



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
CAMPUS PAU DOS FERROS
DEPARTAMENTO DE ENGENHARIAS E TECNOLOGIA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

BIANCA STEPHANIE GUIMARÃES MORAIS

**SISTEMA DE CONTROLE DE ACESSO UTILIZANDO TECNOLOGIA RFID -
GPACCESS**

PAU DOS FERROS – RN

2020

BIANCA STEPHANIE GUIMARÃES MORAIS

**SISTEMA DE CONTROLE DE ACESSO UTILIZANDO TECNOLOGIA RFID -
GPACCESS**

Trabalho de conclusão de curso apresentado
à Universidade Federal Rural Do Semi-Árido
como parte das exigências para a obtenção do título de bacharel em Engenharia de Computação.

Orientadora: Profa. Dra. Veronica Maria
Lima Silva

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei nº 9.279/1996 e Direitos Autorais: Lei nº 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

M827s Morais, Bianca Stephanie Guimarães.
 SISTEMA DE CONTROLE DE ACESSO UTILIZANDO
 TECNOLOGIA RFID - GPACCESS / Bianca Stephanie
 Guimarães Morais. - 2020.
 49 f. : il.

 Orientadora: Veronica Maria Lima Silva.
 Monografia (graduação) - Universidade Federal
 Rural do Semi-árido, Curso de Engenharia de
 Computação, 2020.

 1. RFID. 2. Sistema Embarcado. 3. Sistema Web.
 4. Automação. 5. Controle de Acesso. I. Silva,
 Veronica Maria Lima, orient. II. Título.

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC's) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

BIANCA STEPHANIE GUIMARÃES MORAIS

**SISTEMA DE CONTROLE DE ACESSO UTILIZANDO TECNOLOGIA RFID -
GPACCESS**

Trabalho de conclusão de curso apresentado
à Universidade Federal Rural Do Semi-Árido
como parte das exigências para a obtenção do tí-
tulo de bacharel em Engenharia de Computação.

Aprovada em: 10 / 12 / 2020

BANCA EXAMINADORA

**VERONICA MARIA
LIMA
SILVA:02558212397**

Assinado de forma digital por
VERONICA MARIA LIMA
SILVA:02558212397
Dados: 2020.12.12 10:54:55
-03'00'

Profa. Dra. Veronica Maria Lima Silva – UFERSA

**LENARDO CHAVES
E
SILVA:67090680304**

Assinado de forma digital por
LENARDO CHAVES E
SILVA:67090680304
Dados: 2020.12.12 18:42:34
-03'00'

Prof. Dr. Lenardo Chaves e Silva – UFERSA
Membro Examinador

**REUDISMAM ROLIM DE
SILVA:08392843495**

Assinado de forma digital por
REUDISMAM ROLIM DE
SILVA:08392843495
Dados: 2020.12.12 10:58:14 -03'00'

Prof. Dr. Reudismam Rolim de Sousa – UFERSA
Membro Examinador

Dedico esse trabalho aos meus pais, Antonio Wilton de Moraes Junior, Naiana Narrechy Guimarães Moraes e ao meu irmão Arthur Wilton Guimarães Moraes.

Dedico aos meus avós Ivanilde Carlos de Oliveira (In Memoriam) e Nilton Rosado Guimarães (In Memoriam).

AGRADECIMENTOS

Agradeço a Deus, por ter me dado a dádiva da vida e forças para trilhar o meu caminho, por todas as bênçãos que obtive e estou obtendo.

Agradeço aos meus pais, Antonio Wilton de Moraes Junior e Naiana Narrechy Guimarães Moraes, por toda compreensão, amor, carinho, ensinamentos e apoio durante essa caminhada e na vida, sem vocês nada disso teria sido possível. Agradeço por serem pais excelentes, por nunca me deixarem faltar nada e por terem acreditado em mim. A força de vocês criaram proporções na minha vida nas quais eu achei que nunca chegaria. Agradeço por comemorarem, comigo e por mim, todas as vitórias, desde as mais simples as maiores, todas as minhas conquistas são por vocês.

