
124     pinMode(FIRE_SENSOR, INPUT);
125   }
126
127   if (toggleGasSensor) {
128     pinMode(PIN_GAS, INPUT);
129   }
130
131   pinMode(LED, OUTPUT);
132   digitalWrite(LED, HIGH);
133
134   if (toggleHumidityAndTempertureSensor) {
135     dht.begin();
136
137     lastTemperature = 0.00;
138     lastHumidity = 0.00;
139
140     if ((isnan(whatTemperatureDiference) || whatTemperatureDiference == 0.00) {
141       whatTemperatureDiference = 1.00;
142     }
143
144     if ((isnan(whatHumidityDiference) || whatHumidityDiference == 0.00) {
145       whatHumidityDiference = 1.00;
146     }
147   }
148
149   if (toggleWifiConnection) {
150     WiFi.mode(WIFI_STA);
151     if (!WiFi.config(local_IP, gateway, subnet, primaryDNS, secondaryDNS)) {
152       Serial.println("STA Failed to configure");
153     }
154     WiFi.begin(ssid, password);
155     if (WiFi.waitForConnectResult() != WL_CONNECTED) {
156       Serial.printf("WiFi Failed!\n");
157       return;
158     }
159     Serial.println("IP Address: ");
160     Serial.println(WiFi.localIP());
161     WebSerial.begin(sserver);
162     WebSerial.msgCallback(recvMsg);
163     server.begin();
164   }
165 }

```

Fonte: Elaborada pelo autor (2021).

**Figura 23** - Fluxograma de inicialização do sistema.

Fonte: Elaborada pelo autor (2021).

#### 4.3.4 Funcionamento do receptor rádio frequência 433 mhz e sensor de abertura magnético sem fios

O gerenciamento dos sensores de abertura magnéticos sem fio é feito por meio do receptor de rádio frequência RF-5V-XLC, que, ao receber um sinal na frequência 443 mhz, envia para o processamento do microcontrolador. A função ACT\_HT6P20B\_RX, desenvolvida por Turcato (2014), realiza a checagem do sinal para verificar se é válido para sensores compatíveis.

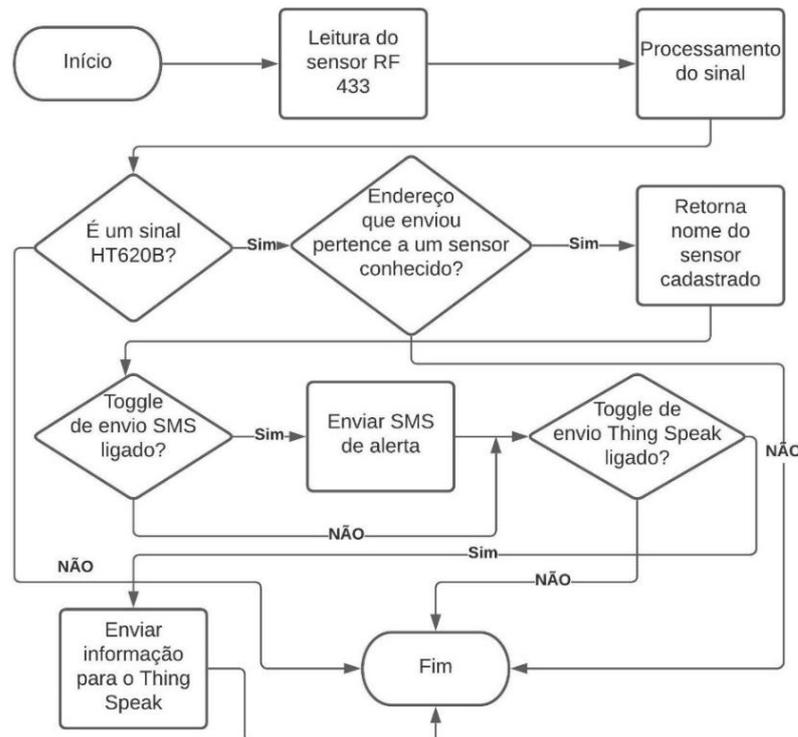
**Figura 24** - Código função da leitura do sensor de rádio frequência.

```

213 void readRFSensors() {
214   int pinRead = digitalRead(pinRF);
215
216   struct rfControl rfControl_1;
217
218   if(ACT_HT6P20B_RX(rfControl_1)) {
219     String sensorFinded = findSensor(String(rfControl_1.addr, HEX));
220
221     if (sensorFinded.length() != 0) {
222       alertDevice("Sensor de abertura detectada: " + sensorFinded);
223       sendThingSpeakInformation(doorWindowsField + "1");
224       delay(milliSecondsToWait());
225     }
226   }
227 }
  
```

Fonte: Elaborada pelo autor (2021).

**Figura 25** - Fluxograma do funcionamento do receptor de rádio frequência.



Fonte: Elaborada pelo autor (2021).

#### 4.3.5 Funcionamento do sensor de temperatura e umidade

A medição da temperatura e umidade é feita por meio do sensor DHT11. Esses parâmetros são importantes para monitoramento do bem-estar, em ambientes domésticos e/ou outras aplicações, a exemplo: estoques de material perecível, *data centers*, estufas e residências com *pets* ou idosos.

A lógica da função de leitura de temperatura e umidade consiste em comparar os valores lidos no ciclo atual com os valores do ciclo passado. Se for detectada diferença configurável, por meio de variáveis globais, as notificações poderão ser disparadas.

