UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM INOVAÇÕES TECNOLÓGICAS
MESTRADO EM INOVAÇÕES TECNOLÓGICAS

REGINALDO BENEDITO DE FREITAS

CONTROLE E SEGURANÇA PATRIMONIAL POR RFID NO DEPARTAMENTO ACADÊMICO DE ELETRÔNICA DA UTFPR CAMPO MOURÃO

CAMPO MOURÃO
2020

REGINALDO BENEDITO DE FREITAS

CONTROLE E SEGURANÇA PATRIMONIAL POR RFID NO DEPARTAMENTO ACADÊMICO DE ELETRÔNICA DA UTFPR CAMPO MOURÃO

Dissertação apresentada ao Curso de Pós-Graduação em Inovações Tecnológicas, Universidade Tecnológica Federal do Paraná, como parte das exigências para a obtenção do título de Mestre em Inovações Tecnológicas.

Orientador: Prof. Dr. Gilson Junior Schiavon

Coorientador: Prof. Me. Lucas Ricken Garcia

CAMPO MOURÃO

2020

Dados Internacionais de Catalogação na Publicação

Freitas, Reginaldo Benedito de

Controle e segurança patrimonial por RFID no departamento acadêmico de eletrônica da UTFPR Campo Mourão / Reginaldo Benedito de Freitas. – Campo Mourão, 2020.

1 arquivo de texto (73 f) : PDF ; 2,4 MB.

Orientador: Gilson Junior Schiavon

Coorientador: Lucas Ricken Garcia

Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná. Programa de Pós-Graduação em Inovações Tecnológicas, Campo Mourão, 2020.

Inclui bibliografia: f. 71-73

1. Radiofrequência - Identificação. 2. Microcontroladores. 3. Propriedade pública. 4. Inovações tecnológicas – Dissertações. I. Schiavon, Gilson Junior, orient. II. Garcia, Lucas Ricken. III. Universidade Tecnológica Federal do Paraná. Programa de Pós-Graduação em Inovações Tecnológicas. IV. Título.

Biblioteca da UTFPR - Câmpus Campo Mourão

Bibliotecária/Documentalista:

Andréia Del Conte de Paiva – CRB-9/1525

TERMO DE APROVAÇÃO

CONTROLE E SEGURANÇA PATRIMONIAL POR RFID NO DEPARTAMENTO ACADÊMICO DE ENGENHARIA ELETRÔNICA DA UTFPR CAMPUS CAMPO MOURÃO

Por

REGINALDO BENEDITO DE FREITAS

Essa dissertação foi apresentada às dez horas, do vinte e oito de fevereiro de 2020, como requisito parcial para a obtenção do título de Mestre em Inovações Tecnológicas, Linha de Pesquisa Desenvolvimento de Equipamentos, Tecnologias e Sistemas Eletrônicos, no Programa de Pós-Graduação em Inovações Tecnológicas - PPGIT, da Universidade Tecnológica Federal do Paraná. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Gilson Junior Schiavon (Orientador - PPGIT)

_____
Prof. Dr. Eduardo Giometti Bertogna (Membro Interno - PPGIT)

_____
Prof. Dr. Arquimedes Luciano (Membro Externo)

Dedico esta pesquisa primeiro a Deus,
por me conceder dom da vida,
minha esposa pelo amor,
paciência e força,
minha família, os amigos,
professores que me ajudaram
tornar um sonho possível e realizável.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus pela minha vida, minha inteligência, por nos dar saúde e forças para que tudo isso fosse possível, por todos os desafios que colocou em meu caminho que me fizeram crescer e desenvolver, como também por todas as vitórias que me ajudou a conquistar.

A minha querida esposa Angelita pelo amor, incentivo e principalmente paciência, que apesar das dificuldades, nunca deixou de acreditar e sempre me dar forças para superar todos os obstáculos, sempre me incentivando a crescer, pois acredito que sem ela isso não seria possível.

Ao meu orientador Prof. Gilson Junior Schiavon, que me auxiliou em todas as dificuldades que tive durante o desenvolvimento desse projeto, me incentivando, motivando e instruindo para levar o trabalho ao melhor resultado possível.

Ao co-orientador Prof. Lucas Ricken Garcia pelas suas orientações de melhorias durante o desenvolvimento do projeto, pela sabedoria com que me guiou e ajudou nesta trajetória.

A todos os professores do programa deste mestrado, pela disposição em nos transmitir conhecimento, incentivar e apoiar nos momentos mais difíceis deste trabalho, com toda certeza vocês foram o diferencial.

Pelo apoio e suporte prestado do estagiário Duane Oliveira Cicolani dos Santos, gratidão por partilhar seus conhecimentos em circuitos e programações.

Enfim, a todos aqueles que de uma forma ou outra, sem ordem de grandeza e valorização, contribuíram para a realização deste projeto.

“Diante da Sabedoria infinita, mais vale um breve desejo de humildade com algum ato da mesma, do que toda a ciência do mundo”.
(Santa Teresa de Jesus)

RESUMO

FREITAS, Reginaldo Benedito de. **Controle e Segurança Patrimonial por RFID no Departamento Acadêmico de Eletrônica da UTFPR Campo Mourão**. 2020. 73 p. Dissertação (Mestrado em Inovações Tecnológicas) - Universidade Tecnológica Federal do Paraná. Campo Mourão, 2020.

Buscando uma maior confiabilidade no controle e segurança patrimonial, empresas públicas e privadas têm investido cada vez mais em novas tecnologias, com adoção de equipamentos mais ágeis e práticos. Contribuindo com a segurança do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná (UTFPR), este trabalho apresenta o desenvolvimento de um sistema de controle de entrada e saída para o almoxarifado, de forma a monitorar equipamentos patrimoniados. Na busca de uma maior eficiência neste processo, foi proposta a criação de um sistema de segurança baseado na tecnologia RFID, no qual todos os equipamentos patrimoniados possuem uma *tag* única e são monitorados por uma antena e leitor de RFID, fazendo conexão por meio do microcontrolador ESP8266 via WiFi. De forma a tornar o trabalho independente de computadores, gerar tabelas e logs, conectado via WiFi, tornando o sistema de baixo custo e de fácil aplicabilidade. Sendo implementado com plataforma de código aberto Arduino para programação das bibliotecas em linguagem C, banco de dados MySQL gratuito, não onerando ao cofre público. Este projeto tem como finalidade principal melhorar o sistema de segurança, de forma ágil, eficaz e barata.

Palavras-chave: Controle patrimonial. Segurança. RFID. ESP8266. Biblioteca em C.

ABSTRACT

FREITAS, Reginaldo Benedito de. **Control and Security Patrimonial by RFID in the Academic Department of Electronic Engineering to the UTFPR Campo Mourão**. 2020. 73 p. Dissertation (Master in Inovation Technologics) - Federal Technology University to the Paraná. Campo Mourão, 2020.

Seeking greater reliability in the control and security of assets, public and private companies have increasingly invested in new technologies, with the adoption of more agile and practical equipment. Contributing to the security of the Academic Department of Electronics at Universidade Tecnológica Federal do Paraná (UTFPR), this work presents the development of an entry and exit control system for the warehouse, in order to monitor heritage equipment. In the search for greater efficiency in this process, it was proposed to create a security system based on RFID technology, in which all heritage equipment has a unique tag and is monitored by an antenna and RFID reader, making a connection through the microcontroller ESP8266 via WiFi. In order to make the work independent of computers, generate tables and logs, connected via WiFi, making the system low cost and easy to apply. Being implemented with an open source Arduino platform for programming the libraries in C language, a free MySQL database, not burdening the public safe. This project's main purpose is to improve the security system, in an agile, effective and inexpensive way.

Keywords: Control patrimonial. Security. RFID. ESP8266. Libraries in C.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ANSI	*American National Standards Institute* (Instituto Nacional Americano de Padrões)
CM	Campo Mourão
DAELN	Departamento Acadêmico de Eletrônica
DER	Diagrama Entidade Relacionamento
DIN	*Deutsches Institut fur Normung* (Instituto Alemão de Normatização)
EEPROM	*Electrically-Erasable Programmable Read-Only Memory* (Memória Somente de Leitura Programável Apagável Eletricamente)
EUA	Estados Unidos da América
EPC	*Electronic Product Code* (Código Eletrônico do Produto)
GPIO	*General Purpose Input Output* (Portas Programáveis de Entrada e Saída de Dados)
HF	*High Frequency* (Alta Frequência)
HTML	*Hypertext Markup Language* (Linguagem de Marcação de Hipertexto)
IDE	*Integrated Development Environment* (Ambiente de Desenvolvimento Integrado)
IP	*Internet Protocol* (Protocolo de Internet)
ISO	*International Organization for Standartization* (Organização Internacional de Normalização)
I2C	Protocolo de Comunicação Serial por dois fios
LF	*Low Frequency* (Baixa Frequência)
MYSQL	Banco de Dados com Linguagem de Consulta Estruturada
RFID	*Radio Frequency Identification* (Identificação por Rádio Frequência)
SGBD	Sistema de Gerenciamento de Bando de Dados
SPI	*Serial Peripheral Interface* (Interface Periférica Serial)
SQL	*Structured Query Language* (Linguagem de Consulta Estruturada)
TAG	Etiqueta
UART	*Universal Assynchronous Receiver/Transmitter* (Receptor / Transmissor Assíncrono Universal)
UHF	*Ultra High Frequency* (Ultra Alta Frequência)

URL	*Uniform Resource Locator* (Localizador Padrão de Recursos)
USB	*Universal Serial Bus* (Barramento Serial Universal)
UTFPR	Universidade Tecnológica Federal do Paraná
WEB	*World Wide Web* (Rede Mundial de Computadores)
WIFI	*Wireless Fidelity* (Rede Sem Fio)

SUMÁRIO

1 INTRODUÇÃO

O controle patrimonial é uma forma de controle interno dentro de qualquer instituição pública ou privada; assim como na Universidade Tecnológica Federal do Paraná (UTFPR). Geralmente é efetuado para assegurar a existência de informações corretas sobre a localização física dos equipamentos, agente responsável, movimentações, estado de conservação, histórico de circulação, e ainda por ocasião da baixa patrimonial de um determinado bem.

Desde os tempos mais remotos, o ser humano sente a necessidade de identificar-se e controlar seus bens. A busca por novas tecnologias, e novas formas de resolver os problemas atuais, reflete em nosso cotidiano mudando totalmente nossos costumes e práticas habituais.

São constantes os fatos noticiados em mídias especializadas, acerca da inadequada gestão do patrimônio público, no qual os bens móveis prematuramente tornam-se inúteis, ou ainda são extraviados por falta de controle. Quando não identificados os responsáveis pelo dano causado, resta o ônus para toda a sociedade.

Por mais que exista a preocupação e a dedicação por parte da maioria dos servidores que atuam sobre o controle patrimonial, procedimentos realizados de maneira aleatória em decorrência da inexistência de padronização e, ainda o não emprego de tecnologias, acabam por prejudicar a realização de um controle patrimonial fidedigno.

Avanços ocorreram nos sistemas de informações patrimoniais, que caminharam desde a simples digitação, passando pelos códigos de barras e leitores 3D, até as atuais etiquetas eletrônicas de identificação por radiofrequência. Sendo que essas tecnologias proporcionam um elevado grau de integração e segurança, na medida em que possibilitam a atualização das informações em tempo real, gerando ainda o desenvolvimento de maiores aplicações em sistemas de identificação baseados na transmissão por radiofrequência.

A implantação desta tecnologia em etiquetas eletrônicas, apresenta um diferencial tecnológico, pois ela depende de processos que estão acontecendo em nosso meio físico e facilitando seu uso, devido à mesma ser integrada ao sistema

atual da instituição, ou seja, aproveitando informações já existentes nos bancos de dados.

Em relação às tecnologias empregadas na identificação e controle patrimonial, com base em pesquisas bibliográficas foram identificados três tipos principais**:** plaquetas numéricas, plaquetas com códigos de barras e etiquetas com RFID.

Como forma de contribuir, esta pesquisa tem como objetivo principal analisar o controle patrimonial dos bens permanentes dentro do almoxarifado do curso de Engenharia Eletrônica da Universidade Tecnológica Federal do Paraná Campo Mourão (UTFPR-CM); pois possui um vasto rol de equipamentos em seu almoxarifado, deixando assim muito difícil o controle dos equipamentos emprestados a alunos e pesquisadores, utilizando controle manual pelo preenchimento de anotações e planilhas.

A contribuição deste trabalho está na criação da metodologia de integração entre a tecnologia de identificação por radiofrequência (RFID) e o sistema utilizado até o momento, ou seja, criar um sistema de segurança patrimonial, no qual quaisquer equipamentos patrimoniados com etiquetas RFID, que saiam e passem pela porta do almoxarifado sejam lidos e reconhecidos por este sistema de controle. Gerar histórico com dia, horário e tipo do bem que saiu do local em que estava armazenado, tendo assim por consequência uma menor intervenção humana e uma maior confiabilidade nos equipamentos existentes no almoxarifado.

Partindo destas informações, conseguimos controlar e tentar localizar o bem patrimoniado e etiquetado que saiu do almoxarifado do Departamento Acadêmico de Eletrônica (DAELN) em tempo real, pois esta sala e corredores de acesso dispõem de câmeras de segurança.

Para conseguir efetuar a localização destes bens, utilizou-se o dispositivo ESP8266 que faz uso da rede WiFi disponível na instituição, mais um sistema de antena para leitura das etiquetas RFID compatível com frequência utilizada pelas etiquetas RFID, além de um sistema para a leitura e gerenciamento de todo processo.

1.1 Objetivo

1.1.1 Objetivo Geral

O objetivo geral deste trabalho é desenvolver um sistema de segurança dos equipamentos patrimoniados dentro do almoxarifado DAELN, utilizando um sistema para identificar os equipamentos por meio do uso da etiqueta eletrônica RFID, no qual dados como: responsáveis e características do bem são armazenados em um banco de dados vinculados a uma etiqueta RFID, monitorando entrada e saída destes, aumentando a segurança e localização dos bens em circulação em qualquer horário, através da vinculação dos horários de saída juntamente as imagens gravadas no circuito interno de câmeras presente na UTFPR Campo Mourão.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Vincular aos equipamentos patrimoniados uma *tag* RFID;
- Desenvolver uma interação entre o leitor RFID, ESP8266 e o banco de dados, por meio da rede WiFi;
- Criar/simular portal com leitor RFID dimensionado de forma a ler a *tag* que entre ou saia do almoxarifado DAELN;
- Criar banco de dados para o cadastramento, controle de entrada/saída e, responsável pelo bem patrimonial em circulação;
- Gerar *log* sobre entrada/saída a fim de facilitar o controle e o inventário anual;
- Criar uma interface *web* sistema-usuário de fácil uso e compreensão, para obtenção de relatórios em tempo real.

1.2 Justificativa

O interesse pelo assunto surgiu com a participação como membro da comissão de inventário patrimonial da UTFPR campus Campo Mourão, no qual tive

o primeiro contato com o controle patrimonial e, principalmente, a vivência das adversidades peculiares à função de servidor público.

Com a admissão no Mestrado Profissional em Inovações Tecnológicas da UTFPR-CM, ficou mais evidente a necessidade do debate acerca do tema sobre controle patrimonial na universidade, principalmente pela facilidade do rastreio dos bens patrimoniados em meu nome e dos demais servidores.

As experiências pessoais, tanto no serviço público quanto no privado, possibilitaram a conclusão de que organizações públicas possuem vários desafios acerca do controle patrimonial, como por exemplo, a existência de informações desatualizadas, ausência de identificação dos bens, movimentações irregulares, segurança e principalmente, não localização dos bens nos inventários realizados anualmente pelos servidores responsáveis pela área de patrimônios.

Considera-se que os resultados obtidos com esta pesquisa, poderão contribuir para o aumento dos conhecimentos sobre o controle do patrimônio público, consolidação das boas práticas de controle e, poderão ser considerados pela instituição ao aperfeiçoamento de sua gestão, por meio de relatórios mais precisos e confiáveis.

O levantamento de patrimônio possui uma dinâmica difícil quando se utiliza os sistemas atuais, tais como: numeração para leitura visual ou códigos de barras, processo de leitura demorado, exigindo uma equipe de pessoas destacadas para que esta tarefa seja feita com agilidade, onerando os recursos da instituição em questão, podendo ainda ocorrer o descolamento das etiquetas de código de barras nos equipamentos ou bens móveis.

O controle de patrimônio (controle de bens móveis) exige uma supervisão permanente e nem sempre é possível fazê-la com eficácia, sendo sua conferência feita com base em planilhas e relatórios, que muitas vezes se tornam confusas para entendimento e leitura, são impressos e podem causar uma curva de erro em todo o processo executado.

Levando-se em conta todos estes fatores, surgiu a proposta de desenvolver uma solução de controle e segurança de equipamentos e mobiliário, que atenda adequadamente as necessidades, utilizando tecnologia RFID, trazendo agilidade e eficácia ao processo. Além disso, contando com leitura instantânea dos equipamentos por meio de sistema de informações e antena para captura dos dados

colocados nos equipamentos patrimoniados, quando estes saírem da sala do almoxarifado DAELN.

Com o sistema aqui proposto, torna-se mais fácil e rápida a emissão de relatório dos equipamentos que constam na sala do almoxarifado DAELN, uma vez que este sistema faz a leitura de entrada/saída em tempo real, além de proporcionar segurança dos dados inseridos no sistema de patrimônio.

Partindo-se da implantação deste sistema de segurança, não teremos mais a necessidade de conferência anual de todos os equipamentos patrimoniados e etiquetados constados nas salas, pois a qualquer momento pode-se emitir relatório e detectar a falta de tais equipamentos.

Constatando-se a falta de alguns equipamentos, podemos rastreá-los por meio das câmeras espalhadas por todo o perímetro da universidade, pois o sistema emitirá alerta e gerará um *log* de entrada/saída destes equipamentos etiquetados.

Tendo em vista a instalação deste sistema de segurança em RFID no almoxarifado DAELN, podemos implementar em quaisquer salas ou departamentos, pois trabalha com rede WiFi, enviando informações online sobre todo o processo, por se tratar de um sistema com mobilidade, baixo custo e de fácil implementação.

1.3 Organização da Dissertação

Após a introdução feita neste Capítulo 1, serão apresentados no Capítulo 2 os fundamentos básicos e teóricos da tecnologia RFID, bem como os principais componentes necessários para um sistema de controle e segurança patrimonial, detalhando as características, especificidades de cada um e ainda algumas aplicações de RFID.

No Capítulo 3, serão apresentadas uma introdução aos materiais e metodologia adotados, tipo de pesquisa escolhida, etapas desenvolvidas para a escolha dos componentes, módulos mais adequados para este projeto, configuração, desenvolvimento da aplicação e a implementação do banco de dados.

No Capítulo 4 serão descritos os resultados do desenvolvimento do projeto, dados obtidos, testes e simulações.

As considerações finais deste trabalho serão apresentadas no Capítulo 5, assim como perspectivas para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Controle Patrimonial

Com o uso cada vez mais comum da tecnologia e acessos à internet, fica evidenciada a facilidade em controlar os equipamentos nas empresas e instituições públicas, principalmente quando se trata de controle de estoque e fluxo de ferramentas, facilitando o controle de entrada e saída nos almoxarifados.

De acordo com Ballou (1993), um dos fatores mais relevantes ao desenvolvimento dos processos administrativos é a aplicação de tecnologia de informação, proporcionando um grande aumento em sua eficiência. Tais sistemas abrangem todas as ferramentas que a tecnologia disponibiliza para o controle e gerenciamento do fluxo de informação de uma organização.

Para Santos (2010), o controle patrimonial é uma das funções da administração de recursos patrimoniais, o qual compreende uma sequência de atividades que iniciam com a aquisição, terminando com a retirada ou alienação do bem do patrimônio.

De acordo com Torres Júnior e Silva (2003), a proteção e segurança destes bens patrimoniados, é dever de todos e abrange um aspecto que transcende o presente, servindo de garantia para que as próximas gerações tenham um ambiente saudável.

O patrimônio público não é propriedade dos ocupantes de cargos ou funções públicas, mas sim, da coletividade. Desta forma, seu uso deverá atender ao interesse público e à concretização do bem comum.

A importância dos mecanismos de controle pode ser mais compreendida por meio de vários métodos ou estudos, nos quais demonstram que busquem os objetivos de todos os cidadãos brasileiros.

Para Brady Jr. (2001), a tecnologia baseada no sistema de plaquetas ou chapas numéricas de identificação, consiste na atribuição de um número de tombo que vincula o bem ao sistema patrimonial. As plaquetas numéricas visam registrar o número do tombo e identificar que determinado bem faz parte do patrimônio de uma organização, além dos números são postos símbolos, siglas ou outra forma de identificação institucional.