Agradeço a minha avó Ivanilde Carlos de Oliveira que nos primeiros anos desse curso esteve rezando e cuidando de mim e agora ela cuida de mim do céu, tenho certeza que a senhora está feliz e comemorando onde estiver, essa conquista, em especial, eu dedico a senhora. Agradeço a minha avó Maria de Lourdes Siqueira por todo amor, carinho, apoio e cuidado, que reza sempre por mim, essa conquista também é pela senhora.

Agradeço a professora doutora Veronica Maria Lima Silva, que esteve no papel de orientadora, professora, amiga e, também, de mãe de coração. Agradeço pelas conquistas que me ajudou a obter, pelos ensinamentos, cuidado, companheirismo e apoio. A senhora foi uma excelente orientadora. Muito obrigado por tudo!

Agradeço aos docentes do curso de Engenharia de Computação, em especial, Cecílio Martins de Souza Neto e Francisco Carlos Gurgel da Silva Segundo por terem sido, além de grandes mestres, amigos que me ajudaram muito durante essa caminhada. Obrigado por tudo!

Agradeço aos discentes do curso de Engenharia de Computação, meus amigos, minha segunda família, obrigado por tudo!

Agradeço aos amigos e amigas, pela torcida, amizade e companheirismo, vocês estão no meu coração!

Agradeço a Universidade Federal Rural do Semi-Árido por todo o aparato para que eu pudesse obter o conhecimento durante essa caminhada.

Agradeço ao Grupo de Pesquisa em Sistema Críticos de Segurança (GPSiCS) por acreditarem nesse projeto e ceder o seu espaço para a criação e evolução desse trabalho.

Obrigado a todos que contribuíram direta e indiretamente para a conclusão desse trabalho.

RESUMO

Neste trabalho é apresentado o desenvolvimento de um sistema de controle de acesso a ambientes públicos, utilizando Identificação por Radiofrequência (RFID) e Comunicação Sem Fio (*wireless*), com aplicação no laboratório do grupo de Pesquisa em Sistemas Críticos de Segurança (GPSiCS), localizado na Universidade Federal Rural do Semi-Árido (UFERSA), Centro Multidisciplinar de Pau dos Ferros. No laboratório do GPSiCS não há registro de controle de utilização. Desta forma, tendo em vista a preocupação de se zelar pelo ambiente e pelos materiais nele dispostos, a implementação de um sistema de controle automatizado é de fundamental importância para a integridade do local e dos seus usuários. O sistema de controle de acesso GPACCESS (acrônimo de Acesso a Grupo de Pesquisa) tem como objetivo resolver esta problemática. O sistema GPACCESS é composto por um sistema embarcado e um sistema *web*. O sistema *web* é uma aplicação que utiliza as linguagens Node.js e React.js, o qual atende aos requisitos funcionais e não funcionais levantados a partir das necessidades dos coordenadores do laboratório, como a exibição de um relatório de acesso, cadastro dos usuários, entre outras. O sistema embarcado é formado por componentes integrados e de baixo custo, tendo como principal função identificar por meio da leitura de uma *tag* RFID os usuários que efetuam ao acesso o ambiente controlado. Dentre os componentes utilizados pode-se destacar a antena RFID (leitor), o NodeMCU ESP8266 (microcontrolador com módulo Wi-Fi) e um relé para acionamento de uma carga, como, por exemplo, uma fechadura elétrica. O sistema embarcado se comunica via Wi-Fi com o sistema *web* para registro dos acessos e liberação do acesso ao ambiente somente para usuários cadastrados. O sistema atendeu a todos os requisitos especificados com êxito. Este trabalho pode ser utilizado como base para desenvolvimento de aplicações de controle de acesso para ambientes públicos de maneira geral.