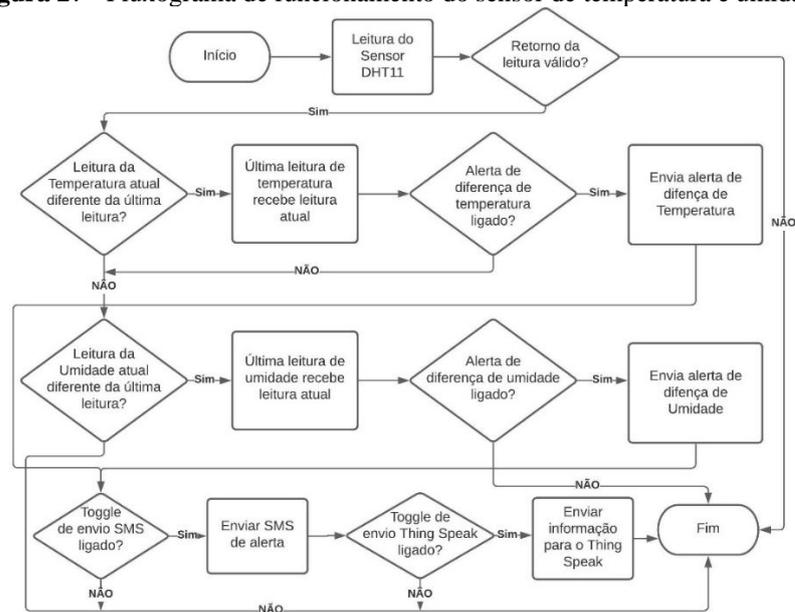
**Figura 26** - Código função da leitura de temperatura e umidade.

```

229 void readTemperatureAndHumidity() {
230     float nowHumidity = dht.readHumidity();
231     float nowTemperature = dht.readTemperature();
232
233     //Humidity and Temperature
234     if (isnan(nowTemperature) || isnan(nowHumidity)) {
235         writeSerial("Falha no sensor DHT11");
236     }
237     else {
238         if (lastTemperature == 0.00) {
239             lastTemperature = nowTemperature;
240         }
241
242         if (lastHumidity == 0.00) {
243             lastHumidity = nowHumidity;
244         }
245
246         float temperatureDifference = (nowTemperature - lastTemperature);
247         float humidityDifference = (nowHumidity - lastHumidity);
248
249         if (abs(temperatureDifference) > whatTemperatureDifference) {
250             printTemperatureDifference(nowTemperature, temperatureDifference);
251             sendThingSpeakInformation(temperatureField + String((int)nowTemperature));
252             lastTemperature = nowTemperature;
253             delay(millisSecondsToWait());
254         }
255
256         if (abs(humidityDifference) > whatHumidityDifference) {
257             printHumidityDifference(nowHumidity, humidityDifference);
258             sendThingSpeakInformation(humidityField + String((int)nowHumidity));
259             lastHumidity = nowHumidity;
260             delay(millisSecondsToWait());
261         }
262     }
263 }
  
```

Fonte: Elaborada pelo autor (2021).

**Figura 27** - Fluxograma de funcionamento do sensor de temperatura e umidade.



Fonte: Elaborada pelo autor (2021).

#### 4.3.6 Funcionamento do sensor de gás

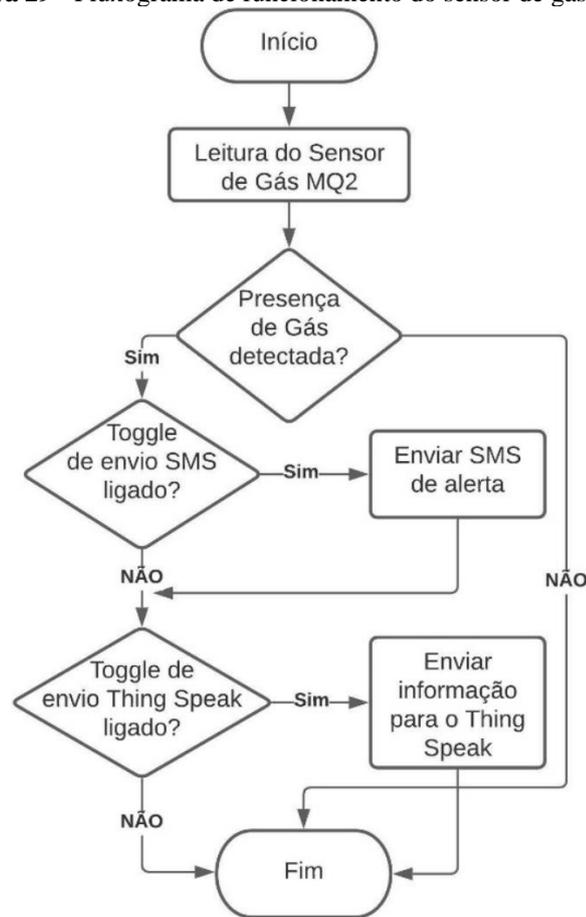
A presença de gás inflamável no ar pode gerar riscos ao ambiente. Por causa disso, o sensor de gás MQ-2 é utilizado para detectar e enviar sinal ao microcontrolador. Este sensor necessita da regulagem de sensibilidade feito pelo potenciômetro presente no componente, conforme **Figura 5**.

**Figura 28** - Função de leitura do sensor de gás MQ2.

```

291 void readGasSensor() {
292   if (digitalRead(PIN_GAS) == LOW) {
293     alertDevice("Gas detectado.");
294     sendThingSpeakInformation(gasField + "1");
295     delay(millisSecondsToWait());
296   }
297 }
  
```

Fonte: Elaborada pelo autor (2021).

**Figura 29** - Fluxograma de funcionamento do sensor de gás MQ2.

Fonte: Elaborada pelo autor (2021).

#### 4.3.7 Funcionamento do sensor de fogo

O sensor de detecção de fogo funciona com a leitura da onda de luz que vai de 760 a 1100 nm, a sensibilidade do acionamento precisa ser configurada fisicamente pelo potenciômetro presente no componente, conforme **Figura 6**. Caso seja acionado o sensor de chama, este envia informação para o microcontrolador que aciona a lógica desenvolvida, conforme fluxograma da **Figura 39**.