Ainda, segundo Brady Jr. (2001), o controle patrimonial por plaquetas, consiste na identificação manual dos bens por meio do contato visual com o número de tombo e a conferência com os relatórios gerenciais, sendo a interligação entre o bem e o sistema de controle realizado por intermédio da ação humana.

2.2 RFID

A identificação por radiofrequência (RFID) está fundamentada nas descobertas da indução mútua ou eletromagnética de Faraday e, no advento das transmissões por rádio e por radar. A tecnologia RFID surgiu nos campos de batalha da primeira guerra mundial, por aviões de metal que se tornaram capazes de levar milhares de quilogramas de explosivos, viajando a centenas de quilômetros por hora, sem serem identificados. Começou-se então uma forma de tentar identificar aviões amigos e inimigos, pois muitas vezes apenas descobrindo a presença destes, não os impediriam de serem atacados, conforme Santini (2008).

A partir desta identificação, cada avião dispunha de transmissores com frequências únicas, capazes de enviar e receber dados, sem enganar os radares, com esse mesmo princípio a tecnologia RFID funciona, ou seja, identificação única de cada dispositivo ou etiqueta RFID.

Uma das formas para facilitarmos a identificação de equipamentos é a RFID, sendo uma tecnologia que, por meio de ondas de rádio frequência, permite que dados sejam armazenados e recuperados em um circuito integrado (*chip*). A RFID tem como objetivo básico viabilizar a captura automática de características e identidade de objetos (veículos, documentos, caixas, paletes, produtos), animais e até pessoas, existindo ainda um grande número de sistemas que são implementados utilizando RFID.

Segundo Bernardo (2004), a RFID não é simplesmente um substituto do código de barras, é uma tecnologia de transformação que pode ajudar a reduzir desperdício, limitar roubos, gerir inventários, simplificar a logística, aumentar a produtividade e, ainda prover segurança para a instituição ou empresa privada, mas também traz a desvantagem do custo dos sistemas, regulamentações nacionais e internacionais incompatíveis e ainda a interferência eletromagnética no uso de

materiais metálicos ou condutivos, dificultando a transmissão dos sinais de radiofrequência.

Basicamente a tecnologia RFID, segundo Santini (2008), consiste numa comunicação por radiofrequência sem fios, para transmitir dados a um dispositivo móvel, este podendo ser uma etiqueta ou um chaveiro, sendo chamados simplesmente de *tags*, contendo estes componentes uma antena e um *chip* envoltos por algum material, como vidro ou plástico, os quais respondem a sinais remotos de um leitor conectado a um computador.

Segundo Taufenbach (2004), a tecnologia de identificação por meio da rádio frequência RFID, vem sendo usada em identificação de objetos desde 1969 e patenteada em 1973, mas somente a partir de 2004 está se tornando comercialmente e tecnologicamente viáveis.

De acordo com Matsubayashi (2004), a RFID é a tecnologia que permite identificação por rádio frequência, ou seja, permite a leitura sem contato visual direto. Afirma ainda o autor que essa nova tecnologia será rotina, tendo impacto direto no cotidiano das pessoas e nos processos logísticos de toda cadeia de abastecimento.

Para Nogueira (2005), a tecnologia RFID apresenta características peculiares que nenhuma outra oferece. Por exemplo, leitura simultânea de até 30 itens num período de um segundo, utilizando-se de poderosos algoritmos de anti-colisão. Com isto podem-se realizar inventários de milhares de itens, utilizando um leitor de RFID manual.

De acordo com Pressman (2016), as RFID’s trazem a computação para uma base industrial e para o ramo de produtos de consumo. A tecnologia da informação vem auxiliando as indústrias, o planejamento de uma empresa no sentido de aumentar a produtividade e os lucros.

Segundo Moura (2013), quanto à percepção de como se deve utilizar a RFID, chegou-se a conclusão que a convergência era a melhor saída, juntamente com aplicação desta tecnologia em circuitos fechados controlados por uma empresa, especialmente o fabricante. Atualmente, a etiqueta eletrônica pode ser associada a gerenciamento de ativos, associações de dados coletados por sensores ou pode ser associada a um banco de dados.

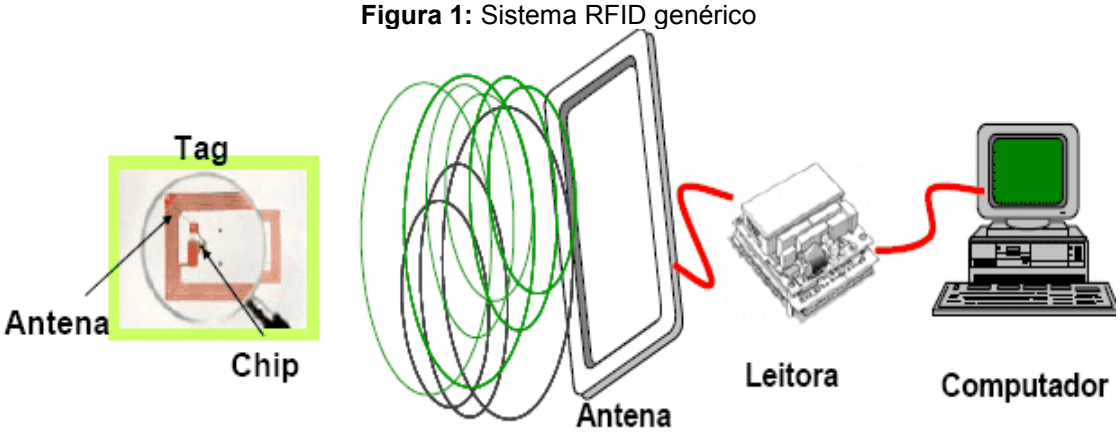
Segundo Santana (2018), a tecnologia RFID permite a captura automática de dados, para identificação de objetos com dispositivos eletrônicos, conhecidos como *tag* ou *transponder* que emitem sinais de radiofrequência para leitores ou antenas, que captam estas informações com alta velocidade e segurança.

De acordo com Finkenzeller (2010), todo sistema de captura de dados por RFID possui o seguinte conjunto de componentes:

- Leitores/gravadores;
- Antenas;
- Etiquetas RFID;
- *Software* para gerenciamento do sistema de leitura;
- Infraestrutura de instalação.

Segue figura 1 referenciando sobre um sistema RFID genérico.

Figura 1: Sistema RFID genérico



Fonte: Retirado do site embarcados.com (2020)

2.3 Etiqueta RFID (*tag*)

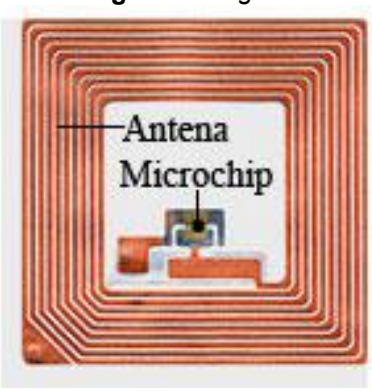
Segundo Dresch Jr. (2008), as etiquetas RFID propiciam a automatização de processos, a desmaterialização de operações e a consequente redução na necessidade de emprego de trabalho manual, o que elimina os erros advindos de falha humana. Também, o fato das ondas de radiofrequência ter acesso a qualquer ambiente, permite que bens situados em recintos de difícil acesso sejam identificados e que a situação patrimonial real seja apresentada nos inventários.

A palavra *transponder* é um acrônimo de *TRANSmite/resPONDER,* em que sua função é transmitir e responder comandos recebidos por radiofrequência, sendo *transponder*, RF *tag* ou simplesmente *tag* a etiqueta RFID.

As *tags* RFID podem estar apresentadas nas mais diversas formas, serem colocadas ou acopladas a rótulos de papel, cartões plásticos, cápsulas de vidro, pulseiras, relógios, animais e em seres humanos. A escolha correta do material e formato é de fundamental importância na aplicação, pois vários fatores podem influenciar tais como: durabilidade, resistência e intempéries.

Segundo Santini (2008), a estrutura básica de uma *tag* é bem simples, sendo um *chip* capaz de armazenar informações e ter uma resistência para fazer o papel de antena, envoltos por um material como plástico ou silicone, sendo que seu principal propósito é de fisicamente anexar dados sobre um determinado objeto, segue figura 2 como exemplo desta *tag*.

Figura 2: *Tag* RFID



Fonte: Retirado do site electrosome.com (2020)

Com relação a sua fonte de energia, RFID JOURNAL (2013) classifica as *tags* em:

1. Passivas: não possuem fonte de energia ou bateria. A energia necessária ao seu funcionamento é recebida do leitor por meio dos sinais emitidos por este. Em virtude desta característica, são mais baratas e têm uma maior duração em comparação as *tags* ativas. Contudo, possuem capacidade computacional e memória limitadas, são aquelas que quando passam dentro de uma zona eletromagnética gerada pelo leitor RFID, são detectados, lidos e decodificados os dados que estão armazenados em sua memória, passando-o para um computador realizar o processamento.

Segue exemplo com tipos de *tags* passivas encontradas no mercado na figura 3.

Figura 3: Tipos de *tags* passivas

Fonte: Retirado do site ravirajtech.com (2020)

2. Semi-passivas ou semi-ativas: possuem bateria interna, porém utiliza a energia fornecida pelos leitores para transmitir o sinal a estes, como ocorre com as *tag*s passivas. Neste caso, a bateria fornece energia ao seu *microchip*, permitindo que este tenha uma maior capacidade de processamento.
3. Ativas: possuem fonte de energia interna, o que possibilita o envio de sinais de transmissão de dados ao leitor, bem como alimentar circuitos mais complexos e sensores (acelerômetros para detectar movimento, temperatura, umidade e outros). Este tipo de *tag* possui um valor comercial mais alto, também um tempo de duração menor em comparação as *tag*s passivas, pois baterias descarregam com o tempo, gerando uma manutenção maior em comparação com as demais *tag*s. Segue exemplo com tipos de *tag*s ativas encontradas no mercado na figura 4, sendo citado o caso da empresa SEMPARAR com atuação na concessão de pedágios rodoviários.

Figura 4: Tipo de *tag* ativa

Fonte: Retirado do site semparar.com.br (2020)

2.4 Antena e Leitor de RFID

A antena no sistema RFID, tem como principal função transformar a energia eletromagnética guiada pela linha de transmissão em energia eletromagnética irradiada e vice-versa, ou seja, receber também. O tipo e modelo de antena utilizada são fatores determinantes para o alcance das *tag*s, tal qual seu funcionamento e tipo de sistema utilizado.

Segundo Dobkin (2008), antenas do ponto de vista de transmissão, são estruturas especialmente arranjadas para criar ondas eletromagnéticas a partir de tensões e correntes elétricas que não se cancelam, sendo os principais parâmetros: padrão de irradiação, diretividade, impedância, ganho, largura de banda, abertura efetiva e polarização.

A antena emite um sinal de rádio que ativa a *tag,* fazendo a escrita ou leitura dos dados, que depois de lidos são enviados ao sistema, sendo esta emissão de ondas de rádio irradiada em várias direções, sentidos e distâncias, dependendo da frequência e potência utilizada, pois o tempo de exposição da *tag* é bem pequeno.

Todo e qualquer sistema de RFID possui pelo menos duas antenas, uma na etiqueta e outra no leitor, seu estilo e posicionamento são fatores que alteram sua área de cobertura, seu alcance e ainda sua precisão na comunicação. Elas operam sob os mesmos princípios, mas os desafios práticos entre elas são bastante distintos, relacionados principalmente com custo e tamanho.

Os modelos para antena e leitor, podem ser de vários tipos, tais como: túnel, portal, portátil, entre outras, sendo definidos pelo tipo de aplicação em que será utilizado o sistema RFID.

Devido a grande quantidade de antenas existentes no mercado, dependendo de vários fatores e também da frequência de operação, se faz necessário conhecer as principais grandezas físicas que as caracterizam e influenciam no comportamento do sistema, sendo estas grandezas: polarização, diretividade e ganho.

Entre os tipos de antenas que mais se destacam, quanto à polarização segundo RFID JOURNAL (2013) são:

1. Linearmente polarizada: antena que concentra a energia de rádio do leitor numa orientação ou polaridade, aumentando assim a distância de leitura possível e proporcionando maior penetração em materiais densos. Etiquetas projetadas para este uso devem estar alinhadas com antena leitor para serem lidas.
2. Circularmente polarizada: antena leitora UHF que emite ondas de rádio em padrão circular, são usadas em situações que a orientação das etiquetas para o leitor não podem ser controladas, uma vez que as ondas estão se movendo em padrão circular, elas tem melhor chance de acertar a antena, mas em contrapartida possui um alcance de leitura mais curto do que antenas polarizadas linearmente.

Para Brown (2006), a diretividade é a característica física da antena que define a direção de propagação do sinal de radiofrequência ou RF emitido pela mesma, por meio desta análise é definida a área de cobertura das antenas. Podendo assim as antenas ser classificadas da seguinte forma:

1. Antenas diretivas: são aquelas em que o campo de RF é propagado em um feixe bem restrito, com maior intensidade em uma direção do que em outra, delimitando uma pequena área, *tag* e antena em posições definidas e sem alteração desta posição;
2. Antenas omnidirecionais: são aquelas em que o campo de RF tem propagação em 360 graus em relação à antena, ou seja, sinal RF propagado em todas as direções, diminuindo assim sua intensidade e

facilidade de instalação, *tag* e antena em qualquer posição, mas com distâncias reduzidas entre elas;

3. Antena painel: aquela utilizada pela grande maioria de sistemas RFID, propagam sinal de RF com ação do campo em aproximadamente 160 graus, usada em montagem de portais.

Conforme Kim (2005), ganho é o nível de amplificação do sinal que uma antena acrescenta no leitor de RFID, fazendo o sinal de RF alcançar a *tag* com nível suficiente para atender as necessidades do sistema, quanto maior o ganho maior será a intensidade de energia que alimenta a *tag*, aumentando assim a distância de identificação da mesma. A unidade de medida para o ganho é o decibel (db), e antenas mais comuns para aplicações RFID estão em torno de 6 decibéis de ganho.

O sistema RFID se dá quando há transmissão de informação, energia ou em ambos por meio da indução magnética ou campo eletromagnético.

Para Santini (2008), um leitor num sistema RFID tem como verificação de desempenho, o fato de se comunicar com as *tags* pela antena e repassar a informação para o *software* implementado.

Segundo Taufenbach (2004), o leitor de radiofrequência cria um campo magnético que aciona a *tag*. As *tags* RFID são *chips* com capacidade para armazenarem informações que podem ser lidas dentro do campo magnético provido pelos leitores RFID.

Para Finkenzeller (2010), operações de leitura e escrita na *tag* são executadas usando o princípio mestre-escravo, sendo que a leitora assume o papel de mestre e a *tag* apenas responde aos comandos da leitora.

De acordo com Pinheiro (2004), o leitor RFID não precisa de campo visual para realizar a leitura da *tag*. Essa leitura pode ser feita por meio de diversos materiais como plásticos, madeira, vidro, papel, cimento. Esse campo magnético precisa ser forte o bastante para englobar a *tag*.

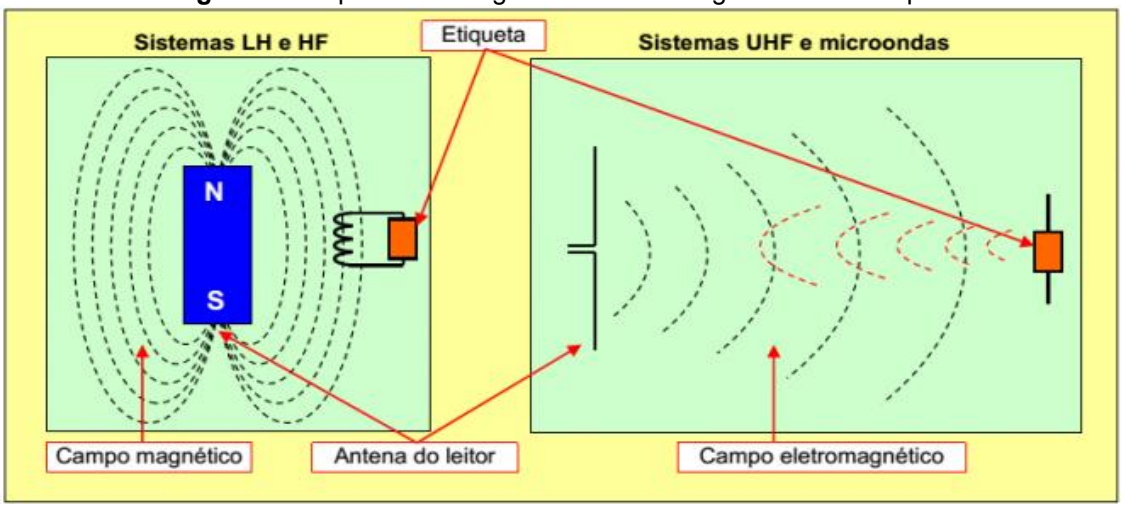
Segundo Want (2006), a leitura de uma etiqueta RFID pode funcionar de duas formas: indução magnética e radiação eletromagnética. Ambas as formas de leitura usam propriedades eletromagnéticas associadas a uma antena de radiofrequência, podendo transferir energia suficiente para que a etiqueta possa executar sua função.

Na indução magnética, o leitor é responsável por gerar um campo magnético por meio da bobina de detecção, fornecendo ainda toda energia necessária para o correto funcionamento do *chip*. Caso uma etiqueta esteja ao alcance deste campo, ou seja, dentro da área de cobertura do leitor, uma tensão alternada irá aparecer em sua bobina, que será retificada e alimentará o *chip*, enviando seu ID para o leitor, sendo pequeno o alcance da leitura, a frequência de operação será baixa.

A radiação eletromagnética possui campo magnético e campo elétrico que se propagam por meio do espaço, e é propagada por uma antena dipolo que está conectada ao leitor. Uma antena dipolo presente na etiqueta recebe esta propagação como uma diferença de potencial alternado, aumentando por consequência o alcance e trabalhando com frequências maiores de operação.

Para facilitar e realçar o funcionamento dos campos magnéticos e eletromagnéticos na etiqueta RFID mostramos na figura 5.

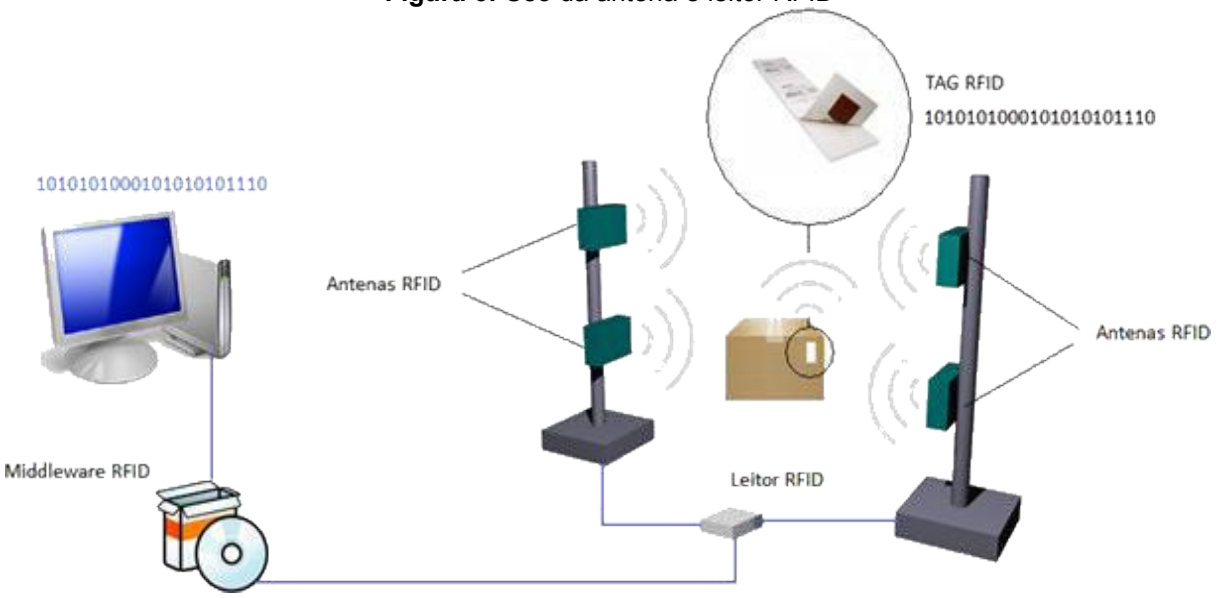
Figura 5: Acoplamento magnético e eletromagnético dos campos



Fonte: Retirado do site embarcados.com (2020)

Em ambas as formas, ressaltando que não se trata de campos estáticos e sim oscilantes, a tensão que é induzida na etiqueta é retificada e acoplada a um capacitor, gerando um reservatório de cargas suficiente para alimentar o *chip* da etiqueta. Quando alimentada, a etiqueta transmite os dados para o leitor, que faz o processamento destes dados. Após a transmissão e o processamento dos dados, é possível, por meio do sistema computacional, identificar cada etiqueta individualmente, pois cada etiqueta tem um número único, segue como forma ilustrativa do processo de leitura da etiqueta a figura 6.