Palavras-chave: RFID. Sistema Embarcado. Sistema *Web*. Automação. Controle de Acesso.

ABSTRACT

This work presents the development of an access control system to public environments, using Radio Frequency Identification (RFID) and Wireless Communication with application in the Laboratory of the Research Group on Critical Security Systems (GPSiCS), located at the Federal Rural University of Semi-Árido (UFERSA), Multidisciplinary Center of Pau dos Ferros. In the GPSiCS laboratory there is no record of use control. Thus, in view of the concern with care for the environment and the materials disposed in it, the implementation of an automated control system is of fundamental importance for the integrity of the place and its users. The access control system GPACCESS (acronym for Access to Research Group) aims to solve this problem. The GPACCESS system consists of an embedded system and a web system. The web system is an application that uses the languages Node.js and React.js, which takes into account the functional and non-functional requirements raised from the needs of the laboratory coordinators, such as displaying an access report, user registration, among others. The embedded system consists of low-cost and integrated components, whose main function is to identify users who access the controlled environment by reading an RFID tag. Among the components used can be highlighted the RFID antenna (reader), the NodeMCU ESP8266 (microcontroller with Wi-Fi module) and a relay for driving a load, such as, for example, an electric lock. The embedded system communicates via Wi-Fi with the web system to register access and release access to the environment only for registered users. The system has successfully met all specified requirements. This work can be used as a basis for the development of access control applications for public environments in general.

Keywords: RFID. Embedded Systems. Web System. Automation. Access Control.

LISTA DE ILUSTRAÇÕES

Figura 1 – Visão Geral do Sistema de Controle de Acesso GPACCESS	15
Figura 2 – <i>Kit</i> Módulo RFID	18
Figura 3 – Arduino UNO R3	19
Figura 4 – NodeMCU ESP8266 Lolin V3	20
Figura 5 – Proposta de Sistema	23
Figura 6 – Tela de <i>Login</i>	27
Figura 7 – Tela de Cadastro	28
Figura 8 – Tela de Recuperação de senha	28
Figura 9 – Menu Inicial	29
Figura 10 – Módulo de Gerenciamento de Usuários	29
Figura 11 – Tela de Edição de Dados	30
Figura 12 – Modelo Lógico do Banco de Dados do GPACCESS	32
Figura 13 – <i>Sketch</i> do <i>Hardware</i>	33
Figura 14 – Tela de <i>Login</i> (Versão Final)	35
Figura 15 – Tela de Cadastro (Versão Final)	35
Figura 16 – Tela de Recuperação de Senha (Versão Final)	36
Figura 17 – Tela Inicial (Versão Final)	37
Figura 18 – Tela de Gerenciamento de Usuários (Versão Final)	37
Figura 19 – Tela de Atualização de Dados (Versão Final)	38
Figura 20 – Tela de Cadastro de <i>TAG</i> (Versão Final)	39
Figura 21 – Tela de Perfil (Versão Final)	39
Figura 22 – Modelo de Relatório (Versão Final)	40
Figura 23 – Fluxograma do Funcionamento do Arduino	41
Figura 24 – Fluxograma do Funcionamento do ESP8266	42
Figura 25 – Protótipo de <i>Hardware</i> Final	43
Figura 26 – Fluxograma do Cadastro de Usuários	44
Figura 27 – Fluxograma do Cadastro de <i>Tag</i>	45
Figura 28 – Fluxograma da Geração de Relatórios	46

LISTA DE TABELAS

Tabela 1 – Requisitos Funcionais do Administrador	26
Tabela 2 – Requisitos Funcionais do Usuário	26
Tabela 3 – Requisitos Não-Funcionais	26