**Figura 30** - Função de leitura do sensor de fogo.

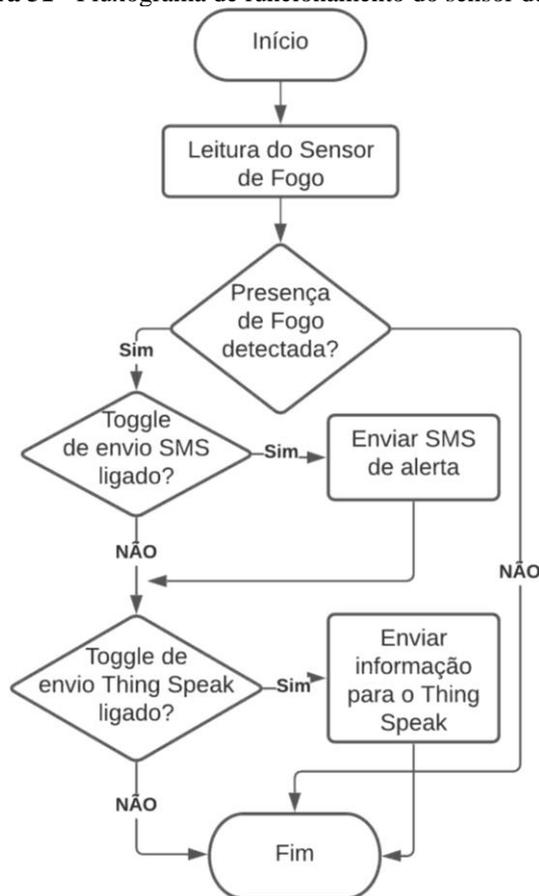
```

299 void readFireSensor() {
300   if (digitalRead(FIRE_SENSOR) == LOW) {
301     alertDevice("Fogo detectado.");
302     sendThingSpeakInformation(fireField + "1");
303     delay(milliSecondsToWait());
304   }
305 }

```

Fonte: Elaborada pelo autor (2021).

**Figura 31** - Fluxograma de funcionamento do sensor de fogo.



Fonte: Elaborada pelo autor (2021).

#### 4.3.8 Integração *ThingSpeak*

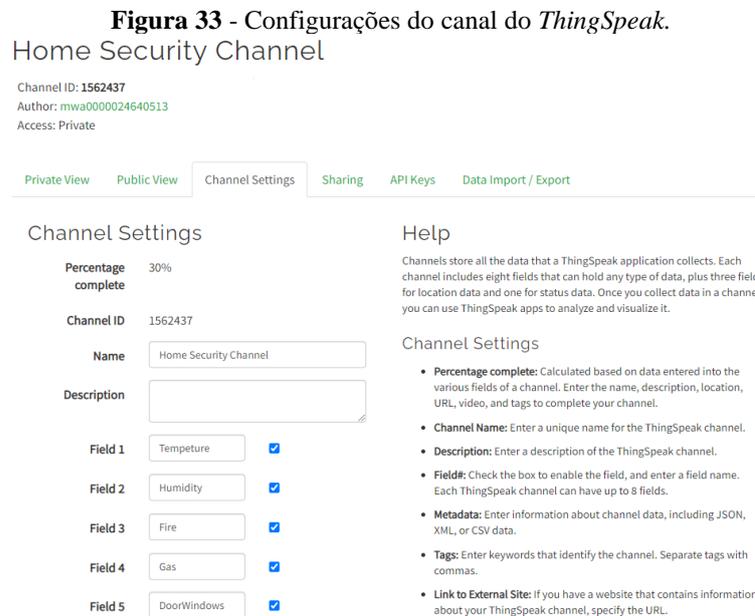
Para o monitoramento de envio dos dados da central de segurança para nuvem, foi utilizada a plataforma *ThingSpeak*. Esta é grátis e permite a criação de até cinco canais para receber informações de dispositivos diferentes.

**Figura 32** - Página inicial do *ThingSpeak*.

Name	Created	Updated
🔒 Home Security Channel	2021-11-08	2021-11-08 01:13

Fonte: Arquivos do autor (2021).

Feito o cadastro na plataforma, é necessária a criação de um canal para o dispositivo monitorado. Assim, utiliza-se os campos da requisição para distinguir os dados recebidos, conforme **Figura 33**.



Fonte: Arquivos do autor (2021).

A função de envio dos dados lidos pelo sensor para a plataforma é relativamente simples, pois utiliza-se da capacidade de conexão com a internet presente no microcontrolador ESP32. Essa conexão abre uma conexão HTTP, realizando uma requisição com os dados lidos pelos sensores. Essa lógica do código é demonstrada na **Figura 34**.

**Figura 34** - Função de envio dos dados para plataforma *ThingSpeak*.

```

265 void sendThingSpeakInformation(String data) {
266   if (!toggleThingSpeak) {
267     return;
268   }
269
270   if (WiFi.status() == WL_CONNECTED) {
271     if (client.connected()) {
272       client.stop();
273       delay(1000);
274     }
275
276     if (client.connect(thingSpeakUrl, 80)) {
277       client.print("POST /update HTTP/1.1\n");
278       client.print("Host: " + thingSpeakUrl + "\n");
279       client.print("Connection: close\n");
280       client.print("X-THINGSPEAKAPIKEY: " + thingSpeakWriteKey + "\n");
281       client.print("Content-Type: application/x-www-form-urlencoded\n");
282       client.print("Content-Length: ");
283       client.print(data.length());
284       client.print("\n\n");
285       client.print(data);
286       writeSerial("Informações enviadas ao ThingSpeak: " + data);
287     }
288   }
289 }

```

Fonte: Elaborada pelo autor (2021).

Com a integração é possível enviar as informações dos sensores para uma *dashboard* de análise, facilitando o acesso e a gestão de múltiplos dispositivos, recurso recomendado para grandes ambientes corporativos.

Para que o dispositivo consiga enviar informações para o canal, é necessário criar uma *Write API Key* na aba *API Keys* do canal, conforme **Figura 35**.