Figura 6: Uso da antena e leitor RFID



Fonte: Retirado do site roisoft.com.br (2020)

2.5 Frequências de Operação RFID

Como faz uso de ondas eletromagnéticas, o sistema ainda é classificado como dispositivo de radiotransmissor, assim segundo a legislação de cada país, não pode interferir em faixas de serviços de emergência ou de transmissão de televisão. As aplicações em RFID estão restritas ao seu uso apenas em escalas de frequências que foram reservadas especificamente para aplicações industriais, cientificas ou médicas, ou ainda para dispositivos de curto alcance, no qual a forma de transmissão do sinal de RFID é particular para cada faixa de frequência, implicando equipamentos distintos para as diferentes faixas.

Conforme Finkenzeller (2010), a frequência de operação é a frequência eletromagnética utilizada para comunicação e obtenção da alimentação pelas etiquetas. Atualmente existem quatro faixas de frequência nos sistemas em RFID. Elas são divididas em baixa frequência (LF) usadas para identificação de animais e rebanhos, alta frequência (HF) usadas em lojas de departamentos em sistemas antifurto, ultra alta frequência (UHF) usadas em processos logísticos e micro-ondas usadas em aplicações industriais, científicas e médicas. Com relação à faixa de frequência em que operam Finkenzeller (2010) e RFID JOURNAL (2013), classificam os sistemas RFID em:

1. Baixa Frequência (LF – *Low Frequency*): atuam numa frequência de 30 a 300 kHz, e possuem uma transferência de dados bem lenta, assim como um pequeno alcance de leitura (até 1 metro). Vide exemplo de *tag* baixa frequência figura 7.

Figura 7: *Tag* baixa frequência

Fonte: Retirado do site afixgraf.com (2020)

2. Alta Frequência (HF – *High Frequency*): atuam numa frequência na faixa de 3 a 30 MHz, geralmente podem ser lidas até 1 metro de distância, e possuem transmissão de dados mais rápida que as *tag*s de baixa frequência, mas também consomem mais energia do que estas. Vide exemplo de *tag* alta frequência figura 8.

Figura 8: *Tag* alta frequência

Fonte: Retirado do site afixgraf.com (2020)

3. Ultra Alta Frequência (UHF – *Ultra High Frequency*): atuam numa faixa de frequência de 300 MHz a 3 GHz, e tipicamente operam entre 866 e 960 MHz. *Tag*s UHF possuem taxas de transferência mais altas e maior alcance do que as *tag*s de alta e baixa frequência. No entanto, as ondas de rádio, nesta frequência, não passam por itens com alto teor de água. Em comparação às *tag*s de baixa frequência, as *tag*s UHF são mais caras e utilizam mais energia. Vide exemplo de *tag* ultra alta frequência figura 9.

Figura 9: *Tag* ultra alta frequência

Fonte: Retirado do site afixgraf.com (2020)

4. Micro-ondas: atuam numa frequência acima de 3 GHz. *Tags* micro-ondas têm taxas de transferência muito altas e podem ser lidas a longas distâncias, contudo, elas usam uma grande quantidade de energia e são mais caras em comparação as demais, exemplo típico de uso seriam os pedágios.

Para haver comunicação entre *tag*s, leitores e servidor RFID é necessária utilização de protocolos, nos quais se definem regras de como esta comunicação acontecerá. Tais regras definem, dentre outras questões, quais sinais são reconhecidos, como a comunicação se dará, qual o significado dos dados recebidos das *tags* e quais dispositivos podem transmitir a cada tempo (resolvendo problemas de colisão entre diversas *tags* lidas).

Para Finkenzeller (2010), baixas frequências são melhores em situações de uso das *tags* em que precisam ser lidas por meio de materiais que tenham líquidos ou partes metálicas, pois aumentando a frequência de uso, as ondas de rádio passam a ter um comportamento semelhante ao da luz, ou seja, elas não passam com facilidade por certos materiais e ainda são refletidas por outros.

Ainda conforme Finkenzeller (2010), aumentando a frequência de operação, também aumentaremos a tensão induzida na etiqueta, isto implica dizer que sistemas com maior frequência de operação, tendem a ter uma maior eficiência e alcance na transmissão dos dados.

A segurança dos sistemas que utilizam RFID engloba uma série de quesitos relacionados à proteção dos dados contidos nas *tags* e, disponibilidade dos serviços aos quais se destinam a identificação por elas fornecida. Além do número de identificação, as *tags* podem armazenar outros dados relacionados ao departamento, por exemplo, ou ao tipo que ela se destina. Estes dados podem

comprometer a segurança dos processos envolvidos, bem como comprometer a privacidade das pessoas, para tal alguns procedimentos devem ser adotados. Todo sistema de transação precisa ter segurança, desde o tráfego de dados até a integridade dos mesmos.

A tecnologia RFID, quando desenvolvida de forma proprietária, faz com que essas regras sejam distintas a cada fabricante, inibindo a sua expansão e uso, visto que produtos de diferentes fabricantes não poderiam se comunicar entre si. Por isso, é importante uma padronização, para que sistemas e equipamentos diferentes sejam compatíveis, diminuindo custo e ainda facilitando sua implantação. Neste quesito, duas organizações se destacam: *International Standards Organization* (ISO) e a *Electronic Product Code global* (EPCglobal).

Segundo Finkenzeller (2010), a ISO é uma união mundial de instituições nacionais de normalização, tais como DIN (Alemanha) e ANSI (EUA), contribuindo com inúmeros comitês e grupos de trabalho para o desenvolvimento de padrões de RFID. Dentre os padrões ISO podem-se citar os de baixa frequência, utilizado no rastreamento de animais (ISO 11784, ISO 11785, ISO 14223), os de alta frequência utilizados em cartões inteligentes (ISO 10536, ISO 14443, ISO 15693) e os da série ISO 18000, utilizados no gerenciamento de itens, dentre os quais atuam em diferentes frequências.

Ainda conforme Finkenzeller (2010), a EPCglobal é uma organização sem fins lucrativos que visa à padronização da RFID por meio do Código Eletrônico de Produto (EPC - *Electronic Product Code*) e da EPC *Network*. O EPC é um meio para identificar de forma única paletes, caixas ou itens, sendo que uma *tag* EPC não carrega informações pessoais, servindo apenas para rastrear o objeto e não para manuseá-lo. Todas as informações sobre o objeto com a *tag* EPC é administrada exclusivamente no EPCglobal *Network*, sendo que esta tecnologia permite parceiros comerciais documentar e determinar a localização de bens individuais na cadeia de abastecimento em tempo real. O EPC possui identificador global e único, sendo que as etiquetas podem ser confeccionadas em todos os tamanhos e formatos. Sendo utilizado para este projeto apenas etiquetas EPC Classe 0, na qual será efetuado apenas leitura das mesmas e não gravação, pois já vem programadas com número único de fábrica.

Segundo Glover & Bhatt (2007), as etiquetas possuem classes de identificadores EPCglobal, sendo divididas desta forma:

- Classe 0, sendo passivas e apenas para leitura, sendo os tipos mais simples, contêm apenas um número de série e não tem memória no *chip*;
- Classe I, sendo passiva e grava uma vez, tornando mais completa, vem programada de fábrica ou permite anexar dados, por exemplo, nome de um computador;
- Classe II, sendo passiva e permite a gravação de dados a qualquer momento, sendo o tipo mais flexível, pois durante um processo de produção permite agregar várias informações até o término ou montagem de um equipamento, facilitando levantar um histórico do mesmo;
- Classe III, sendo regravável, semi-passiva (*chip* com bateria, comunicações com energia do leitor), sensores integrados, possibilitando coletar dados como temperatura, pressão, tensão elétrica e entre outros;
- Classe IV, sendo regraváveis, ativa, funciona como minirrádios, podendo se comunicar não somente com os leitores, mas também com outras etiquetas, podem conversar com outros identificadores, energizando suas próprias comunicações, formando redes inteligentes de logística;
- Classe V pode energizar e ler identificadores das Classes I, II e III e ler identificadores das classes IV e V, conceitualmente é leitor.

2.6 MySQL

O MySQL é o banco de dados de código aberto mais popular nos dias atuais. É um *software* muito confiável, fácil de ser manipulado e com uma enorme faixa de *softwares* em que é possível fazer interação.

Definimos banco de dados, como sendo o local em que os dados são armazenados e gerenciados, sendo os dados organizados em tabelas e ainda, que cada tabela estará relacionados uma com a outra de alguma maneira.

Para Júnior (2007), um sistema sem banco de dados não faz sentido, pois quando utilizamos um dado para identificar alguma coisa, isto tem que ser comparado com algo, para que o usuário possa receber e tratar esta informação da melhor forma possível para ele.

Segundo Date (2004) as características de um sistema relacional podem ser descritas analisando três aspectos: estrutural, em que seus dados são organizados em tabelas com linhas e colunas; integridade de dados no qual ocorre restrição para que os dados recebam apenas informações válidas, intervalos ou únicas; e manipulação de dados podendo ocorrer derivação de outras tabelas já existentes.

Para utilizá-lo necessita-se instalar um servidor e uma aplicação cliente, sendo o servidor responsável por armazenar os dados, responder todas as requisições, controlar a consistência dos dados além de executar as transações concomitantes e a aplicação cliente se comunicará com o servidor por meio da SQL.

Conforme Date (2004), a SQL é linguagem padrão para sistemas relacionais e foi desenvolvida pela *IBM* por volta dos anos 70, inclui operações de definição e manipulação de dados, sendo a operação de definição de dados chamada de *CREATE TABLE,* que pode ser traduzida para “Criar Tabela”, em que o nome da tabela a ser criada é especificado, assim como o nome e o tipo das colunas desta tabela, operações de manipulação de dados são as operações de seleção, inserção, exclusão e atualização, isto tudo já com a tabela criada.

Os comandos mais comuns de SQL e mais utilizados são:

- *CONNECT* é o comando usado para estabelecer a primeira conexão com o banco de dados, pois antes de realizar qualquer consulta, é necessário fazer a conexão;
- *SELECT* é utilizado para realizar uma consulta ao banco de dados, pela consulta podemos escolher quais dados queremos trazer (filtros);
- *INSERT* é usado para inserir dados no banco, ou seja, criar um novo registro no banco de dados;
- *UPDATE* é o comando usado para atualizar dados no banco;
- *DELETE* é usado para apagar dados.

Neste trabalho o sistema de gerenciamento de banco de dados (SGBD), será utilizado para a criação do banco de dados, responsável por armazenar os dados referentes à aplicação desenvolvida para a leitura das *tags* RFID, assim como a autenticação das mesmas, e ainda pelo fato do MySQL ser um *software* protegido por licença livre e gratuito.

2.7 ESP8266

O ESP8266 é um microcontrolador produzido pela empresa Espressif Systems, possui um sistema de comunicação sem fio (WiFi) próprio e permite que se rode programas carregados em sua própria memória, sendo este o seu grande diferencial, por esse motivo ele é largamente utilizado como módulo WiFi para outros microcontroladores, como por exemplo o modelo Arduino, sendo mais simples e com menos recursos. Uma grande vantagem de utilizar este modelo de microcontrolador ESP8266 é o seu baixo custo, geralmente na faixa de 20 a 50 reais no varejo, estando presente no mercado desde 2014.

Segundo Gimenez (2005), o microcontrolador é um dispositivo semicondutor em forma de circuito integrado, que integra as partes básicas de um microcomputador para aplicações específicas. Entre estas partes básicas estão: processador, memórias e portas de entrada e saída. Suas vantagens giram em torno de baixo custo e o baixo consumo de energia.

Para Bertogna (2014), os microcontroladores são sistemas microprocessados num único circuito integrado e, produzidos para oferecer uma variedade muito grande de dispositivos, memória e portas de entrada e saída, utilizadas em sistemas que não exigem alta complexidade de implementação e ótima relação custo/benefício.

Conforme Oliveira (2017), módulo ESP8266 é um microcontrolador WiFi-SOC, ou seja, ele possui a capacidade de se conectar a uma rede WiFi com um sistema integrado ao seu *chip*, podendo atuar como uma aplicação *stand-alone*, não precisando de nenhum outro componente para funcionar ou como um servidor escravo, podendo ainda funcionar também como um adaptador WiFi para outro microcontrolador, como por exemplo o Arduino, importante ressaltar que normalmente neste tipo de condição de acoplamento entre microcontroladores, é necessário utilizar adaptadores do tipo SPI ou UART, pois alguns modelos não os possuem.

Segundo Bertogna (2014), a SPI provê um tipo de comunicação serial síncrona de alta velocidade, possibilitando: interconexão entre microprocessadores e periféricos, *full duplex* sendo a comunicação em três fios, capaz de receber e transmitir simultaneamente, operação como mestre ou escravo, quatro taxas de bits

programáveis, sinalizador de proteção de colisão de escrita e ainda sinalizador de fim de transmissão.

Conforme Leens (2009), o protocolo SPI utiliza quatro sinais para realizar conexão entre um dispositivo mestre e um dispositivo escravo, sendo eles:

- SCLK - *Serial* de *clock*, todos os sinais do barramento são sincronizados com este sinal;
- SSn - Seletor de dispositivo escravo (*Slave Selection*), utilizado para selecionar o dispositivo escravo que o mestre deseja realizar uma comunicação;
- MOSI - Linha de dados do mestre para o escravo (*Master-Out Slave-In*);
- MISO - Linha de dados do escravo para o mestre (*Master-In Slave-Out*).

Ainda segundo Leens (2009), o barramento SPI permite a utilização de apenas um mestre, não limitando o número de escravos a ele conectados. Havendo somente um dispositivo mestre no barramento, qualquer comunicação é iniciada a partir dele. Quando o dispositivo mestre deseja enviar dados e/ou receber dados de um dispositivo escravo, ele seleciona o dispositivo alvo pela linha seletora (SSn), ativa o *clock,* envia dados por meio da linha MOSI enquanto amostra os dados da linha MISO, sendo assim o protocolo SPI *full duplex*, pois é capaz de enviar e receber dados simultaneamente.

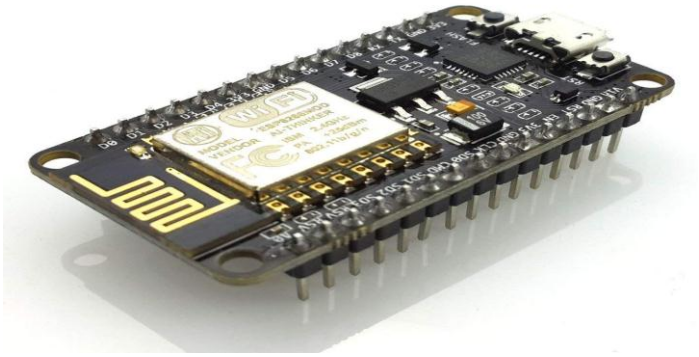
Para Škraba (2016), o ESP8266 em operação pode funcionar em duas configurações, sendo elas: *access point* e *client*. Na primeira configuração, ele funciona basicamente como um roteador, criando uma rede WiFi restrita por *login* e senha. Neste modo o ESP8266 cria um servidor com endereço IP aleatório ou predefinido dependendo da programação realizada, este servidor pode conter uma página *web* com informações dos componentes ligados ao ESP8266. Como *client*, ele estabelece uma conexão com a rede WiFi escolhida, uma vez conectado também cria um servidor e todos os dispositivos conectados na mesma rede WiFi que o ESP8266 têm acesso a este servidor pelo endereço IP. Este servidor também pode conter uma página *web* e seu endereço IP também pode ser aleatório ou predefinido na programação.

Neste projeto o ESP8266 funciona na configuração *client*, para que fosse possível utilizarmos o leitor de RFID e transmitirmos os dados.

Para carregar o programa ao ESP8266, utilizou-se a compilação em linguagem de máquina, por isso a necessidade de um compilador. A programação é implementada geralmente na linguagem C num computador e conectado por uma porta USB, após o código ser compilado, transferido a placa e enquanto esta estiver energizada, ele será executado de forma repetida. Sendo assim após compilar e gravar o programa na placa ESP8266, esta poderá rodar de forma independente, desde que continue sendo alimentada por apenas uma fonte.

Segue figura 10 para visualização do ESP8266 modelo ESP-12E NodeMCU, pois foi este modelo escolhido para se utilizar neste projeto.

Figura 10: ESP8266 ESP-12E NodeMCU



Fonte: Retirado do site amazon.com (2020)

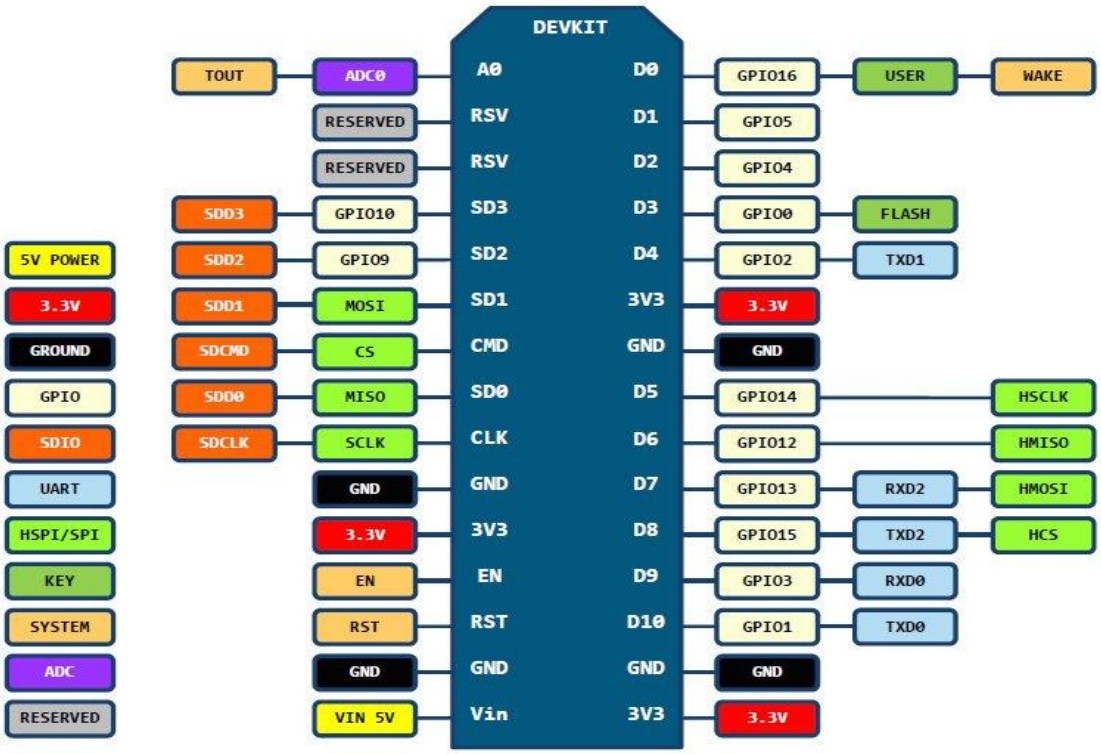
A partir de uma página *web* todos os comandos serão executados no ESP8266, pois ao conectá-lo na rede WiFi seu acesso fica disponível desta forma, desde que esteja configurado e carregado com o programa, caso contrário ele terá que se conectar via USB com o computador para programação e, ainda utilizar uma plataforma de programação, podendo ser o ambiente de desenvolvimento IDE, que seria a mesma plataforma do Arduino, apenas escolhendo o modelo correto de configuração e conexão.

Manitel (2016), descreve o módulo ESP8266 modelo ESP-12E NodeMCU que possui 16 pinos multiuso de entrada e saída, sendo 11 pinos digitais que podem ser utilizados para uso que operam com tensão de 3,3 V não podendo ultrapassar a corrente de 12 mA em cada pino. Esses pinos podem proporcionar outras funções, como controle de motores por meio de PWM, comunicação serial, havendo os seguintes protocolos: UART, SPI e I2C, além de possuir interrupções externas.

Ainda conforme Manitel (2016) existe a possibilidade de dano caso não seja respeitado o nível de tensão em 3,3 V, por mais que exista literatura informando a possibilidade de alimentação em 5 V, isto não é recomendado, mas caso haja esta necessidade de ligação, um divisor de tensão deverá ser implementado, para que não ocorra a queima da mesma.

Segue na figura 11, a pinagem do módulo ESP8266 ESP-12E NodeMCU, nela encontramos entradas e saídas.