LISTA DE SIGLAS E ABREVIATURAS

API	<i>Application Programming Interface</i>
DC	<i>Direct Current</i>
GPIOs	<i>General-purpose input/output</i>
GSM	<i>Global System for Mobile</i>
GUI	<i>Graphical User Interface</i>
I2C	<i>Inter-Integrated Circuit</i>
LCD	<i>Liquid Crystal Display</i>
PDF	<i>Portable Document Format</i>
RAM	<i>Random Access Memory</i>
RFID	<i>Radio Frequency Identification</i>
SMS	<i>Short Message Service</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
USB	<i>Universal Serial Bus</i>

SUMÁRIO

1	INTRODUÇÃO	14
1.1	OBJETIVOS	15
1.1.1	Objetivo Geral	15
1.1.2	Objetivos Específicos	15
1.2	ESTRUTURA DO TRABALHO	16
2	FUNDAMENTAÇÃO TEÓRICA	17
2.1	<i>RADIO FREQUENCY IDENTIFICATION</i> (RFID)	17
2.2	ARDUINO	18
2.3	NODEMCU - ESP8266	19
2.4	SISTEMAS EMBARCADOS	20
3	TRABALHOS RELACIONADOS	22
3.1	RFID-INITIATED WORKFLOW CONTROL TO FACILITATE PATIENT SAFETY AND UTILIZATION EFFICIENCY IN OPERATION THEATER	22
3.2	RFID BASED ACCESS CONTROL AND REGISTRATION SYSTEM . . .	22
3.3	A DIGITAL SECURITY SYSTEM WITH DOOR LOCK SYSTEM USING RFID TECHNOLOGY.	23
3.4	RFID BASED SECURITY AND ACCESS CONTROL SYSTEM	24
3.5	CONTRIBUIÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO	24
4	METODOLOGIA	25
4.1	SISTEMA <i>WEB</i>	25
4.1.1	Requisitos Funcionais	26
4.1.2	Requisitos Não-Funcionais	26
4.1.3	Protótipação de Telas	27
4.1.4	Banco de Dados	30
4.2	SISTEMA EMBARCADO	32
5	RESULTADOS E DISCUSSÕES	34
5.1	SISTEMA <i>WEB</i>	34
5.1.1	Modelo Final GPACCESS	34
5.2	SISTEMA EMBARCADO	40
5.2.1	Funcionamento do Arduino	41
5.2.2	Funcionamento do ESP8266	41

5.2.3	Protótipo Final	43
5.3	FUNCIONAMENTO DO SISTEMA	43
5.3.1	Cadastro de Usuário	44
5.3.2	Cadastro de <i>Tags</i>	44
5.3.3	Gerar Relatório	45
6	CONCLUSÃO	47
	REFERÊNCIAS	48

1 INTRODUÇÃO

Ambientes públicos em algumas universidades no Brasil, tais como laboratórios, salas de aulas, salas de equipamentos de rede, entre outros, em sua maioria, não possuem controle de acesso automático. Em especial na Universidade Federal Rural do Semi-Árido (UFERSA), Centro Multidisciplinar de Pau dos Ferros, o controle de acesso dos laboratórios de pesquisa é realizado por meio da distribuição de chaves aos discentes e docentes associados, como também o acesso dos profissionais terceirizados. O controle normalmente é realizado da seguinte forma: as pessoas que têm o acesso, munidas da chave, podem utilizar o ambiente dentro do horário permitido para transitar dentro da universidade. Concentrando-se na rotina de um laboratório de pesquisa, a ausência de controle e/ou registro de acesso ocasiona problemas como: o acesso de pessoas não associadas ao grupo de pesquisa, que podem estar acompanhando os associados. Além disso, o fato do laboratório possuir dispositivos eletrônicos caros que são disponibilizados pela universidade, sendo assim, necessários de um cuidado especial, também é um fator motivador para a existência de um controle de acesso mais rigoroso. Um sistema de controle automatizado pode, portanto, fornecer informações claras sobre a utilização do local em situações de violação do código de conduta para o uso do ambiente. Diante dessa problemática, neste trabalho foi desenvolvido um sistema de controle de acesso automatizado a ser aplicado em ambientes públicos, especialmente, laboratórios de pesquisa.