**Figura 35** - Configuração das chaves do canal do *ThingSpeak*.

Private View Public View Channel Settings Sharing API Keys Data Import / Export

### Write API Key

Key

Generate New Write API Key

### Read API Keys

Key

Note

Save Note Delete API Key

### Help

API keys enable you to write data to a channel or read data from a private channel. API keys are auto-generated when you create a new channel.

### API Keys Settings

- **Write API Key:** Use this key to write data to a channel. If you feel your key has been compromised, click **Generate New Write API Key**.
- **Read API Keys:** Use this key to allow other people to view your private channel feeds and charts. Click **Generate New Read API Key** to generate an additional read key for the channel.
- **Note:** Use this field to enter information about channel read keys. For example, add notes to keep track of users with access to your channel.

### API Requests

Write a Channel Feed

```
GET https://api.thingSpeak.com/update?api_key=
```

Fonte: Arquivos do autor (2021).

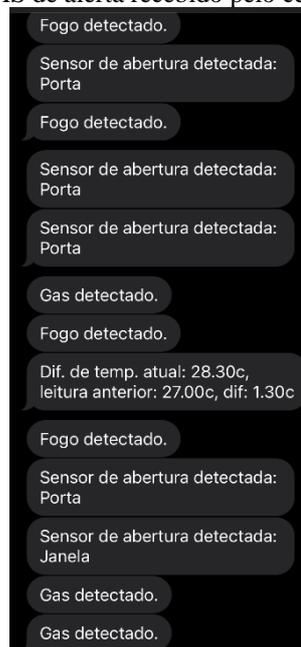
## 5 RESULTADOS E ANÁLISE

Neste capítulo são demonstrados os resultados alcançados com a solução desenvolvida, conforme os objetivos pretendidos. A aplicação da solução e a criação dos produtos também são apresentadas.

### 5.1 Dados e interfaces da solução

O alerta padrão da solução é o envio de SMS por meio de uma operadora de telefonia móvel. Para tanto, é necessário um chip SIM6 colocado no componente SIM800L. Este chip é responsável pelo envio de mensagens cujas ações, posteriormente, serão as seguintes: acionamento de sensor de abertura conhecido, detecção de gás e fogo, mudança de temperatura e umidade. É importante ressaltar que a escolha da operadora deve passar por uma análise que envolve custo e disponibilidade de sinal na região em que a solução será instalada.

**Figura 36** - SMS de alerta recebido pelo celular cadastrado.



Fonte: Arquivos do autor (2021).

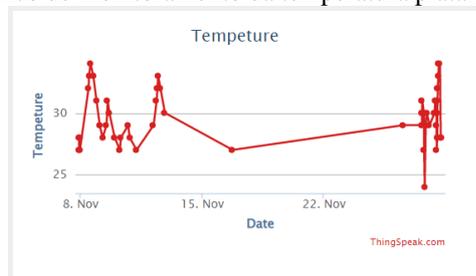
Outra forma de análise dos dados gerados pela solução pode ser realizada através da interface *web* da plataforma *ThingSpeak*. Nas **Figuras 37** e **38** são demonstrados gráficos e

---

<sup>6</sup> Módulo físico de identificação de assinante.

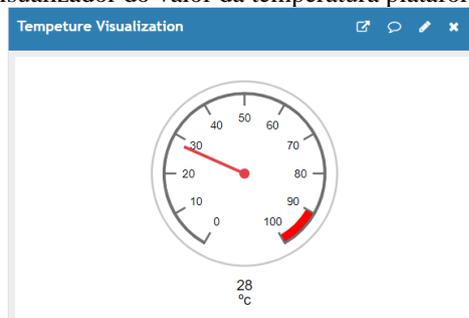
visualizadores dos dados da temperatura, e nas **Figuras 39 e 40** estão representados os dados da umidade obtidos pela solução.

**Figura 37** - Gráfico de monitoramento da temperatura plataforma *ThingSpeak*.



Fonte: Elaborada pelo autor (2021).

**Figura 38** - Visualizador do valor da temperatura plataforma *ThingSpeak*.



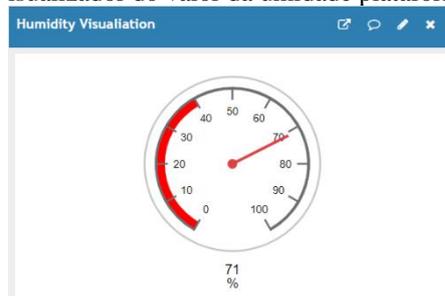
Fonte: Arquivos do autor (2021).

**Figura 39** - Gráfico de monitoramento da umidade na plataforma *ThingSpeak*.



Fonte: Arquivos do autor (2021).

**Figura 40** - Visualizador do valor da umidade plataforma *ThingSpeak*.



Fonte: Arquivos do autor (2021).

## 5.2 Central de segurança residencial

O circuito para solução com os componentes fixos tem dimensões de 100 mm x 55 mm, montado no interior de uma caixa hermética juntamente da bateria e fonte para proteção, ficando externo os sensores DHT11, MQ2 e de fogo.

A alimentação externa é feita por meio do cabo de energia que sai pela extremidade esquerda da caixa, a extremidade direita fica reservada para as conexões com os sensores externos.

**Quadro 7** - Especificações da solução.

Especificações do Sistema	
Dimensões do Circuito	100 mm x 55 mm
Dimensões da caixa	220 mm x 250 mm
Peso	2.7 Kg
Tensão do circuito	5.0 V
Capacidade nominal circuito	480 mA
Tensão da solução completa	110V ~ 230V
Capacidade nominal solução completa	1000 mA

Fonte: Elaborada pelo autor (2021).

**Figura 41** – Proposta de solução montada.



Fonte: Elaborada pelo autor (2021).

### 5.3 Custo da solução

O custo final da solução ficou em R\$ 381,25 não considerando a margem de lucro e os custos com frete e impostos. O detalhamento do custo de cada componente da solução foi disponibilizado no Apêndice B.