Figura 11: Pinagem ESP8266 ESP-12E NodeMCU



Fonte: Retirado do site autocorerobotica.com.br (2020)

Segue especificações do módulo ESP8266 ESP-12E NodeMCU segundo o fabricante Espressif:

- Programação e alimentação via Micro-USB;
- CPU 32-bit RISC;
- CPU operando em 80 MHz, podendo operar em 160 MHz;
- *Chip* USB serial CH340;
- Tensão de operação: 5 V – 9 V (Via Micro-USB e pino VIN);
- Corrente de operação: em média 70 mA (com picos de 200 mA);

- *Chip* WiFi ESP8266-12E com conexão WiFi padrão 802.11 b/g/n e antena embutida;
- Alcance da antena: 90 m;
- Memória RAM: 20 KB;
- Memória FLASH: 4 MB;
- 10 (dez) portas GPIO: Com funções: MISO, MOSI, SCK, PWM, I2C, SPI, RX, TX (Comunicação Serial);
- 01 (uma) porta ADC – 10 bits de resolução;
- 03 (três) Modos de operação: *Access Point* /*Station* /*Access Point* + *Station*;
- Suporta até 5 conexões TCP/IP e comunicação TCP e UDP;
- Pinos extras para acesso à GND, VIN (Tensão de Entrada) e 3,3 V;
- Temperatura de operação: - 40 ºC à +125 ºC;
- Modos de programação: (IDE Arduino, Python, entre outros);
- *Update* remoto de *firmware* (via Arduino OTA);
- Dimensões: 49 x 25,5 x 7 mm;
- Peso aproximado: 8 g.

3 PROCEDIMENTOS METODOLÓGICOS

Para realização deste trabalho, conforme Gil (2008), a metodologia escolhida sobre o enfoque da natureza a pesquisa foi aplicada, pois gerou uma solução para um problema específico; sobre a abordagem a pesquisa foi qualitativa, visto que se baseou na interpretação dos fenômenos observados e nos significados que carregam; quanto aos objetivos a pesquisa foi de caráter exploratório, pois permitiu uma construção de hipóteses e tornou a questão mais clara, quanto aos procedimentos a pesquisa foi experimental, pois esta pesquisa gera um sistema de segurança patrimonial para identificação de equipamentos pelo uso da tecnologia RFID, uma vez que existem muitos equipamentos patrimoniados na UTFPR, no qual filtramos para o almoxarifado do DAELN.

Por haver uma grande quantidade de equipamentos cadastrados no sistema de patrimônio da UTFPR, uma abordagem acerca daqueles que circulam entre alunos, pesquisadores e professores do DAELN foi realizada, considerando os que possuem um maior valor agregado.

Experiências e amostragens foram feitas levantando-se nomes e modelos, números de série e patrimônio, incluídos no banco de dados, pois já estavam cadastrados na instituição, servindo de referência no trabalho proposto.

Após levantar todos os dados pertinentes aos perfis de cada equipamento ou bem patrimonial, criou-se uma tabela e códigos específicos no banco de dados e vinculados a uma *tag* RFID para rastreio, para melhorar a segurança e confiabilidade de todo sistema de segurança. Testes no almoxarifado do DAELN, com leituras e verificação de roubo dos equipamentos, por meio da entrada e saída dos mesmos.

Usou-se a tecnologia RFID com o objetivo de identificar o bem patrimoniado que poderia estar saindo do almoxarifado pelo portal instalado, saber se foi retirado sem autorização prévia de circulação, garantindo e reforçando a segurança com o auxílio da etiqueta RFID e ainda, com o sistema criado para cadastro e consulta.

Foi utilizado um módulo ESP8266 ESP-12E NodeMCU, que possui módulo WiFi integrado e leitor de RFID, para fazer a ponte entre o sistema de cadastro e banco de dados, pelo fato da facilidade de programação e por possuir várias entradas, sendo que sua escolha foi pela robustez e capacidade de processamento. Sua programação foi efetuada pela interface IDE que é a mesma utilizada pelo

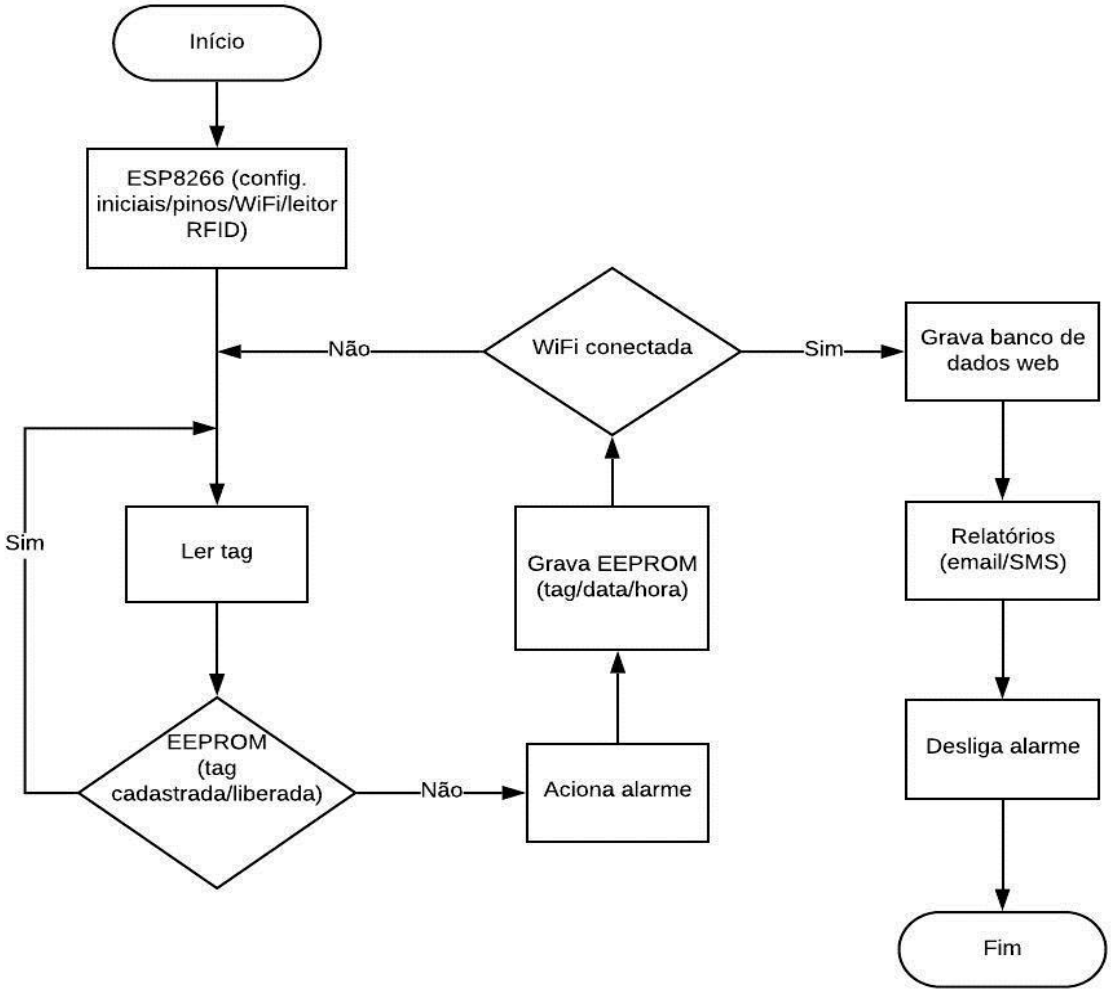
Arduino. Pelo fato do ESP8266 trabalhar com sistema embarcado, sem precisar estar ligado a nenhum outro dispositivo fisicamente, facilita-se o acesso a suas portas de entradas/saídas, pois leitor/antena RFID foi conectado em uma de suas entradas.

Utilizou-se o banco de dados relacional MySQL para vincular equipamentos já cadastrados no sistema da UTFPR, aproveitando tabelas já existentes e relacionadas, para gerar relatórios e *logs* no sistema, por meio de acesso via *web* ainda em construção.

Para facilitar o entendimento sobre o correto funcionamento do sistema de segurança, segue abaixo na figura 12 o fluxograma do sistema implementado. Com o ESP8266 carregado com as configurações iniciais, pinos devidamente setados, WiFi conectada e configurada com nome da rede WiFi e senha de acesso, leitor RFID pronto para leitura, memória EEPROM (memória interna do ESP8266) com dados carregados obtidos pela página *web* por meio dos métodos *GET* (busca de informações) e *POST* (inclusão de informações). Quando na leitura da *tag*, efetuada e comparada na memória EEPROM, verifica se determinado equipamento patrimoniado está liberado para sair do almoxarifado DAELN. Se a *tag* estiver liberada o alarme não será acionado, caso contrário o sistema enviará sinal para pino GPIO, configurado no ESP8266 de forma a disparar alarme/sirene, gravando neste momento um *log* na EEPROM contendo um sequencial, número da *tag* e data/hora do evento.

Na sequência, o sistema de segurança verifica se a rede WiFi está conectada, caso não esteja, continua com alarme disparado e segue processo de leitura de outras *tags*, e caso esteja conectada efetua gravação no banco de dados da página *web*, novamente pelos métodos *GET* e *POST*. Feito o processo de envio dos dados e gravação no banco de dados, página web em desenvolvimento poderá emitir relatórios de disparos, contendo equipamentos que saíram sem permissão, enviar SMS e assim por diante. Dentro da página *web*, mais precisamente na página de relatórios, existe a possibilidade de desativação do alarme, não findando o processo aqui, visto que tudo isso acontece em *loop*, reiniciando novamente as leituras e verificação de todos os processos do sistema de segurança.

Figura 12: Fluxograma do sistema de segurança



Fonte: Autoria própria (2020).

3.1 Programação ESP8266

O ESP8266 permite rodar *sketchs* carregados diretamente em sua memória, sendo assim ele pode funcionar de forma embarcada, sem estar ligado fisicamente a outro dispositivo, podendo se comunicar por WiFi ou por cabo USB conectado ao computador.

Para carregarmos um *sketch* ao ESP8266, precisamos compilá-lo em uma linguagem de máquina necessitando de um compilador, que geralmente utiliza linguagem C, sendo assim para facilitar este processo usou-se uma interface de programação chamada de IDE, existindo várias IDE's disponíveis e muitos trabalhos relacionados.

Linguagem de programação C é considerada de alto nível, sendo esta usada para programar microcontroladores e, estes conseguem se comunicar com mundo exterior por intermédio de pinos, sendo que alguns deles podem ser conectados a uma tensão de alimentação, a um sinal digital de referência (*clock*), enquanto outros pinos podem reiniciar a execução de um código (*reset*), ou converter sinais analógicos em digitais (A/D) e vice-versa, ou podem ser definidos como pinos GPIO. Alguns destes pinos podem também ser configurados no programa residente (*Firmware*), para atuar como uma entrada ou como uma saída.

3.1.1 IDE do Arduino

Para começarmos a utilizar o ESP8266 devemos instalar a interface de programação IDE do Arduino, encontrado no site arduino.cc, por proporcionar uma maior facilidade de uso, além de possuir uma vasta documentação e ser gratuita, trazendo muitas vantagens ao programador como menor tempo e esforço para escrever o código.

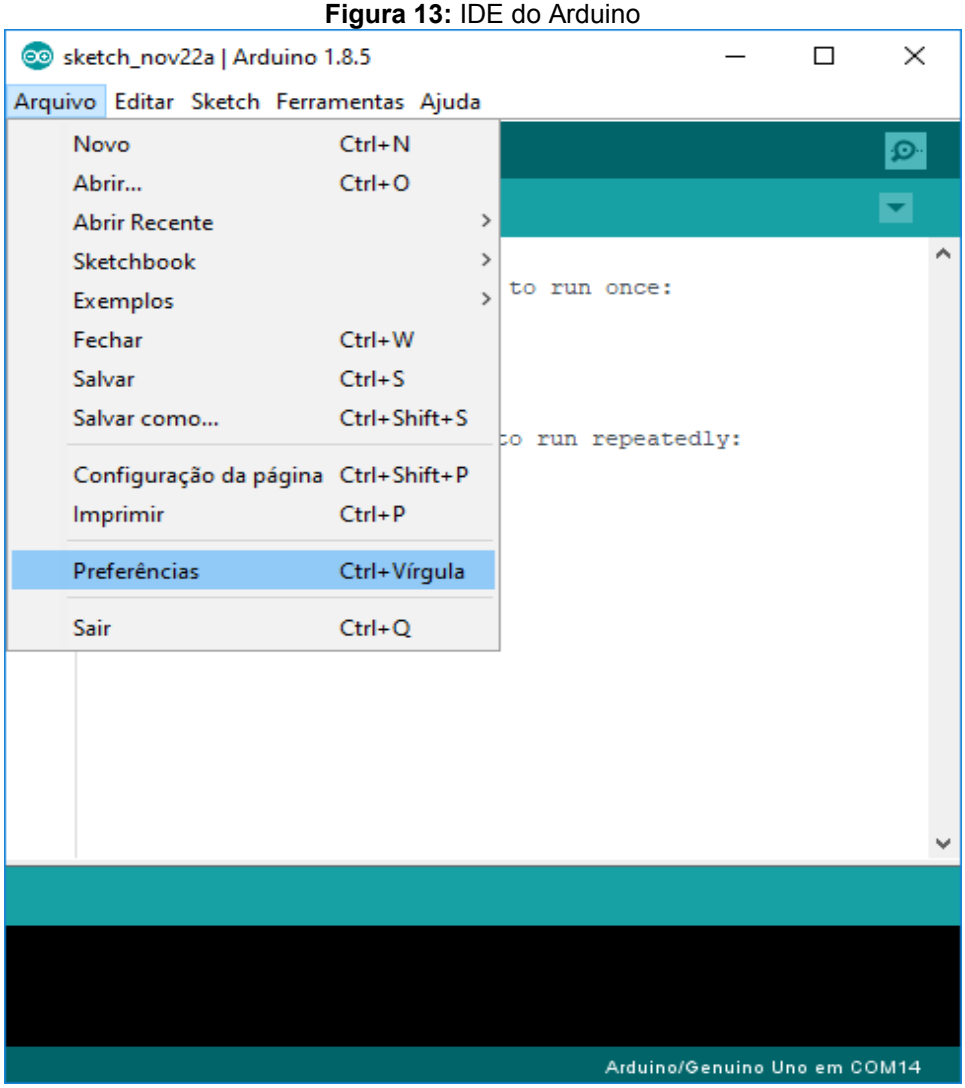
Outro fator determinante na escolha deste IDE foi pelo fato do mesmo possuir um monitor serial, que permite monitoramento da conexão entre o computador e o microcontrolador NodeMCU, facilitando a depuração do código e permitindo que o usuário forneça comandos ao microcontrolador.

Pelo fato de ser uma plataforma de código aberto, foi implementado pelo fabricante da placa (Espressif) a possibilidade de selecionarmos o ESP8266 no ambiente de desenvolvimento IDE.

Para fazermos a configuração correta da placa ESP8266, segue passo a passo procedimento de correta instalação da mesma:

1. Abrir janela de preferências, conforme figura 13 a seguir.

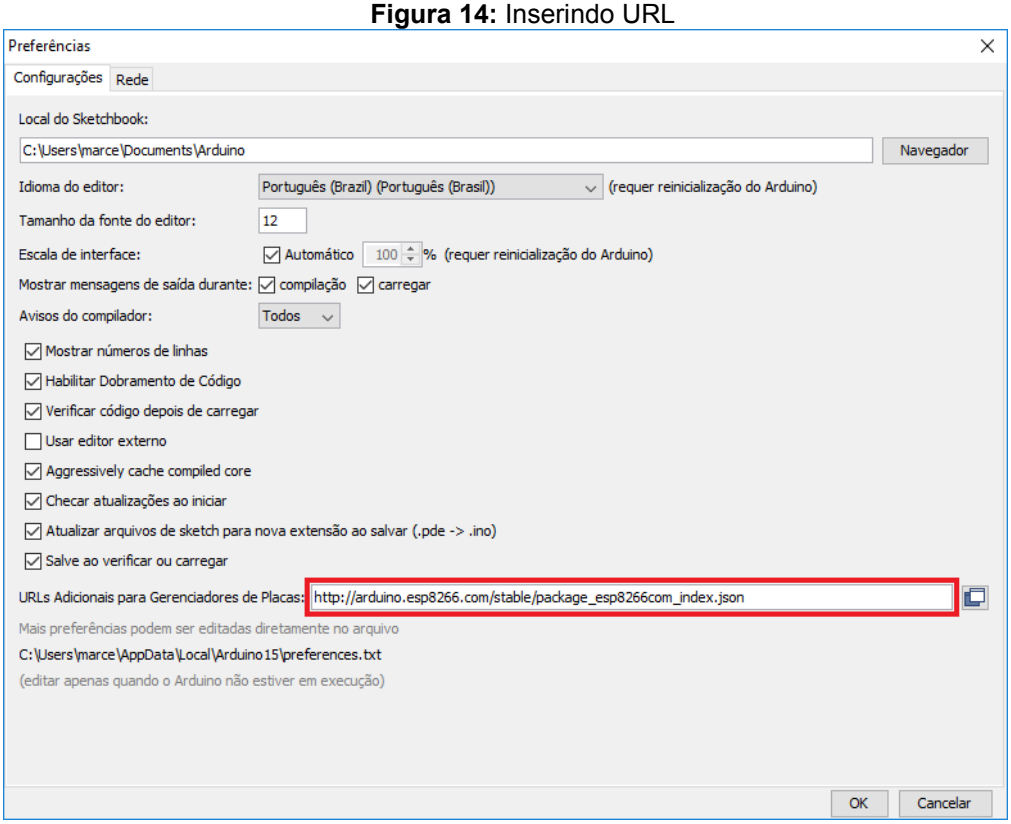
Figura 13: IDE do Arduino



Fonte: Retirado do site autocorerobotica.com.br (2020)

2. Inserir URL no campo de gerenciamento de placas adicionais: http://arduino.esp8266.com/package_esp8266com_index.json, como mostrado na Figura 14.