Na **Tabela 4** é demonstrada a comparação entre a Central de Segurança IoT e algumas soluções de mercado, ficando evidente que a solução desenvolvida contém mais funcionalidades que as encontradas em outras soluções do mercado.

O custo-benefício da solução desenvolvida, portanto, destaca-se pela maior abrangência de parâmetros monitorados, e pela maior possibilidade de aplicação. Além disso, a possibilidade de modularização da solução faz com que o custo final possa ser adequado para cada situação, indo de monitoramento simples de portas e janelas, a sensor de presença de gás, ou sensor de detecção, cada um destes com o alerta via SMS e envio para plataforma em nuvem.

**Tabela 4** - Comparação de funcionalidades e valores entre soluções de segurança;

Solução	Alerta SMS	Sensor Temperatura e Umidade	Sensor de Fogo	Sensor de Gás	Valor
Central de Segurança IoT	X	X	X	X	R\$ 381,25
Central de Alarme Smart Cloud (JFL)	X				R\$ 282,45
Central de Alarme Intelbras	X				R\$ 407,55
Kit de Alarme Sem Fio	X				R\$ 714,85

Fonte: Elaborada pelo autor (2021).

A solução pode ser aplicada a um conjunto maior de cenários, descritos no quadro a seguir.

**Quadro 8** - Aplicação da solução.

<b>Aplicação de Solução Central de Segurança IoT</b>
<ul style="list-style-type: none"> <li>• Segurança residencial;</li> <li>• Gerenciamento de Temperatura e Acesso a <i>Data Centers</i>;</li> <li>• Gerenciamento de temperatura e Umidade de Locais de Estoques perecíveis;</li> <li>• Segurança de Estoques de Gás Inflamáveis;</li> <li>• Segurança Predial (escolas, condomínios etc.).</li> </ul>

Fonte: Elaborada pelo autor (2021).

## 6 CONCLUSÃO

Este trabalho apresentou o desenvolvimento de um dispositivo voltado para segurança residencial que tinha como um dos objetivos ser de baixo custo. Uma das etapas da pesquisa foi procurar na literatura sobre Internet das Coisas soluções voltadas para segurança doméstica. Com isso, desenvolveu-se um circuito com componentes que permitem monitorar aspectos do bem-estar, como: acesso não autorizado de portas e janelas, presença de gás inflamável no ar, ocorrência de chama, variação da temperatura e umidade. O monitoramento desses aspectos tenciona alertar os proprietários caso algum desses parâmetros seja modificado.

Apesar de já existirem soluções comerciais para segurança residencial, o dispositivo desenvolvido se destaca por conter funcionalidades não encontradas nos produtos presentes no mercado, a exemplo: combinação do alerta via plataforma em nuvem (*ThingSpeak*), presença de gás no ar, ocorrência de incêndio e temperatura e umidade.

A solução desenvolvida alcançou seus objetivos, dentre eles, o de ter baixo custo e oferecer mais recursos que as soluções de mercado. O dispositivo possibilita uma alternativa para a sociedade proteger as residências de eventos adversos, não somente de acesso não autorizado, mas de outras preocupações que ocorrem em casas e locais em relação à segurança.

O *software* que acompanha a solução permite evolução e adaptação aos cenários variados, também pode-se estabelecer modificações pontuais para cobrir possíveis lacunas que a solução inicial possa apresentar. Buscou-se utilizar boas práticas de desenvolvimento de *software* visando garantir qualidade do código, fator primordial para garantir que um sistema não se torne legado, permitindo sua evolução gradual.

O circuito impresso desenvolvido pode ser utilizado de base para outros projetos sobre Internet das Coisas, os quais utilizem os componentes bases: microcontrolador ESP8266, regulador de tensão e *shield* SIM800L. Dessa forma, contribui-se com outros projetos devido a característica aberta e de componentes acoplados via soquete na placa, o que pode facilitar o desenvolvimento de novas soluções.

Os resultados alcançados são satisfatórios em relação aos objetivos alcançados. As etapas metodológicas puderam contribuir para o desenvolvimento de um dispositivo que atenda a aspectos críticos da segurança residencial, auxiliando na prevenção de furtos e roubos a residências, ainda podendo ser aplicado a outras finalidades também importantes como descritos na tabela de aplicação no subcapítulo 5.3.

## 6.1 Trabalhos futuros

A solução desenvolvida por este trabalho demonstrou ser útil e viável, dos pontos de vista técnico e econômico. No entanto, recomenda-se a evolução, partindo do aprimoramento do circuito montado com adição de *displays* de monitoramento dos valores obtidos, de alerta de carga da bateria e de ausência de corrente vinda da rede de energia.

Ainda nos pontos de evolução, o desenvolvimento de um sistema próprio para armazenamento dos dados coletados pode acrescentar, na aplicação desta solução, uma maior competitividade diante dos produtos concorrentes. Esta aplicação própria aumentaria a possibilidade de aplicação da solução podendo ser, inclusive, ferramenta auxiliar para pesquisas em outras áreas, a exemplo: pesquisa de monitoramento climático, pesquisa de acompanhamento de parâmetros do solo, pesquisas voltadas à piscicultura e outras aplicações agrícolas.

É possível ainda ser adicionado o recurso de alerta sonoro através de sirenes de alerta, agregando maiores possibilidades, em caso de acesso não autorizado, e servindo de ferramenta inibidora para residências. Outro recurso que pode ser adicionado, somente por via de *software*, é a possibilidade do alerta ser por chamada telefônica, recurso que não substituiria o alerta via SMS, mas adicionaria uma camada maior de alerta.

## 7 CONTRIBUIÇÕES E PUBLICAÇÕES

**ARTIGO A2 - TÍTULO: PUBLIC SECURITY AND THE INTERNET OF THINGS: AT THE SERVICE OF COMMUNITY POLICING**

Link: <https://ijaers.com/detail/public-security-and-the-internet-of-things-at-the-service-of-community-policing/>

ISSN: 2349-6495

**ARTIGO B1 - TÍTULO: REVISÃO DA LITERATURA SOBRE USO DE INTERNET DAS COISAS NO DESENVOLVIMENTO DE DISPOSITIVOS DE BAIXO CUSTO PARA SEGURANÇA RESIDENCIAL**

Link: <https://jnt1.websiteseuro.com/index.php/JNT/article/viewFile/1279/843>

ISSN: 2526-4281

**APRESENTAÇÃO NA FEIRA TECNOLÓGICA UNIVERSIDADE E EMPRESA (UNITEC). APRESENTAÇÃO DO TRABALHO PALMAS/TO - TÍTULO: TECNOLOGIA DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO É APRESENTADA NA UNITEC**

Link: <https://ww2.uft.edu.br/index.php/en/ultimas-noticias/26251-tecnologia-de-seguranca-residencial-de-baixo-custo-e-apresentada-na-unitec>

**APRESENTAÇÃO NO 2º SEMINÁRIO DE POLÍCIA PREVENTIVA QUE TEVE O TEMA “TECNOLOGIAS APLICADAS NA POLÍCIA OSTENSIVA” - TÍTULO: CENTRAL DE SEGURANÇA RESIDENCIAL DE BAIXO CUSTO NO AUXÍLIO DO POLICIAMENTO COMUNITÁRIO**

Link: <https://www.pm.to.gov.br/noticia/2019/4/24/policia-militar-realiza-2-seminario-de-policia-preventiva/>

**REGISTRO DE PROPRIEDADE INTELECTUAL – SOFTWARE**

**TÍTULO: IOT HOME SECURITY CENTRAL**

**RESPONSÁVEL PELO REGISTRO: NÚCLEO DE INOVAÇÃO TECNOLÓGICA (NIT) UFT**

**STATUS: AGUARDANDO ASSINATURAS**

**REGISTRO DE PROPRIEDADE INTELECTUAL – CIRCUITO IMPRESSO**

**TÍTULO: IOT HOME SECURITY CENTRAL**

**RESPONSÁVEL PELO REGISTRO: NÚCLEO DE INOVAÇÃO TECNOLÓGICA (NIT) UFT**

**STATUS: PROCESSO EM ANDAMENTO**

**ARTIGO A2 - TÍTULO: A STUDY ON THE BUDGETARY IMPACT WITH NEW HIRES IN A MILITARY INSTITUTION**

Link: <http://www.journalijdr.com/study-budgetary-impact-new-hires-military-institution/>

ISSN: 2230-9926

**ARTIGO B2 - TÍTULO: UM ESTUDO SOBRE FERRAMENTAS DE APRENDIZAGEM COLABORATIVA**

Link: <https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/1994>

ISSN: 2358-8322

**ARTIGO B1 - TÍTULO: REVISÃO DA LITERATURA SOBRE O USO DO DESENVOLVIMENTO ÁGIL EM SOFTWARES CORPORATIVOS**

Link: <http://revistas.faculdefacit.edu.br/index.php/JNT/article/view/1093>

ISSN: 2526- 4281

**CAPÍTULO DE LIVRO - TÍTULO: A GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO E A ANÁLISE DA MATURIDADE DOS PROCESSOS UTILIZANDO COBIT**

Link: <http://repositorio.uft.edu.br/handle/11612/1342>

ISBN: 978-85-60487-67-7

## REFERÊNCIAS

- ALDAWIRA, C. R.; PUTRA, H. W.; HANAFIAH, N.; et al. Door Security System for Home Monitoring Based on ESP32. **Procedia Computer Science**, v. 157, p. 673–682, 2019. Elsevier.
- AOSONG. Temperature and humidity module DHT11 Product Manual. , 2019. Aosong. Disponível em: <[https://img.filipeflop.com/files/download/Datasheet\\_DHT11.pdf](https://img.filipeflop.com/files/download/Datasheet_DHT11.pdf)>. .
- BARASCH, E. Datasheet Planet Batery 12V 7A. , 2020. Disponível em: <<http://www.supriwireless.com.br/images/Produtos/Manual/Bateria-12V7.0A.pdf>>. .
- BATRINU, C. **Projetos de Automação Residencial com ESP8266: Aproveite a potência deste minúsculo chip Wi-Fi para construir incríveis projetos de casas inteligentes**. Novatec Editora, 2018.
- BOHN, M. F. Policiamento comunitário: a transição da polícia tradicional para polícia cidadã. **Revista Jus Navigandi**, a, v. 19, p. 1–15, 2014.
- DORNELLES, R. J. A utilização de tecnologias de Internet na educação a distância: o caso de uma disciplina de graduação da Escola de Administração da Universidade Federal do Rio Grande do Sul. , 2001. Disponível em: <<https://www.lume.ufrgs.br/bitstream/handle/10183/2585/000322602.pdf>>. .
- ESPRESSIF, S. ESP8266EX Datasheet. **Espr. Syst. Datasheet**, p. 1–31, 2015.
- EVANS, D. The internet of things: How the next evolution of the internet is changing everything. **CISCO white paper**, v. 1, p. 1–11, 2011.
- FLYING, F. TECHNICAL DATA MQ-2 GAS SENSOR. , 2019. Disponível em: <<http://gas-sensor.ru/pdf/combustible-gas-sensor.pdf>>. .
- GALEGALE, G. P.; SIQUEIRA, É.; SILVA, C. B. H.; SOUZA, C. A. DE. INTERNET DAS COISAS APLICADA A NEGÓCIOS-UM ESTUDO BIBLIOMÉTRICO. **JISTEM-Journal of Information Systems and Technology Management**, v. 13, n. 3, p. 423–438, 2016. SciELO Brasil.
- INSTRUMENTS, T. LM2596 SIMPLE SWITCHER® Power Converter 150-kHz 3-A Step-Down Voltage Regulator. , 2020. Disponível em: <<https://www.ti.com/lit/ds/symlink/lm2596.pdf>>. .