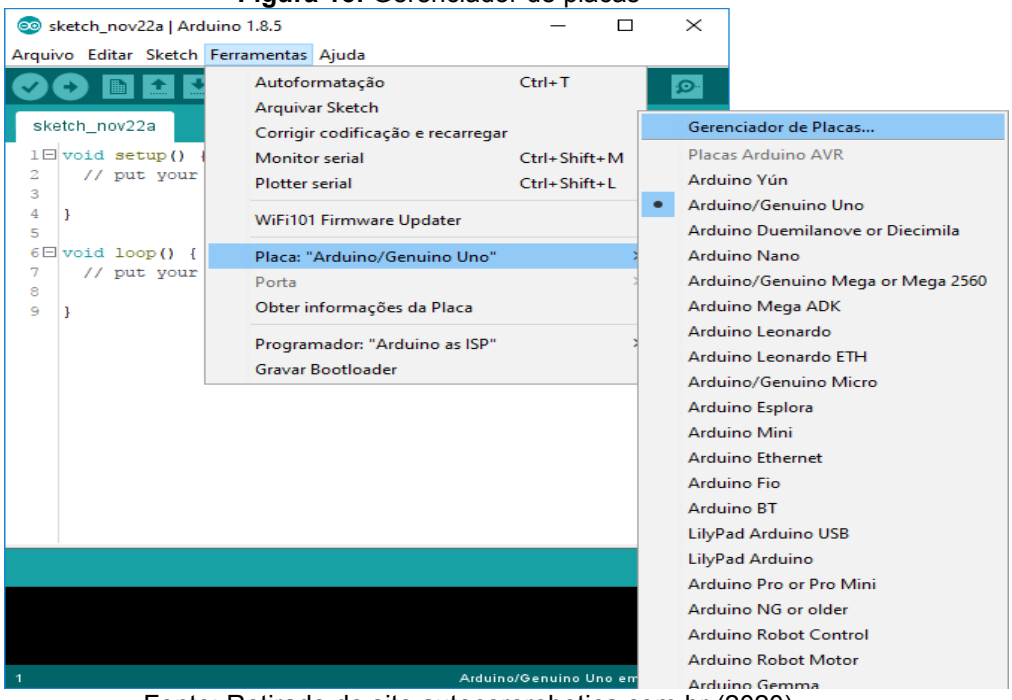
Figura 14: Inserindo URL



Fonte: Retirado do site autocorerobotica.com.br (2020)

3. Clicar em ferramentas, placas, selecionar gerenciador de placas, como mostrado na Figura 15.

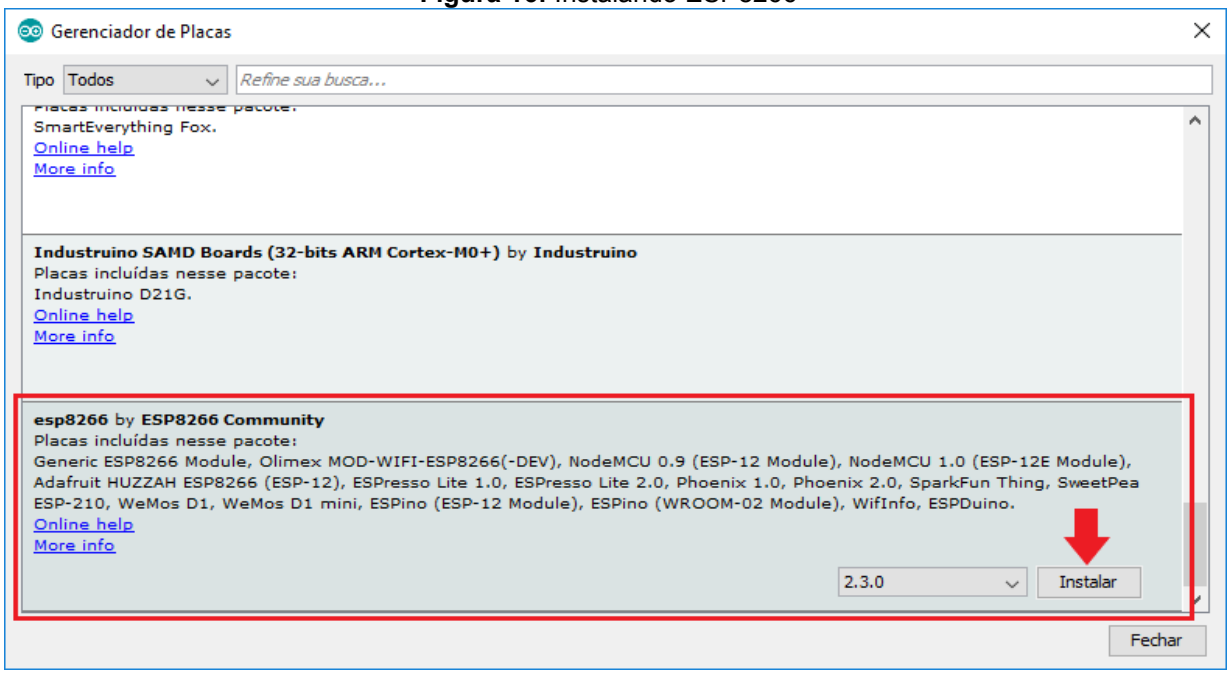
Figura 15: Gerenciador de placas



Fonte: Retirado do site autocorerobotica.com.br (2020)

4. Instalar a placa ESP8266, selecionando gerenciador de placas o item do ESP8266, como na Figura 16.

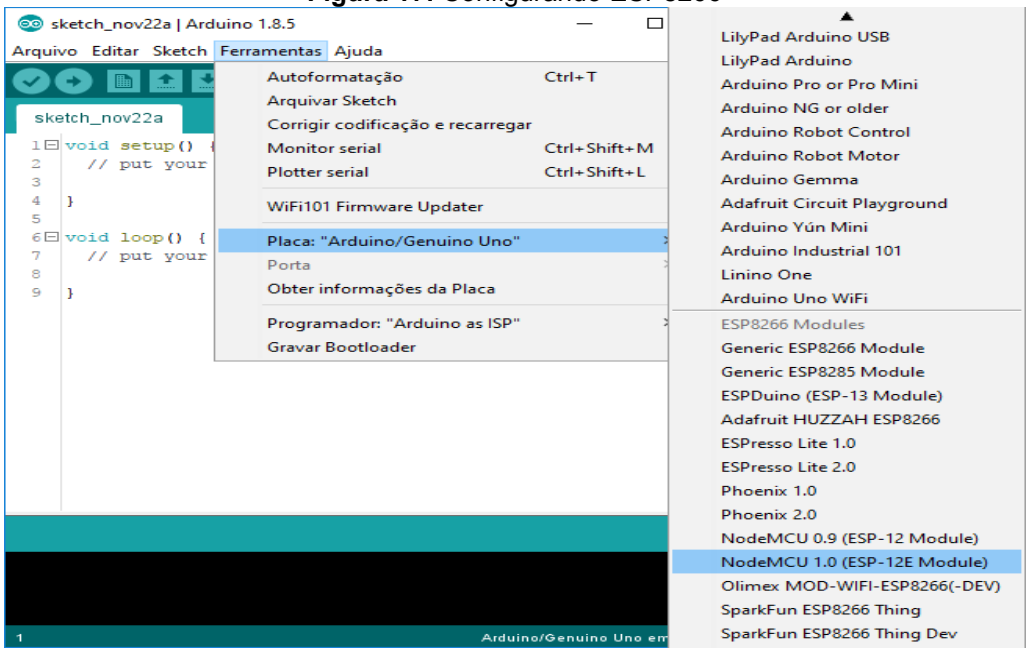
Figura 16: Instalando ESP8266



Fonte: Retirado do site autocorerobotica.com.br (2020)

5. Próximo passo escolher a placa desejada para uso, que neste caso será NodeMCU 1.0 (ESP-12E Module). Conforme sequência na figura 17.

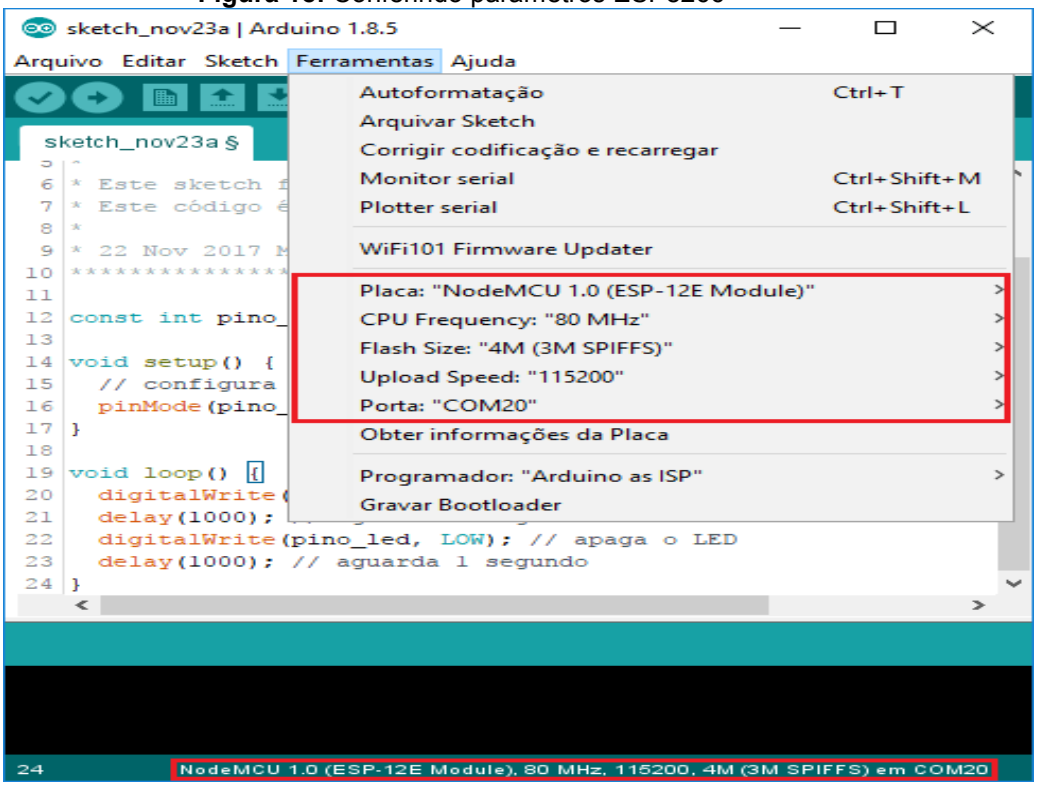
Figura 17: Configurando ESP8266



Fonte: Retirado do site autocorerobotica.com.br (2020)

6. Conferir parâmetros da configuração para concluir instalação do IDE, marcados conforme figura 18.

Figura 18: Conferindo parâmetros ESP8266



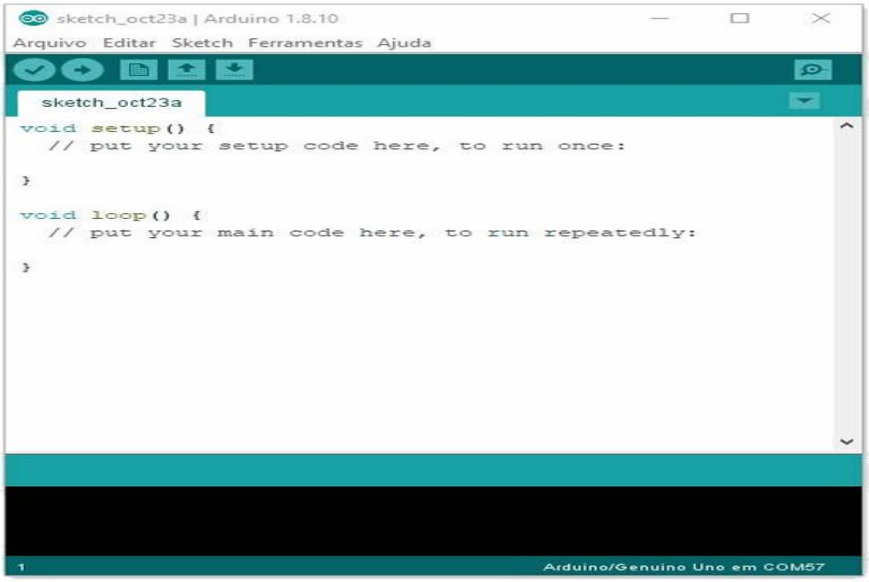
Fonte: Retirado do site autocorerobotica.com.br (2020)

3.1.2 Desenvolvimento com o IDE do Arduino

O desenvolvimento de qualquer aplicação neste ambiente se utiliza da linguagem C++, sendo chamados "*sketchs*" e dividido em três etapas: primeira etapa inclusão de bibliotecas e definição de variáveis a serem utilizadas, podendo adicionar tantas bibliotecas quanto forem necessárias; segunda etapa configuração e inicialização de periféricos e variáveis na função chamada *void setup()* e a terceira etapa em que a aplicação permanece rodando indefinidamente até o ponto de interrupção, nesta área no qual o código está rodando, chamada de *void loop()*.

Segue figura 19 exemplificando um exemplo de *sketchs* no ambiente IDE do Arduino.

Figura 19: *Sketch* ambiente IDE do Arduino



Fonte: Retirado do site autocorerobotica.com.br (2020)

A função *setup* é chamada toda vez que o dispositivo é ligado, sendo a primeira função a ser chamada, realizará todas as chamadas de inicialização do programa, tais como: funções e variáveis usadas no código, modos de operação dos pinos de entrada ou saída, pino digital ou analógico.

A função *loop* é chamada necessariamente após a função *setup*, funcionando como um laço, sempre ao seu final a função é chamada novamente, até que um comando seja dado para a função parar ou o dispositivo seja desligado. Nessa função são realizadas todas as chamadas pertinentes ao funcionamento normal da placa, o que o programa deve realizar ao longo do seu funcionamento.

Para que possamos interpretar todas as funcionalidades ou sinais de sensores, como outro dispositivo conectado na placa e transmitir informações para o programa, serão necessárias as bibliotecas que são os códigos que executam tarefas, facilitando o desenvolvimento de novos códigos e evitarmos erros. Tendo como principal função, fornecer suporte por meio do *software* para acesso aos componentes e que geralmente são fornecidos pelos fabricantes, encontrados em suas páginas na internet disponibilizadas por comunidades de desenvolvedores.

Segue na figura 20, desenvolvimento deste projeto no ambiente IDE do Arduino, nas três etapas.

Figura 20: Ambiente de desenvolvimento IDE para ESP8266

```
#include<wifi.h>
#include<RC522.h>
#include<storeTag.h>
#include<systemSecurity.h>

#define RST_PIN    D3
#define SS_PIN     D8

unsigned long timeAtual;
unsigned long timeAnterior;

String TAG="";
int AmountTag=0;
//inicia uma classe de autoria propria, para trabalhar com o armazenamento das TAG's.
StoreTag* store = new StoreTag(4096);
//inicia uma classe de autoria propria, para trabalhar com a leitura dos dados do RC522
Rc522* rc522 = new Rc522(SS_PIN,RST_PIN);
//inicia uma classe de autoria propria, para trabalhar com a leitura e escrita do banco de dados
//WIFI_CONNECT* wifi = new WIFI_CONNECT("TP-LINK_4386","HEMI2016","192.168.1.25");
WIFI_CONNECT* wifi = new WIFI_CONNECT("[illegible]","[illegible]","192.168.1.2");
//inicia classe do sistema de segurança passando o objeto rc522, o pino de interurpção do rc522, e os objetos store e wifi
SystemSecurity* Sys = new SystemSecurity(rc522,store,wifi);

void setup() {
  Serial.begin(115200); //inicia o monitor serial do arduino com a frequencia de 115200 bits/s
}
void loop() {
  Sys->main();
}
```

Fonte: Autoria própria (2020).

As bibliotecas declaradas e necessárias para execução deste projeto estão listadas abaixo:

- ESP8266WiFi.h: permite que o projeto utilize classes como: WiFi, *Client*, *Server* e IP *adress*, possuem funções que serão utilizadas dentro da função *setup* e da função *loop*, para realizar tanto a parte de conexão com a rede, monitoramento desta conexão e também toda a parte de operação do ESP8266 na configuração *client*.;
- WiFiCliente.h: permite criar um cliente para poder se conectar num endereço e portas específicas;
- ESP8266WebServer.h: possui a função para hospedar uma página da *web* a partir de uma rede WiFi, respondendo com HTML ao navegador, sendo suficiente para exibir os valores de entrada dos pinos lógicos;
- ESP8266HTTPCliente.h: permite realizar requisições HTTP, sejam elas *GET* (busca de informações), *POST* (inclusão de informações), *PUT* (atualização) ou *DELETE* (remoção);
- SPI.h: responsável por fornecer funções capazes de realizar comunicação entre o microcontrolador e um dispositivo periférico, por um protocolo serial de dados adequado;

- MFRC522.h: específica para reconhecer e gerenciar várias funções deste leitor de RFID;
- EEPROM.h: utilizada para disponibilizar acesso a memória EEPROM, fornecendo comandos para ler e escrever dados.

Como forma de facilitar a fase de programação do microcontrolador e evitar atrasos na escrita do código e, ainda em relação ao número total de linhas digitadas, além das bibliotecas mencionadas anteriormente, outras foram adicionadas e criadas com métodos próprios para um desenvolvimento mais facilitado e resumido, no qual métodos foram adicionados utilizando programação orientada a objetos, para demonstrar em que todos os arquivos com extensão ".h" são as bibliotecas com as declarações dos métodos, tipos e variáveis declaradas utilizadas no projeto, sendo todos estes arquivos presentes no pacote biblioteca no IDE Arduino.

A figura 21 apresenta a declaração da biblioteca WiFi.h, declarando métodos e classes, pegando o endereço IP e conectando o ESP8266 a rede WiFi.

Figura 21: Declaração da biblioteca WiFi.h

```
C wifi.h > WIFI_CONNECT
1   #ifndef WIFI_CPP
2   #define WIFI_CPP
3   #include <Arduino.h>
4   #include <ESP8266WiFi.h>
5   #include <WiFiClient.h>
6   #include <ESP8266WebServer.h>
7   #include <ESP8266HTTPClient.h>
8   class WIFI_CONNECT{
9       private:
10          IPAddress host;
11          String link; // link padrao do site
12      public:
13      WIFI_CONNECT(char* ssid,char* password,char* host); //construtor
14      //metodos de acoes externas
15      String setDatabase(String page,String output); //setar informação no banco de dados
16      String getStringDatabase(String page,String actions); //pegar informação no banco de dados
17      //metodos de acoes internas
18      IPAddress getLocalIp(); //pegar ip do esp
19      boolean ImConnected(); //estou conectado?
20
21
22  };
23
24  #endif
```

Fonte: Autoria própria (2020).

A figura 22 apresenta a declaração da biblioteca RC522.h, configurando os pinos do leitor RFID modelo RC522 e verificando sua disponibilidade e funcionamento no sistema.

Figura 22: Declaração da biblioteca RC522.h

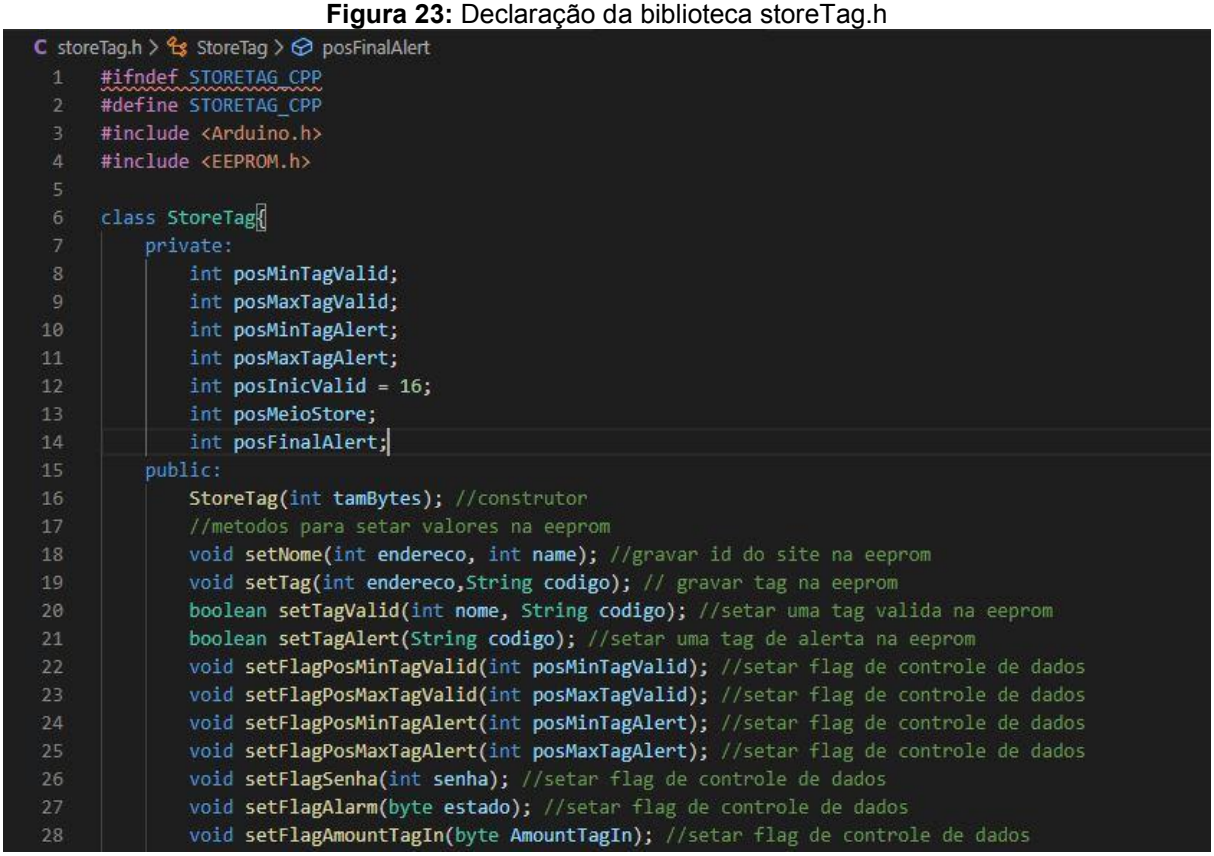
```
#ifndef RC522_CPP
#define RC522_CPP
#include <Arduino.h>
#include <SPI.h>
#include <MFRC522.h>

class Rc522{
    private: // apenas metodos das classes podem acessar essas variaveis
        uint8_t ss_pin; // Select pin
        uint8_t rst_pin; // Reset pin
        MFRC522* RFID; // Ponteiro do objeto MFRC522
    public: // qualquer classe pode acessar
        Rc522(uint8_t ss_pin, uint8_t rst_pin); //Construtor
        boolean Rc522available(); //Verificar se o sensor esta funcionando
        String getTag(); //Leitura do sensor
};
#endif
```

Fonte: Autoria própria (2020).

A figura 23 apresenta a declaração da biblioteca storeTag.h, contendo as variáveis declaradas, construtores e métodos utilizados, início de posição de gravação na memoria EEPROM do ESP8266 e principalmente controle de dados gravados e excluídos no ESP8266.