- JUNIOR, W. B. L.; DE ARAUJO, H. X.; TAVARES, F. M. MONITORAMENTO DA QUALIDADE DA ÁGUA UTILIZANDO PLATAFORMA DE INTERNET DAS COISAS. **Humanidades & Inovação**, v. 7, n. 9, p. 46–53, 2020.
- LETOUZE, P.; SOUSA JÚNIOR, J.; SILVA, V. **Um breve guia para revisões sistemáticas aplicado à ciência da computação**. Editoria UFT, 2016.
- MATRAK FILHO, R. A doutrina de polícia repressiva e a sua aplicação na filosofia de polícia comunitária. **Revista Ordem Pública**, v. 3, n. 1, p. 41–56, 2010.

MURTA, G. Guia básico dos Módulos TX / RX – RF 433MHZ. **Eletrogate Blog**, 2018. Disponível em: <<https://blog.eletrogate.com/guia-basico-dos-modulos-tx-rx-rf-433mhz/>>. Acesso em: 3/8/2020.

NADAF, R. A.; HATTUREA, S.; BONALA, V. M.; NAIKB, S. P. Home Security against Human Intrusion using Raspberry Pi. **Procedia Computer Science**, v. 167, p. 1811–1820, 2020. Elsevier.

OLIVEIRA, S. **Internet das Coisas com ESP8266, Arduíno e Raspberry PI**. Primeira Edição ed. São Paulo, 2017.

P. M. DO TOCANTINS. **Diretriz no 001-2017 de novembro de 2017**. 2017.

PADOVEZE, C. L. Aspectos da gestão econômica do capital humano. **Revista de Contabilidade do CRC-SP**, , n. 20, 2000.

PATEL, J.; ANAND, S.; LUTHRA, R. Image-Based Smart Surveillance and Remote Door Lock Switching System for Homes. **Procedia Computer Science**, v. 165, p. 624–630, 2019. Elsevier.

PAUL, A.; UPADHYAY, A.; GAUR, A.; BHANDARI, R. Centralized Security System Based on IoT. **INTERNATIONAL JOURNAL OF RESEARCH IN ADVANCE ENGINEERING**, v. 2, n. 3, p. 15–20, 2016.

SAMPAIO, R. F.; MANCINI, M. C. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. **Brazilian Journal of Physical Therapy**, v. 11, n. 1, p. 83–89, 2007. SciELO Brasil.

SANTOS, B. P. S.; SILVA, L. A. M.; CELES, C. S. F. S.; et al. Internet das Coisas: Da Teoria à Prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. **Anais...** . p.1–50, 2016.

STEVAN, S. L. **Iot - Internet Das Coisas: FUNDAMENTOS E APLICAÇÕES EM ARDUINO E NODEMCU**. ERICA, 2018.

SURANTHA, N.; WICAKSONO, W. R. Design of smart home security system using object recognition and PIR sensor. **Procedia computer science**, v. 135, p. 465–472, 2018. Elsevier.

TURCATO, A. C. DECODIFICADOR PARA O ENCODER HT6P20B COM ARDUINO. **Blog do ACT – Programação levada a sério**, 18. jun. 2014. Blog, . Disponível em: <<https://acturcato.wordpress.com/2013/12/20/decodificador-para-o-encoder-ht6p20b-em-arduino/>>. .

WIRELESS SOLUTIONS, SIMC. SIM800L Hardware Design V1.00. , 2013. Disponível em: <<https://cdn.awsli.com.br/78/78150/arquivos/sim800l-datasheet.pdf>>. Acesso em: 3/8/2019.

## APÊNDICE A - ESTUDOS INCLUÍDOS NA REVISÃO DA LITERATURA

N.	Título	Microcontrolador	Objetivo	Sensores	Ano	Autores
1	Centralized Security System Based on IoT	Beaglebone	Sistema de segurança centralizado utilizando sensores de movimento.	Sensor de movimento PIR e sensor de temperatura.	2016	Amal Paul1, Aakash Upadhyay, Akhil Gaur, Prof. Renuka Bhandari
2	IoT Based Smart Security and Home Automation System	TI-CC3200	Sistema de segurança residencial sem fio, alertas através da internet no acionamento de eventos programados e lidos por sensores.	Sensor de movimento PIR.	2017	Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana
3	An Approach to Smart Home Security System Using Arduino	Arduíno Mega 2560	Sistema que envia vídeo e informações em tempo real utilizando tecnologia GSM. Detecção de arrombamento, incêndio e movimento. Monitoramento de temperatura, umidade.	Módulo GSM Sim900A, sensor de temperatura DHT1, sensor de movimento PIR e sensor de incêndio.	2017	Abel A. Zandamela
4	IoT Based Smart Home System Technologies	ESP8266 e Raspberry Pi	Sistema de controle residencial para ajudar deficientes e idosos a controlar e monitorar eletrodomésticos.	Sensor de temperatura DS18B20	2017	V.Jyothi1, M. Gopi Krishna, B. Raveendranadh, Debashree Rupalin
5	Smart Security for an Organization based on IoT	Arduíno Mega	Sistema de segurança residencial com controle de acesso via senha, alertas via SMS ou ligação GSM. Monitora gás, invasões através de sensores de passagem e movimento.	Modulo GSM SIM800L, sensor de movimento PIR, sensor de gás MQ2, apontador laser e foto resistor, comunicador bluetooth HC-05.	2017	Mohd. Saifuzzaman, Ashraf Hossain Khan, Nazmun Nessa Moon, Fernaz Narin Nur
6	An Advanced Internet of Thing based Security Alert System for Smart Home	Raspberry Pi	Sistema de alerta de segurança baseado em IoT para o Casa Inteligente, a fim de detectar um invasor ou qualquer evento incomum em casa.	Sensor de movimento PIR e webcam.	2017	S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, M. S. Obaidat

7	IoT Application Development: Home Security System	Raspberry Pi	Sistema de detecção de presença e reconhecimento de imagens com alertas através do Telegram.	Sensor de movimento PIR, sensor de abertura de porta e webcam.	2017	Raj G Anvekar, Rajeshwari M Banakar
8	Design of Smart Home Security System using Object Recognition and PIR Sensor	Raspberry Pi 3 e Arduíno UNO	Sistema de segurança residencial com capacidade de reconhecimento humano. Foco no processamento da imagem por algoritmos de reconhecimento.	PIR e Webcam	2018	Nico Surantha e Wingky R. Wicaksono.
9	Embodiment of IoT Based Smart Home Security System	Arduíno Mega	Sistema de segurança e monitoramento residencial de eletrodomésticos.	Módulo HC-06 bluetooth, módulo GSM SIM800C, sensor ultrassônico HC-SR04, sensor de umidade do solo, módulo laser, módulo sensor de gás combustível MQ9, sensor de movimento HC-SR501	2018	Md. Wahidur Rahman, Md. Harun-Ar-Rashid, Rahabul Islam, Dr. Mohammad Motiur Rahman
10	A Low-Cost IoT Smart Home System	Arduíno UNO	Sistema de automação residencial desenvolvimento especialmente para pessoas com deficiência visual e auditiva ou donos de animais. Foco no monitoramento da temperatura e umidade, segurança, monitoramento da saúde e segurança da vida em casa para idosos e deficientes.	Sensor DHT11, Sensor MQ-2, sensor de pulsação e sensor RFID.	2018	Man-Ching Yuen, Shin Ying Chu, Wing Hong Chu, Hoi Shuen Cheng, Ho Lam Ng, Siu Pang Yuen.
11	Smart Home Automation and Security System using Arduino and IOT	Arduíno UNO	Sistema de automação residencial com segurança, que monitora e guarda <i>status</i> de eletrodomésticos e abertura de portas.	Relê 5V, acelerômetro, sensor de incêndio, sensor de luminosidade, interruptor reed.	2018	Siddharth Wadhvani1, Uday Singh, Prakarsh Singh, Shraddha Dwivedi
12	Door Security System for Home Monitoring Based on ESP32	ESP32	Monitoramento do <i>status</i> de portas através de sensor de movimento.	PIR e sensor magnético de abertura para portas.	2019	Andreas, Cornelio Revelivan Aldawiraa, Handhika Wiratama Putraa, Novita Hanafiaha,

						Surya Surjarwoa, Aswin Wibisurya
13	Image-Based Smart Surveillance and Remote Door Lock Switching System for Homes	Raspberry Pi	Sistema de vigilância baseado em análise de fotos tiradas no acionamento de eventos por sensores. A foto é rotulada por algoritmo de reconhecimento facial.	PIR	2019	Jay Patel, Sundar Anand, Rohan Luthra
14	Design and Implementation of an IoT-Based Smart Home Security System	Raspberry Pi 2 e Elegoo Mega 2560 board	Sensor de abertura magnético econômico com alertas em aplicativo móvel Android, informando abertura de portas residenciais ou de escritórios utilizando transmissor de rádio frequência.	Transmissor rádio frequência 433 hz e sensor magnético de abertura de portas.	2019	Mohammad Asadul Hoque, Chad Davidson
15	Internet of Things Based Home Monitoring and Device Control Using Esp32	ESP32	Monitoramento remoto de temperatura, gás, nível de água em tanques. Controle de aparelhos domésticos como: luz, ventilador, motor, botão de gás.	Sensor de gás, módulo de relé, sensor de nível de água, servo motor e sensor de temperatura.	2019	V. Pravalika, Ch. Rajendra Prasad
16	Development of Smart Home System Controlled by Android Application	NodeMCU V1.0	Sistema de controle de iluminação, ventiladores e segurança utilizando IoT com aplicativo Android NETPIE, notificações através do aplicativo LINE Notify.	Sensor de movimento PIR, sensor de temperatura, câmera IP, sensor de luminosidade.	2019	Seree Khunchai, Chaiyapon Thongchaisuratkrul
17	Home Security against Human Intrusion using Raspberry Pi	Raspberry Pi	Sistema de detecção de intrusão utilizando fotos de eventos acionados por sensores.	Raspberry Pi câmera	2020	Raju A Nadafa, S.M. Hatturea, Vasudha M Bonala, Susen P Naikb

Fonte: Elaborado pelo autor (2021).

## APÊNDICE B - CUSTO DA SOLUÇÃO EM NOVEMBRO 2021

O custo dos componentes da solução foi baseado em valor de mercado em novembro de 2021, é importante ressaltar que a variação cambial e inflação afetam diretamente esses valores.

Outro ponto importante comparando com as soluções de mercado apresentadas no capítulo 2.5, **Tabela 1** - Valor médio de equipamento similar encontrado no mercado, é que as soluções presentes no mercado não contemplam todas as funcionalidades encontradas na solução desenvolvida neste trabalho. Diante disto, justifica-se o investimento maior, porém com um ganho significado de aspectos monitorados.

**Tabela 1** - Custo dos componentes microcontrolador e sensores

Componente	Valor
Microcontrolador ESP8266	R\$ 39,90
Sensor de gás e fumaça MQ-2	R\$ 19,90
Regulador de tensão LM2596	R\$ 12,90
Sensor de chama 760 a 1100 nm	R\$ 9,95
Sensor de temperatura e umidade DHT11	R\$ 13,90
Módulo GSM SIM800L EVB	R\$ 59,90
Receptor Rádio Frequência XLC-RF-5V	R\$ 19,90
Bateria 12V 7 A	R\$ 69,90
Fonte 12V 3 A	R\$ 65,00
Impressão do Circuito <sup>7</sup>	R\$ 70,00
<b>TOTAL</b>	<b>R\$ 381,25</b>

Fonte: Elaborada pelo autor (2021).

<sup>7</sup> Custo total de R\$ 700,00 para impressão de 10 unidades, quantidade mínima para fabricação.