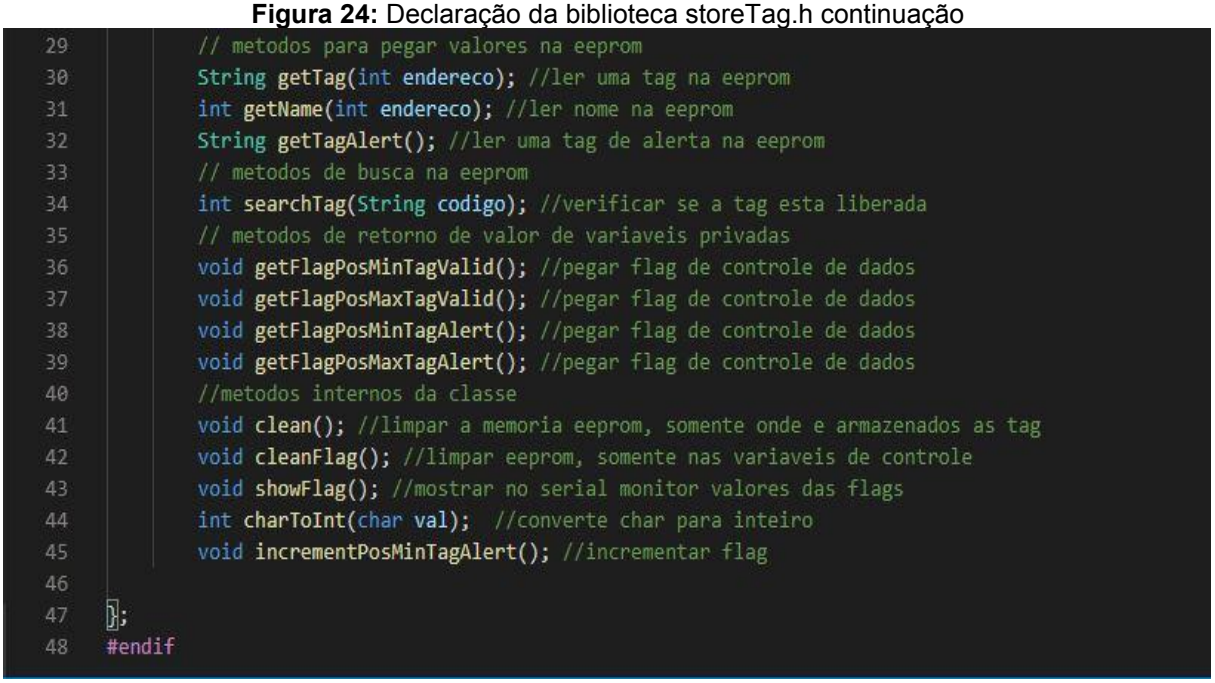
Figura 23: Declaração da biblioteca storeTag.h



Fonte: Autoria própria (2020).

A figura 24 apresenta a continuação da declaração da biblioteca storeTag.h.

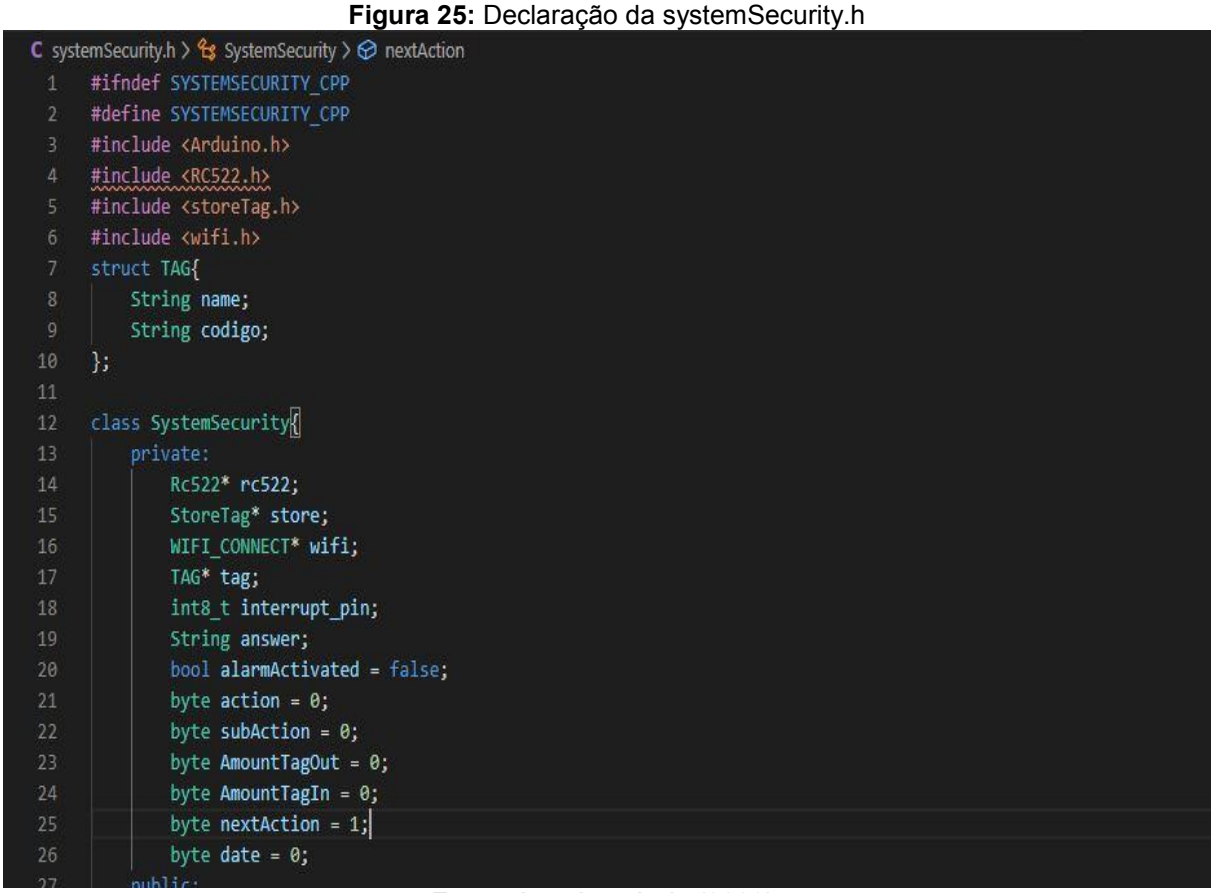
Figura 24: Declaração da biblioteca storeTag.h continuação



Fonte: Autoria própria (2020).

A figura 25 apresenta a declaração da biblioteca systemSecurity.h, contendo declaração de variáveis com seus valores, controle e leitura das *tags*, monitoramento do leitor RFID, acionamento do alarme, *loop* do código digitado e as funções principais do sistema proposto.

Figura 25: Declaração da systemSecurity.h



Fonte: Autoria própria (2020).

A figura 26 apresenta a continuação da declaração da biblioteca systemSecurity.h.

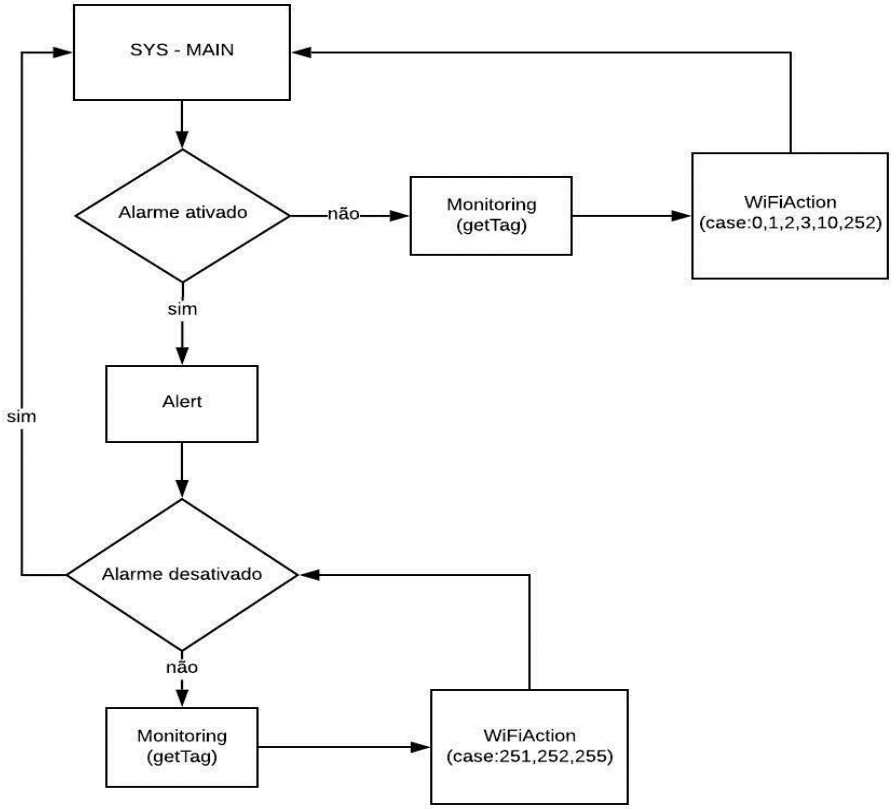
Figura 26: Declaração da systemSecurity.h continuação

```
27      public:
28          SystemSecurity(Rc522* rc522, StoreTag* store, WIFI_CONNECT* wifi); //construtor
29          SystemSecurity(Rc522* rc522, int8_t interrupt_pin, StoreTag* store, WIFI_CONNECT* wifi); //construtor
30          bool authorization(int nome,String Tag); //verificando se a tag passada no sensor esta liberada
31          void monitoring(int nome); //monitora o sensor pra ve se tem uma tag para ler
32          void main(); //loop principal quando o alarme esta desativado
33          void alert(); //loop principal quando o alarme esta ativado
34          void wifiAction(); //fazer uma ação referente ao wifi
35          String variable(int pos, String dado); //pegar variavel apartir da string retornada pelo site
36          //ações possiveis via wifi
37          void actionSetAction(); //verificar se o usuario admin, quer fazer alguma ação em especial.
38          void actionGetDate();  //pegar a data do dia.
39          void actionAmountTag(); //pegar quantidade de tags liberadas no site
40          void actionGetTag(); //buscar tag no site
41          void actionEchoAlert(); //emitir um alerta de alarme ao site
42          void actionEchoTagAlert(); //emitir as tags de alerta ao site gerando um login.
43          void actionDesableAlarm(); //desativar o alarme
44          void actionRegisterTag(); //registrar tag a um equipamento.
45
46      };
47      #endif
```

Fonte: Autoria própria (2020).

Para facilitar o entendimento sobre o correto funcionamento do fluxo de programação da biblioteca systemSecurity.cpp, a qual faz parte da programação orientada a objetos dentro da biblioteca systemSecurity.h de forma a proporcionar uma melhor prática e facilidade de desenvolvimento do sistema de segurança proposto. Funcionamento de suas funções e sub funções, que nada mais são os métodos programados, segue na figura 27 o diagrama do sistema (*loop*). Sendo o principal objetivo do sistema de segurança implementado a leitura das *tags* RFID, sistema monitora o leitor RFID independente se o ESP8266 esteja conectado ao WiFi ou não. A seguir será explicado cada uma destas funções implementadas dentro biblioteca criada systemSecurity.cpp., de forma a facilitar o entendimento da programação efetuada.

Figura 27: Diagrama do sistema (*loop*)



Fonte: Autoria própria (2020).

Na sequência, vimos na figura 28 a declaração das variáveis dentro do método *main*, que são chamadas de forma sequencial e em *loop*, estando o alarme ativado emitirá um alerta/sirene e continuará monitorando/lendo *tags* indiferente se rede WiFi esteja conectada ou não.

Figura 28: Declaração do método SYS-MAIN

```
void SystemSecurity::main(){
    if(this->alarmActivated){
        this->alert();
    }else{
        this->monitoring(1);
        this->wifiAction();
    }
}
```

Fonte: Autoria própria (2020).

Na figura 29 vimos a declaração do método *Alert*, no qual está configurado no pino D1 do ESP8266 para emitir um sinal de disparo do alerta/sirene, que será desabilitado somente por comandos do sistema proposto na *web* em construção.

Figura 29: Declaração do método *Alert*

```
void SystemSecurity::alert(){
    this->action = 250;
    this->subAction = 0;
    digitalWrite(D1,HIGH);
    while(this->alarmActivated){
        this->monitoring(0);
        this->wifiAction();
        //store->showFlag();
        //delay(1000);
    }
    this->subAction = 0;
}
```

Fonte: Autoria própria (2020).

Na figura 30 vimos a declaração do método *Monitoring* que faz a verificação da *tag* disponível, verifica se ela esta liberada na memória EEPROM do ESP8266, caso não esteja muda *flag* de disparo do alarme, salva *log* nesta mesma memória e muda o tipo do usuário do sistema para universal, sendo assim caso equipamento volte para dentro do almoxarifado, passando pelo portal o alarme não será disparado, pois usuário já foi cadastrado e gravado no sistema.

Figura 30: Declaração do método *Monitoring*

```
void SystemSecurity::monitoring(int name){
    String Tag = rc522->getTag();
    Serial.print(" getTag: ");
    Serial.println(Tag);
    if(Tag != "0"){
        Serial.println("entro");
        if(!this->authorization(name,Tag)){
            store->setTagAlert(Tag);
            this->alarmActivated = true;
            Serial.println("alarme");
        }else{
            Serial.println("Liberado");
        }
    }
}
```

Fonte: Autoria própria (2020).

Seguindo sobre métodos, vimos na figura 31 a declaração do método *WiFiAction*, programação feita em que as ações utilizam *case*, que são as decisões no sistema proposto, de forma que o retorno de uma função envia um determinado número que tomará um caminho a seguir dentro deste método, segue abaixo explicado cada *case* com sua ação e o seu significado:

- *Case* 0: setAction, verifica se tem alguma função específica;
- *Case* 1: getDate, pegar a data do dia;
- *Case* 2: amountTag, número de *tags* liberadas no *site*;
- *Case* 3: getTag, pegar *tag* liberada;
- *Case* 10: cadastrar *tag*;
- *Case* 250: echoAlert, emitir alerta ao *site* (*email*);
- *Case* 251: echoTagAlert, emitir ao *site* os *logs*;
- *Case* 255: disableAlert, desativar alarme.

Figura 31: Declaração do método *WiFiAction*

```
void SystemSecurity::wifiAction(){
    if(!wifi->ImConnected()) {
        Serial.println("nao esta conectado");
    }else{
        switch (this->action)
        {
        case 0: // verificar se tem alguma ação forçada pelo site    //Serial.println("0");
            this->actionSetAction();
            break;
        case 1: // get date time   //Serial.println("1");
            this->actionGetDate();
            break;
        case 2: // AmountTag   //Serial.println("2");
            this->actionAmountTag();
            break;
        case 3: // Get tag site   //Serial.println("3");
            this->actionGetTag();
            break;
        case 10: // OUTPUT tag cadastramento   //Serial.println("7");
            this->actionRegisterTag();
            break;
        case 250: //emitir alerta de alarme //Serial.println("250");
            this->actionEchoAlert();
            break;
        case 251: // enviar tag ao site  //Serial.println("251");
            this->actionEchoTagAlert();
            break;
        case 255: //desativar alarme  //Serial.println("255");
            this->actionDesableAlarm();
            break;
        }
    }
```

Fonte: Autoria própria (2020).

Aproveitando os recursos da memória EEPROM do ESP8266 com capacidade para 4096 posições/*bytes*, separamos as 16 primeiras posições desta memória para implementação das *flags* declaradas no sistema, sendo elas: posMinTagValid (2 *bytes*), posMaxTagValid (2 *bytes*), posMinTagAlert (2 *bytes*), posMaxTagAlert (2 *bytes*), alarmActivated (1 *byte*), AmountTagIn (2 *bytes*) e ainda 5 *bytes* para posições futuras de outras aplicações que possam ser adicionadas.

Ainda dentro da memória EEPROM do ESP8266, utilizamos 2040 posições para validação, sendo 2 posições para o id (usuário) e 4 posições para *tag*, totalizando 340 registros de validação dos usuários com suas *tags*, outras 2040 posições para alerta, sendo 4 posições para cada *tag*, totalizando 510 registros de alertas de *tags* que saíram sem autorização do almoxarifado.

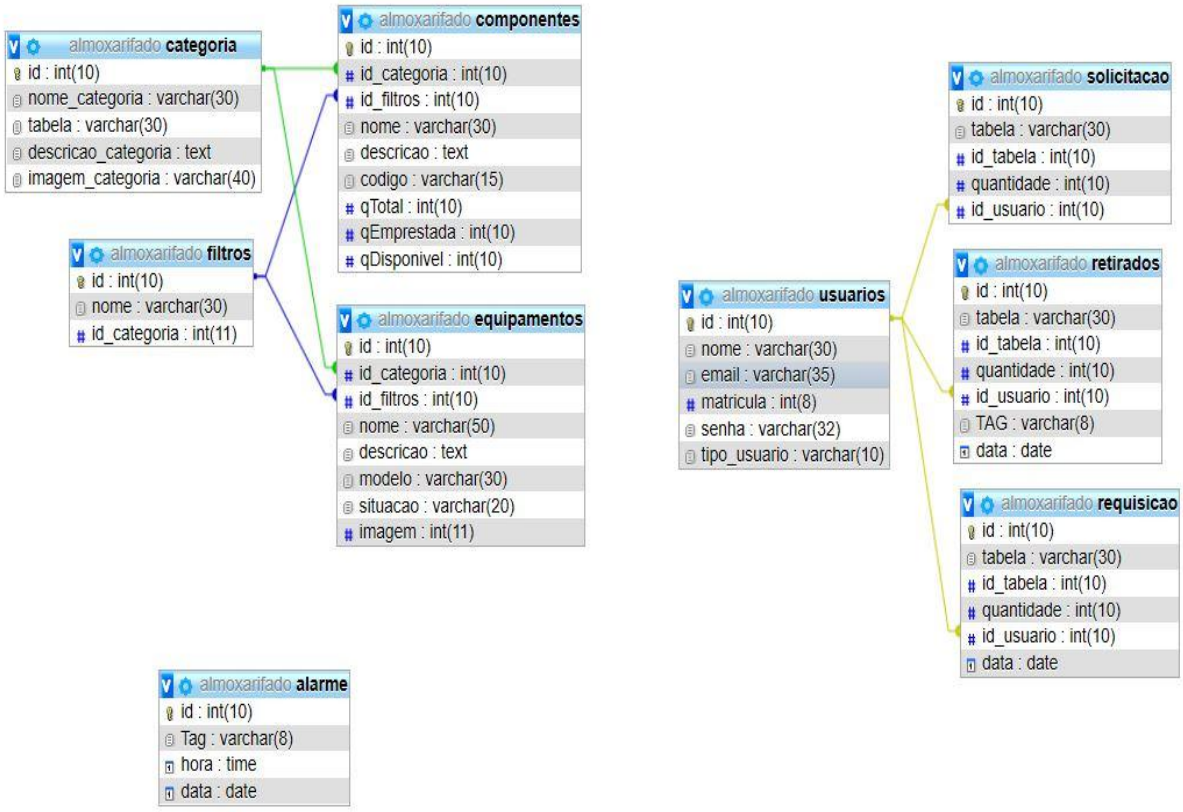
Lembrando ainda, todos estes registros mencionados nestas posições de memória deverão ser reescritos somente após preenchimento de todo espaço reservado para eles, sendo permitidas 10.000 gravações em cada posição de memória EEPROM do ESP8266, por isso o sistema implementado faz a verificação de cada posição no momento de cada gravação. Número de leituras pode ser infinita, apenas gravações tem restrição de quantidade de gravação.

3.2 MySQL

Para o armazenamento de registros de entrada/saída e também de usuários cadastrados, utilizou-se o banco de dados MySQL. Neste projeto o servidor *web* acessa o banco de dados MySQL que faz consulta, inserção e exclusão de dados, encaminha esses pedidos e faz toda a gestão interna dos dados, após devolve ao servidor *web* todos os dados solicitados.

Segue na sequência figura 32, o diagrama entidade relacionamento (DER) do banco de dados MySQL, gerado com todas tabelas criadas contendo a estrutura lógica utilizada neste projeto.

Figura 32: Diagrama entidade relacionamentos (DER) banco de dados



Fonte: Autoria própria (2020).

Testes foram feitos utilizando apenas rede WiFi local, apontando inclusive para um endereço URL, visto que a página *web* está ainda em construção, utilizando métodos *GET* e *POST* para ler e enviar os dados do ESP8266, gravando no banco de dados um *log* com o histórico de leituras dos equipamentos que saíram do almoxarifado, constando um sequencial com o número da *tag* e data/hora do evento, conforme figura 33.

Figura 33: Tabela banco de dados com eventos da página *web*

id	TAG	datetime
1	91A0CC73	2020-02-16 13:42:36
2	D1D1DC73	2020-02-16 13:43:19
3	D1D1DC73	2020-02-16 13:45:49
4	D1D1DC73	2020-02-16 13:45:50
5	D1D1DC73	2020-02-16 13:45:52
6	D1D1DC73	2020-02-16 13:45:53
7	BBAAD773	2020-02-16 13:46:02
8	BBAAD773	2020-02-16 13:46:03
9	E59AD973	2020-02-16 13:46:32
10	E59AD973	2020-02-16 13:46:33
11	B149C773	2020-02-16 13:46:37
12	B149C773	2020-02-16 13:46:38
13	25C1DD73	2020-02-16 13:46:42
14	25C1DD73	2020-02-16 13:46:43
15	B149C773	2020-02-16 14:03:23
16	B149C773	2020-02-16 14:03:24
17	B149C773	2020-02-16 14:03:36
18	B149C773	2020-02-16 14:03:37
19	B149C773	2020-02-16 14:04:06
20	B149C773	2020-02-16 14:04:06
21	B149C773	2020-02-16 14:09:22
22	B149C773	2020-02-16 14:09:23
23	25C1DD73	2020-02-16 14:09:30

Fonte: Autoria própria (2020).

3.3 Leitores RFID

Para simulações e testes de leitura das *tags* RFID em conjunto com o ESP8266 foi utilizado o leitor RC522, trabalhando com *tags* na frequência de operação de 13,56 MHz e alimentação de 3,3 V, facilitando assim sua conectividade

e alimentação ao circuito proposto, segue figura 34 com a pinagem do leitor RFID RC522.

Figura 34: Leitor RFID RC522

Fonte: Retirado do site autocorerobotica.com.br (2020)

Para fazer a leitura das *tags* teremos que conectar os pinos do leitor RC522 pelo protocolo de comunicação SPI no módulo ESP8266, declarar bibliotecas e inicialização do programa no IDE, segue descrição dos pinos deste leitor de RFID:

- MISO (*Master In Slave Out*): uso do barramento *Slave* para enviar dados do escravo para o mestre;
- MOSI (*Master Out Slave In*): uso do barramento *Master* para enviar dados do mestre para os periféricos (escravos);
- SCK (*Serial Clock)*: relógio de pulso que sincroniza a transmissão de dados gerada pelo mestre;
- SS (*Slave Select*): pino de controle para indicar qual escravo comunica com o mestre, isto no caso de mais dispositivos ligados.

3.4 Circuito

O módulo ESP8266 foi escolhido para montagem, devido a sua relação com baixo custo somado ao benefício, tendo integrado em um único componente a comunicação pela rede WiFi, portas digitais, portas analógicas e protocolos de

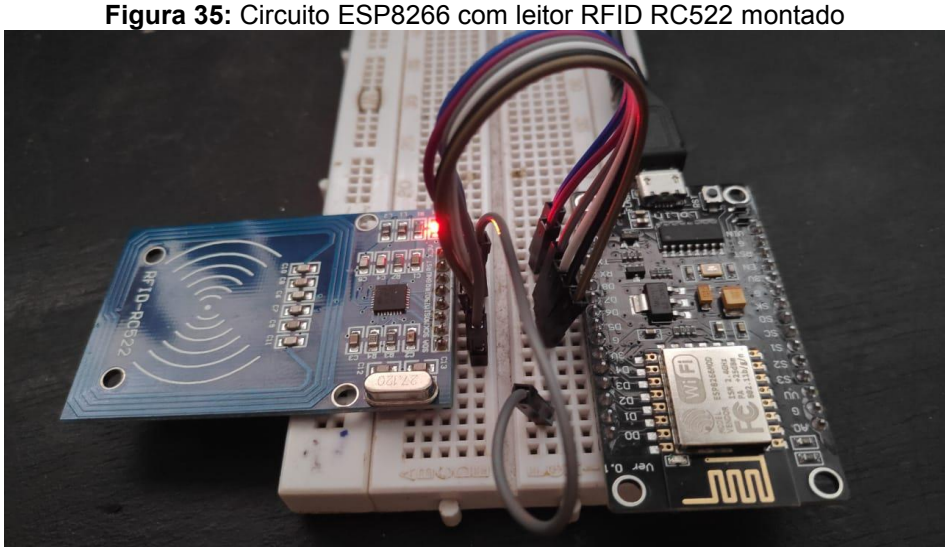
comunicação compatíveis com o leitor RFID RC522, o qual recebe alimentação de 3,3 V fornecida pelo ESP8266.

A alimentação de entrada é de 5 V, podendo ser via USB, fonte chaveada ou 3,3 V. Já os terminais de alimentação internos são de 3,3 V, sendo compatível com uma grande variedade de dispositivos, não excedendo estes valores de tensão para evitarmos possíveis danos as entradas. Sendo ainda possível conectar uma bateria de 9 V em sua entrada de alimentação VIN, deixando aqui uma ressalva de apenas uma fonte de alimentação ao ESP8266, ou seja, uma ou outra e ainda conectado ao pino correto.

Com o circuito montado e alimentado, pode-se definir uma lógica de funcionamento, sendo o ESP8266 o módulo principal de toda a arquitetura, podendo definí-lo como o cérebro de todo o processo e, sendo nele efetuado toda lógica de programação, por isso iniciamos a descrição por este componente.

O módulo ESP8266 alimenta (3,3 V) e comanda o leitor RFID por conectores e fios, a comunicação SPI é usada para a transferência e recepção de dados entre eles, a troca de dados entre o leitor RFID e a *tag* é feita por intermédio de um campo magnético, isto é, sem que exista contato físico entre eles, circuito montado mostrado na figura 35.

Figura 35: Circuito ESP8266 com leitor RFID RC522 montado

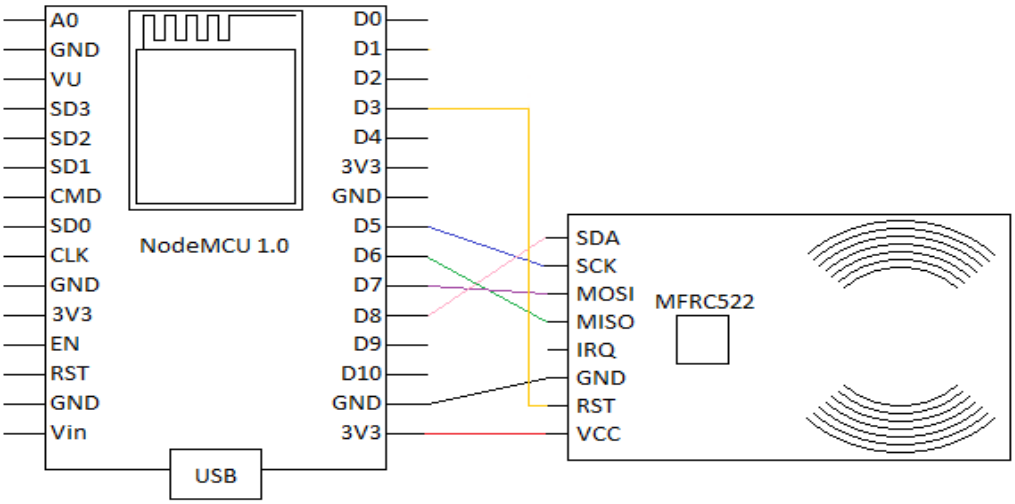


Fonte: Autoria própria (2020).

Para montagem do circuito em testes procedeu-se da seguinte forma: o pino digital D3 do ESP8266 foi ligado ao pino de *reset* do leitor RC522, o pino digital D8

do ESP8266 ligado ao pino de *select slave* do leitor RC 522, o pino digital D5 do ESP8266 ligado ao pino de SCK do leitor RC 522, o pino digital D6 do ESP8266 ligado ao pino MISO do leitor RC 522, o pino digital D7 do ESP8266 ligado ao pino de MOSI do leitor RC 522, seguindo a alimentação de 3,3 V, conforme figura 36.

Figura 36: Diagrama de Ligação ESP8266 e leitor RC522



Fonte: Retirado do site technologytourist.com (2020)

Na transmissão de dados via SPI, existe um único mestre (ESP8266) e vários outros leitores (RC522), de modo que o mestre escolhe um escravo para se comunicar usando o sinal /SS ou em algumas placas também escrito SDA, que é ativo em nível baixo. O SPI é formado por quatro sinais que são: SCK, /SS, MISO e MOSI, quando é iniciada a comunicação, o mestre gera o sinal de "*clock*" (SCK) e o escravo recebe este sinal.

A transferência de dados é de modo *full duplex*, ou seja, dados fluem do mestre para o escravo pelo MOSI e do escravo para o mestre pelo MISO. Durante o processo, o leitor RC522 solicita um sinal de controle vindo do ESP8266 que é o *reset* e este sinal será supervisionado pelo pino GPIO 0 (pino digital D3).

Uma vantagem em trabalhar com protocolo SPI está no fato de utilizar uma comunicação mais rápida quando comparada a outros protocolos, como por exemplo, o I2C que trabalha apenas com dois fios e não em *full duplex*, em contrapartida como desvantagem temos que mapear/configurar mais pinos no ESP8266, tendo suporte de apenas um único mestre no circuito projetado e, nenhum protocolo de verificação de erros sendo definido nele.

4 RESULTADOS

A utilização do leitor RFID RC522 para testes e simulações neste projeto foi de fundamental importância, pois a partir da programação do ESP8266, otimizou-se as bibliotecas e linhas editadas através da linguagem de programação orientada a objetos, possibilitou a implementação deste projeto para qualquer tipo de leitor, desde que configurado os leitores RFID corretamente, quer seja de painel ou portal, verificando a capacidade de alimentação do circuito proposto.

A implementação da gravação na memória EEPROM (4096 *bytes*) do ESP8266 foi uma solução encontrada nos casos em que falte WiFi, pois os dados serão gravados com segurança e rapidez nesta memória, comparando-os com o banco de dados enquanto conectado com a rede WiFi.

Pelo fato de utilizar este leitor RFID proposto, não temos sinal de controle para sabermos se teremos conflitos nos dados em tráfego, mas é possível verificar pelo sinal presente nele chamado DAS (SS), no qual apontamos para este dispositivo como escravo, ou seja, não perdendo a referência de apontamento na hora da transmissão dos dados.

Em relação à interferência eletromagnética de um sistema RFID, com *tags* na frequência de operação de 13,56 MHz, não foram efetuadas simulações com estas etiquetas coladas em carcaças de metal ou plástico, pelo fato de não termos o portal.

Demais testes na página *web* não foram efetuados devido à conclusão da mesma, pois está sendo desenvolvida para o curso de Engenharia Eletrônica e será vinculada ao projeto. Assim como acesso ao banco de dados implementado nesta página *web*, possibilitando cadastro das *tags* e usuários.

Como resultados e testes com o ESP8266 e o leitor RFID RC522, várias leituras foram efetuadas em *tags* na frequência de 13,56 MHz, cadastradas no sistema, conectado ao WiFi e retornando *tags* cadastradas. A captura de tela do computador acessando a página *web* em construção é apresentada na figura 37, sendo visualizado o menu relatório, contendo dia e hora que ocorreu a leitura da *tag*, número da *tag* lida e material correspondente ao cadastro. Nota-se que neste relatório não está vinculando nenhuma *tag* a qualquer usuário cadastrado no

sistema, mostrando apenas leitura e horários de disparo do alarme, assim como equipamento correspondente.

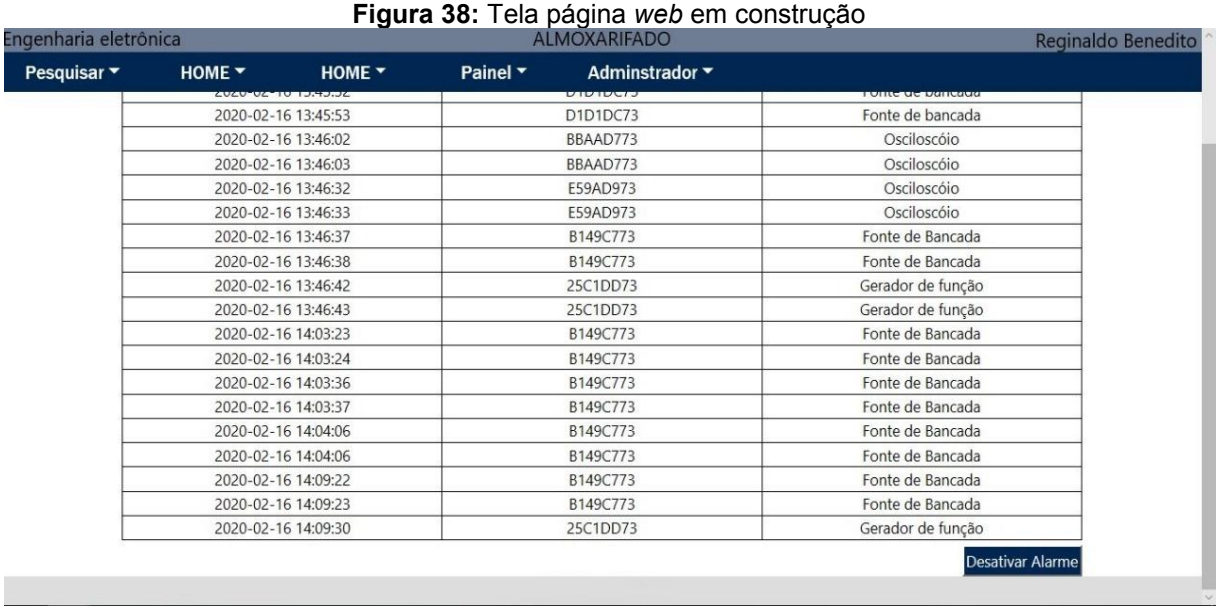
Figura 37: Teste leitura *tags* com conexão ao banco de dados

Dia e hora	TAG	Equipamento
2020-02-16 13:42:36	91A0CC73	Gerador de função
2020-02-16 13:43:19	D1D1DC73	Fonte de bancada
2020-02-16 13:45:49	D1D1DC73	Fonte de bancada
2020-02-16 13:45:50	D1D1DC73	Fonte de bancada
2020-02-16 13:45:52	D1D1DC73	Fonte de bancada
2020-02-16 13:45:53	D1D1DC73	Fonte de bancada
2020-02-16 13:46:02	BBAAD773	Osciloscóio
2020-02-16 13:46:03	BBAAD773	Osciloscóio
2020-02-16 13:46:32	E59AD973	Osciloscóio
2020-02-16 13:46:33	E59AD973	Osciloscóio
2020-02-16 13:46:37	B149C773	Fonte de Bancada
2020-02-16 13:46:38	B149C773	Fonte de Bancada
2020-02-16 13:46:42	25C1DD73	Gerador de função
2020-02-16 13:46:43	25C1DD73	Gerador de função
2020-02-16 14:03:23	B149C773	Fonte de Bancada
2020-02-16 14:03:24	B149C773	Fonte de Bancada
2020-02-16 14:03:36	B149C773	Fonte de Bancada
2020-02-16 14:03:37	B149C773	Fonte de Bancada
2020-02-16 14:04:06	B149C773	Fonte de Bancada

Fonte: Autoria própria (2020).

Foi implementado a possibilidade de desligar o sistema de alarme quando disparado. Esta funcionalidade está presente, acessando a página *web* e clicando no botão “Desativar Alarme” no canto inferior direito, dentro do menu relatório conforme figura 38.

Figura 38: Tela página *web* em construção



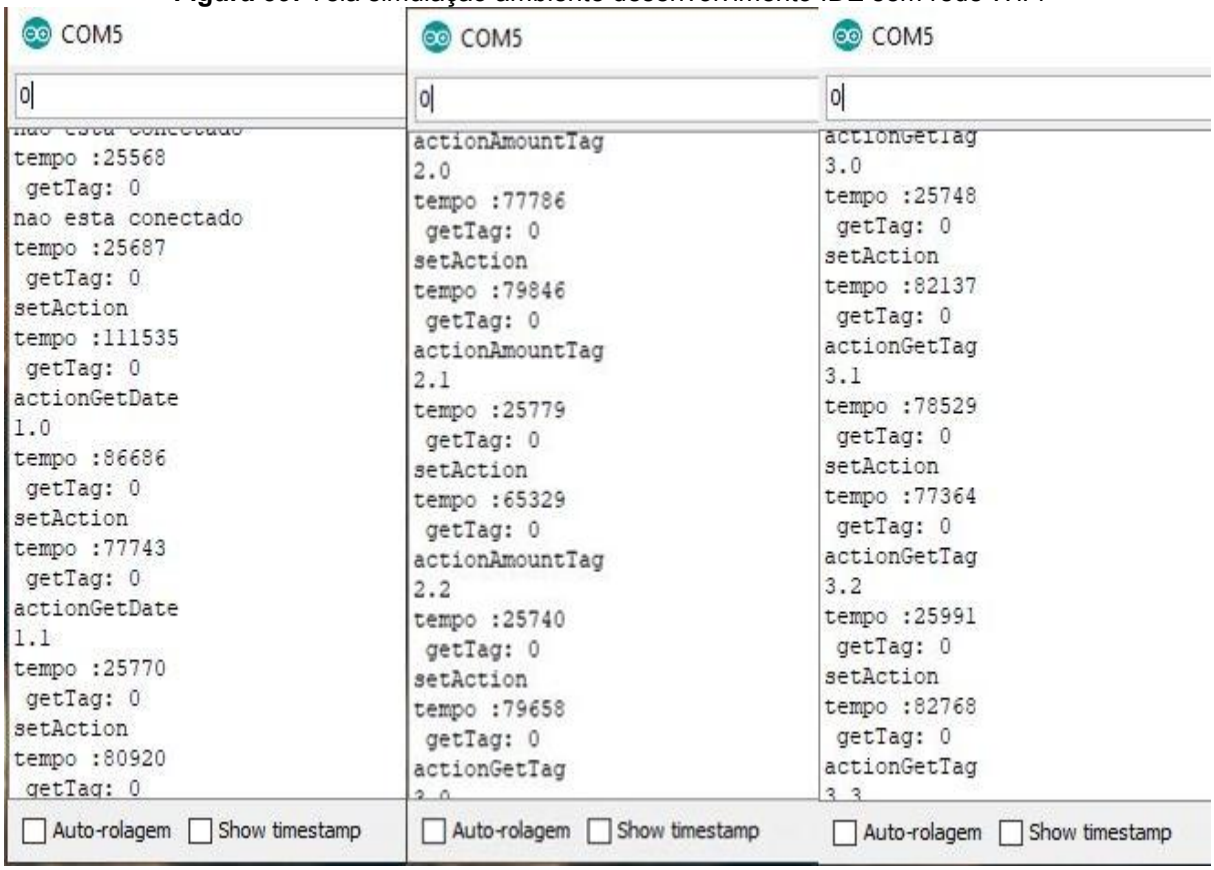
2020-02-16 13:45:53	D1D1DC73	Fonte de bancada
2020-02-16 13:46:02	BBAAD773	Osciloscóio
2020-02-16 13:46:03	BBAAD773	Osciloscóio
2020-02-16 13:46:32	E59AD973	Osciloscóio
2020-02-16 13:46:33	E59AD973	Osciloscóio
2020-02-16 13:46:37	B149C773	Fonte de Bancada
2020-02-16 13:46:38	B149C773	Fonte de Bancada
2020-02-16 13:46:42	25C1DD73	Gerador de função
2020-02-16 13:46:43	25C1DD73	Gerador de função
2020-02-16 14:03:23	B149C773	Fonte de Bancada
2020-02-16 14:03:24	B149C773	Fonte de Bancada
2020-02-16 14:03:36	B149C773	Fonte de Bancada
2020-02-16 14:03:37	B149C773	Fonte de Bancada
2020-02-16 14:04:06	B149C773	Fonte de Bancada
2020-02-16 14:04:06	B149C773	Fonte de Bancada
2020-02-16 14:09:22	B149C773	Fonte de Bancada
2020-02-16 14:09:23	B149C773	Fonte de Bancada
2020-02-16 14:09:30	25C1DD73	Gerador de função

Fonte: Autoria própria (2020).

São apresentados nas figuras 39 a 42 os resultados das simulações no ambiente de desenvolvimento IDE, telas capturadas no mesmo instante da geração de telas anteriores com página *web*, percebe-se que funções e sub funções funcionam perfeitamente, com tempo decorrido de processamento no ESP8266 eficiente e rapidez do código implementado. Nas telas de simulação percebe-se que a prioridade do sistema é a leitura das *tags*, vistos em determinados momentos, leituras de *tags* em duplicidade, justificando a implementação do código orientado a objeto, podendo dizer que o sistema implementado faz execução do código, lê *tag*, executa novamente e volta a leitura antes de executar outras funções.

Na figura 39 percebe-se a execução do código implementado ao sistema proposto, funções e sub funções em sequência, tempo entre funções muito rápidas, priorizando sempre a leitura da *tag*. Nesta tela de simulação o ESP8266 ainda não se encontra conectado a rede WiFi, caracterizando nossa pior situação do sistema de segurança e mesmo assim tentando fazer as leituras das *tags* por meio do leitor RFID RC522.

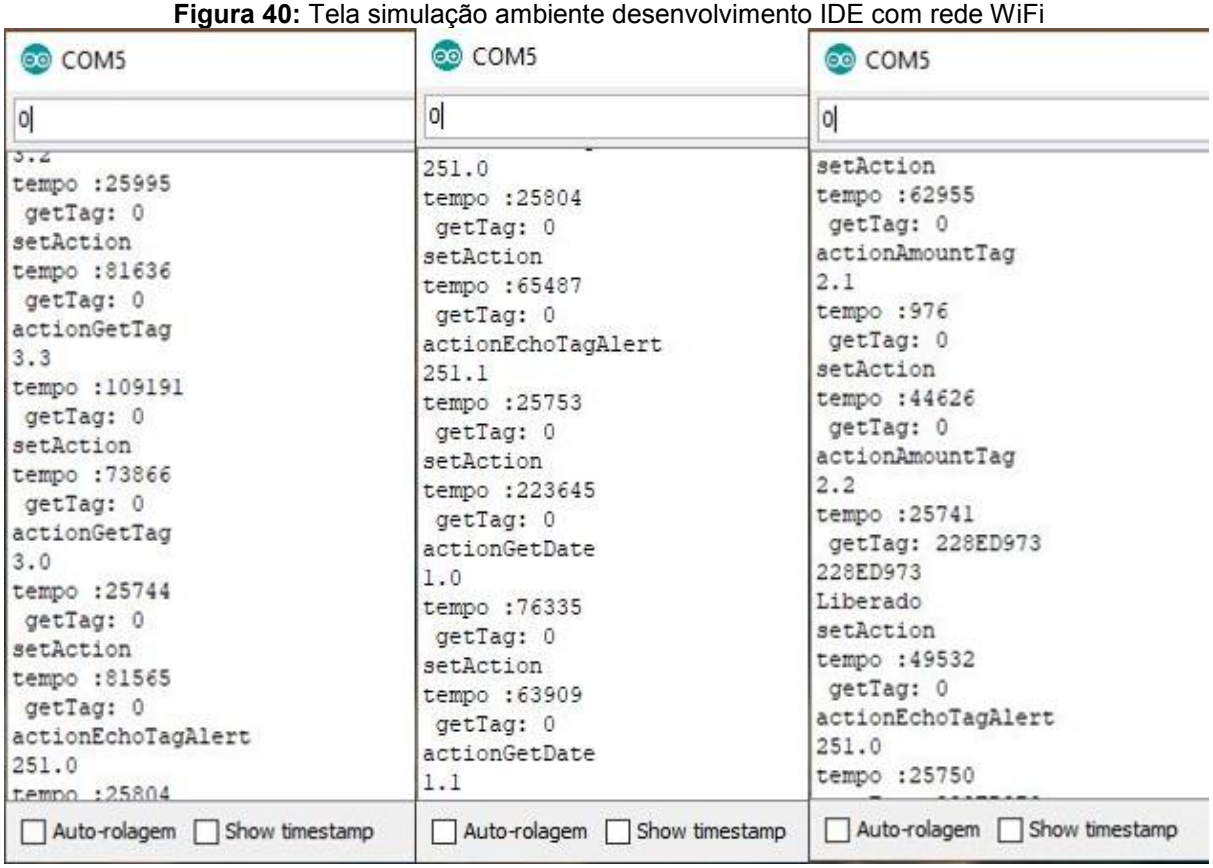
Figura 39: Tela simulação ambiente desenvolvimento IDE sem rede WiFi



Fonte: Autoria própria (2020).

Na figura 40 percebe-se que o ESP8266 conectou-se a rede WiFi, efetuou a leitura de uma *tag* cadastrada no sistema como liberada, preparou-se para uma nova leitura e não disparou o alarme.

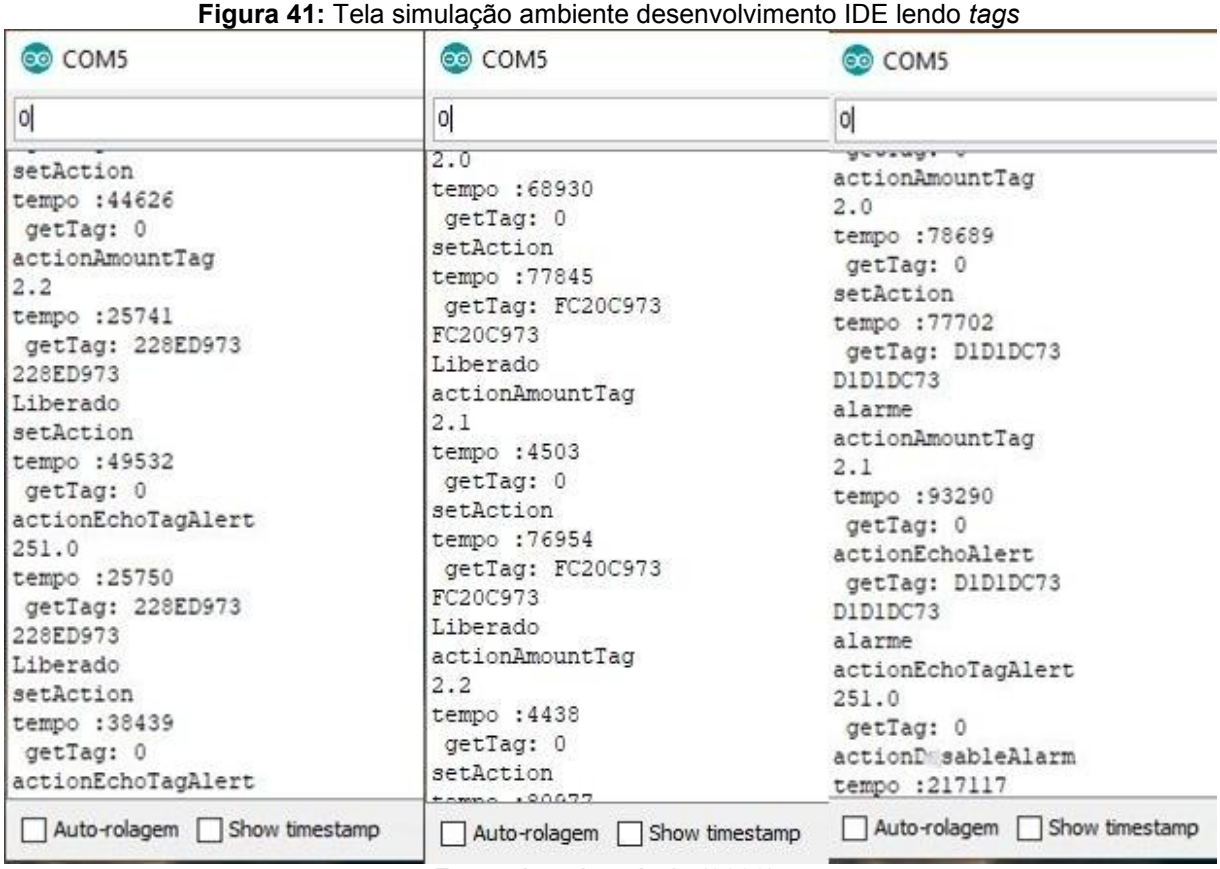
Figura 40: Tela simulação ambiente desenvolvimento IDE com rede WiFi



Fonte: Autoria própria (2020).

Na figura 41 percebe-se a leitura de várias *tags* liberadas ou não, execução do código em *loop*, ou seja, executando funções e sub funções, deixando claro que o sistema proposto a prioridade será sempre a execução da leitura das *tags*, indiferente do tempo percorrido.

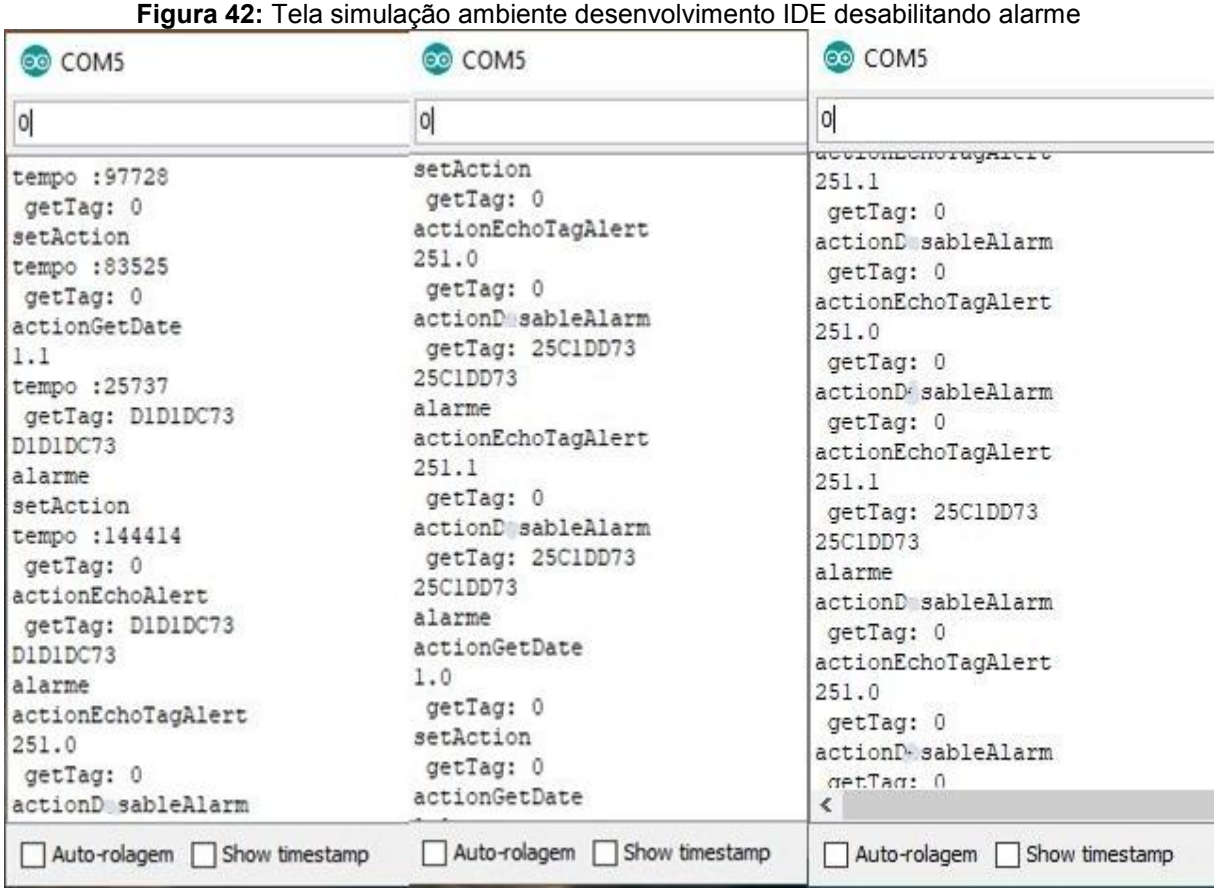
Figura 41: Tela simulação ambiente desenvolvimento IDE lendo *tags*



Fonte: Autoria própria (2020).

Na figura 42 percebe-se as leituras das *tags* por meio do leitor RFID RC522, disparando o alarme para *tags* não cadastradas, chamada de uma ação para desabilitar o alarme do sistema de segurança e continuando o processo de leitura de outras *tags* que por ventura passem pelo leitor RFID.

Figura 42: Tela simulação ambiente desenvolvimento IDE desabilitando alarme



Fonte: Autoria própria (2020).

Para simulação de telas anteriores, foram cadastradas *tags* mencionadas na figura 43 a seguir como liberadas pelo sistema implementado, ou seja, elas não dispararam o alarme nos testes.

Figura 43: *Tags* cadastradas no banco de dados para simulação

id	id_usuario	TAG
1	1	FC20C973
2	1	228ED973

Fonte: Autoria própria (2020).

5 CONSIDERAÇÕES FINAIS

A ideia de usar o ESP8266 neste projeto foi muito válida no sentido da relação custo/benefício, pela facilidade de uso e implementação em qualquer local que tenha acesso WiFi.

Um fator interessante é que se pode utilizar mais de um leitor RFID, devido à comunicação SPI, respeitando a capacidade de alimentação do circuito proposto.

A proposta de utilização da memória EEPROM, utilizando sistema de arquivos e não de cartão de memória FLASH, se deu também pela facilidade de programação e ainda, pela capacidade do número de vezes em que ela pode ser gravada, em torno de 10.000 gravações em cada posição de memória, elevando a vida útil do sistema por vários anos com o mesmo equipamento. Lembrando ainda, que o número de leituras da EEPROM é infinita, apenas escrita possui um limite.

O principal objetivo deste projeto foi alcançado, com o desenvolvimento de um sistema RFID que armazena as informações referentes aos equipamentos patrimoniados, dentro do almoxarifado do DAELN, utilizando programação orientada a objetos nas bibliotecas, facilitando futuras alterações no sistema, visto que podemos adicionar apenas uma classe para mudanças no sistema, sem alterar o programa principal.

A futura implementação deste sistema, contribuirá para instituições públicas, pois permitirá uma maior segurança dos bens patrimoniados em questão, assim como facilitará o trabalho aos encarregados pelo inventário patrimonial, fornecendo relatórios mais precisos.

Como sugestão para futuros trabalhos, fica a sugestão:

- Desenvolvimento página *web*, acesso aos usuários/alunos da UTFPR com maiores informações sobre a quantidade de equipamentos no almoxarifado do DAELN, filtrando os que estão presentes e emprestados;
- Melhorar o sistema de relatórios, vinculando *logs* com imagens de câmeras, unindo-os em arquivos únicos (data/hora, foto, vídeo);
- Substituir leitor RFID por painel em forma de portal, com frequência mais alta (UHF), de forma a conseguir ler mais *tags* simultaneamente, uma vez que o desenvolvimento das bibliotecas foi orientado a objetos, ficando mais fácil ainda sua implementação;

- Vincular disparos de alarme do sistema de segurança pela página *web*, informando usuário/administrador do sistema por SMS instantaneamente, ou ainda por aplicativo similar;
- Melhorar sistema de criptografia e segurança do sistema proposto, uma vez que este funciona com WiFi.

REFERÊNCIAS BIBLIOGRÁFICAS

ARDUINO. Disponível em: http://www.arduino.cc/. Acesso em: 10 ago. 2018.

BALLOU, Ronald H. **Gerenciamento da cadeia de suprimentos: planejamento, organizações e logística empresarial**. 4ª ed. São Paulo: BOOKMAN, 2001.

BERNARDO, Cláudio G. **A tecnologia RFID e os benefícios da etiqueta inteligente para os negócios**. Revista Eletrônica Unibero de Produção Científica, São Paulo, set. 2004. Disponível em: http://www.unibero.edu.br/download/revistaeletronica/Set04_Artigos/A%20Tecnologia%20RFID%20-%20BSI.pdf. Acesso em: 10 ago. 2018.

BERTOGNA, Eduardo G. **Microcontroladores AVR teoria e prática: baseado no ATmega8515.** 1ª ed. Curitiba: Edição do Autor, 2014.

BRADY JR, William D. **Managing Fixed Assets in the Public Setor: Managing for Service Excellence**. 1ª ed. USA: Universal Publishers, 2001.

BROWN, D. **RFID Implementation.** 2ª ed. USA: Editora McGraw-Hill, 2006.

DATE, C. J. **An Introduction to Database Systems**. 8ª ed. London: Pearson, 2004.

DEITEL, H.M. **Java: como programar**. 6ª ed. São Paulo: Pearson, 2005.

DOBKIN, Daniel. **The RF in RFID - Passive UHF RFID in Practice**. 1ª ed. Boston: Elsevier, 2008.

DRESCH JR, Antônio; EFROM, Danny R; GRUMOVSKI, Dieison. **Sistema de Controle de Patrimônio via RFID.** E-Tech. Atualidades Tecnológicas para a Competitividade Industrial. Florianópolis, v. 1, nº 1, 2008.

FINKENZELLER, Klaus. **RFID handbook**. 3ª ed. USA: Wiley, 2010.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5ª ed. São Paulo: Atlas, 2008.

GIMENEZ, Salvador P. **Microcontroladores 8051**. 1ª ed. São Paulo: Pearson, 2005.

GLOVER, Bill e BHATT, Himanshu. **Fundamentos de RFID: Teoria em Prática**. 1ª ed. Rio de Janeiro: Alta Books, 2007.

GOMES, Hugo M. Cravo. **Fundamentos de metodologia científica**. 6ª ed. São Paulo: Atlas, 2005.

JUNIOR, Joel A. **Monografias.com.** Dezembro 2007. Disponível em: http://br.monografias.com/trabalhos3/rfid-identificacao-radiofrequencia/rfid-identificacao-radiofrequencia3.shtml. Acesso em: 14 nov. 2018.

KIM, J.; YU, B.; LEE, H.; PARK, J.: **RFID tag antenna mountable on metallic plates.** Asia Pacific Microwave Conference, v. 4, 2005.

LEENS, F. **An introduction to I2C and SPI protocols.** IEEE Instrumentation and Measurement Magazine. v. 12, nº 1, 2009.

MANITEL, P. **O guia básico de uso das GPIOs do ESP8266.** 2016. Disponível em: http://pedrominatel.com.br/pt/esp8266/o-guia-basico-de-uso-das-gpios-do-esp8266/. Acesso em: 10 nov. 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 6ª ed. São Paulo: Atlas, 2005.

MEC. **Sistema de Administração de Patrimônio das IFES**. Brasília: SESU, 1994.

MOURA, Reinaldo A. **RFID: 10 anos depois, Intra Logística movimentação e armazenagem de materiais.** São Paulo, nº 269, 2013.

NOGUEIRA FILHO, Cícero Casemiro da Costa. **Tecnologia RFID aplicada à Logística**. Rio de Janeiro, 2005.103 f. Dissertação (Mestrado em Engenharia Industrial). Pontifícia Universidade Católica do Rio de Janeiro. Rio de Janeiro, 2005.

O'BRIEN, James A. **Sistemas de Informação e as decisões gerenciais na era da Internet**. 2ª ed. São Paulo: Editora Saraiva, 2004.

OLIVEIRA, Ricardo R. **Uso do microcontrolador ESP8266 para automação residencial**. 2017. 55 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Controle e Automação) Universidade Federal do Rio de Janeiro, Escola Politécnica, 2017. Disponível em: http://monografias.poli.ufrj.br/monografias/monopoli10019583.pdf. Acesso em: 18 ago. 2018.

PINHEIRO, José Mauricio Santo. **RFID: Identificação por Rádio frequência**, 2004. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radio_frequencia.php. Acesso em: 10 ago. 2018.

PRESSMAN, Roger S. **Engenharia de Software: Uma Abordagem Profissional .** 8ª ed. São Paulo: Editora Amgh, 2016.

RFID JOURNAL. **Glossary of RFID Terms.** Disponível em: https://www.rfidjournal.com/glossary/. Acesso em: 20 nov. 2018.

RFID JOURNAL BRASIL. **Perguntas Frequentes.** Disponível em: http://brasil.rfidjournal.com/perguntas-frequentes. Acesso em: 19 nov. 2018.

SANTANA, Sandra Regina Matias. **RFID: Identificação por Radio Frequência**. Disponível em: http://www.wirelessbrasil.org/wirelessbr/colaboradores/sandra_santana/rfid_01.html. Acesso em: 10 ago. 2018.

SANTINI, Arthur Gambin. **RFID: Conceitos, Aplicabilidade e Impactos**. 1ª ed. Rio de Janeiro: Ciência Moderna, 2008.

SANTOS, Gerson dos. **Gestão Patrimonial**. 1ª ed. Florianópolis: Secco, 2010.

ŠKRABA, A. **Prototype of group heart rate monitoring with NODEMCU ESP8266.** MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING. 2016. Disponível em: http://ieeexplore.ieee.org/stamp/stamp.jsp?ar number=7977151. Acesso em: 11 ago. 2018.

TAUFENBACH, Sérgio Luiz Dalcastagne. **RFID: Identificação por Radiofrequência a Etiqueta Inteligente.** Revista de divulgação técnico-científica do ICPG, Santa Catarina, v. 2, nº 7, 2004.

TORRES JÚNIOR, Fabiano; SILVA, Lino Martins. **A importância do controle contábil e extra contábil dos bens permanentes adquiridos pela administração pública federal**. Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ. Rio de Janeiro, v. 8, nº 2, 2003. Disponível em: http://www.e-publicacoes.uerj.br/index.php/rcmccuerj/article/view/5596. Acesso em: 10 ago. 2018.

UTFPR**. Regimento Geral da UTFPR**. 2009. Disponível em: http://www.utfpr.edu.br/a-instituicao/documentos-institucionais/regimento-geral. Acesso em: 10 ago. 2018.

WANT, R. **An Introduction to RFID Technology**. IEEE Pervasive Computing, v. 5, nº 1, jan-mar, 2006.