De uma maneira geral, o sistema proposto visa controlar e registrar o acesso dos usuários, promovendo uma maior segurança ao ambiente utilizado. Dessa forma é possível ter dados como o horário que cada usuário utilizou a sala em determinada situação, como também extrair informações do tipo: maior e menor pico de atividade, melhor horário para estudo no ambiente, entre outras. Além das vantagens já citadas, o sistema desenvolvido permite um melhor aproveitamento do ambiente pelos coordenadores do laboratório, proporcionando a visibilidade dos dados para ações efetivas dentro do mesmo, como, por exemplo, a organização de horários de utilização, definição dos horário de reuniões, entre outras.

O sistema de controle de acesso desenvolvido é composto por um sistema embarcado que se comunica via Wi-Fi com um sistema *web*. O sistema embarcado tem como funções principais identificar o usuário e liberar o acesso ao ambiente. Para desenvolvimento do sistema embarcado foi utilizada a tecnologia de Identificação por Radiofrequência (do inglês, *Radio Frequency Identification* - RFID), no qual é formado por uma etiqueta de identificação única (*tag*) e um leitor que se comunica com a etiqueta por ondas de rádio. O sistema *web* permite

o gerenciamento, cadastro de novos usuários e armazena o registro de acesso ao ambiente. O sistema *web* foi desenvolvido com os *frameworks* Node.js para o *backend* e React.js para o *frontend* e o nome escolhido foi GPACCESS, pois se remete a Acesso a Grupo de Pesquisa.

Uma visão geral do sistema é ilustrada na Figura 1, na qual a abertura da porta somente é liberada para usuários com as etiquetas RFID devidamente cadastradas no sistema. O sistema desenvolvido tem sua primeira versão direcionada para implantação no laboratório do Grupo de Pesquisa em Sistemas Críticos de Segurança (GPSiCS) da Universidade Federal Rural do Semi-Árido (UFERSA), Centro Multidisciplinar de Pau dos Ferros, com o intuito de controlar o uso deste espaço utilizado tanto por discentes, docentes e servidores terceirizados.

Figura 1 – Visão Geral do Sistema de Controle de Acesso GPACCESS



Fonte: (AUTORIA PRÓPRIA, 2020)

1.1 OBJETIVOS

O objetivo geral e os objetivos específicos são descritos nesta seção.

1.1.1 Objetivo Geral

Desenvolver um sistema de controle de acesso a ambientes públicos tais como sala de aulas, laboratórios, refeitórios, dentre outros, utilizando tecnologia RFID.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- a) Projetar um sistema embarcado utilizando tecnologia RFID;

- b) Projetar sistema *web* para cadastro dos usuários e registro do controle de acesso;
- c) Integrar o sistema embarcado ao sistema *web* utilizando comunicação sem fio.

1.2 ESTRUTURA DO TRABALHO

Além desta introdução, a qual apresenta a visão geral do trabalho desenvolvido, o restante deste documento está estruturado em 6 capítulos. No Capítulo 2 são apresentados os conceitos básicos e fundamentais utilizados no projeto, que são: *Radio Frequency Identification* (RFID), Arduino, NodeMCU - ESP8266 e Sistemas Embarcados. No Capítulo 3, os trabalhos relacionados são descritos. No Capítulo 4, os materiais e métodos utilizados para o desenvolvimento do sistema são apresentados. Os resultados da aplicação do projeto juntamente com a discussão sobre os dados obtidos são apresentados no Capítulo 5. No Capítulo 6, as considerações finais são descritas, como também as sugestões de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são introduzidos alguns conceitos teóricos considerados fundamentais para o desenvolvimento deste trabalho.

2.1 RADIO FREQUENCY IDENTIFICATION (RFID)

A identificação por radiofrequência (do inglês, *Radio Frequency Identification* - RFID) é considerada uma tecnologia que utiliza ondas de rádio para identificar e rastrear objetos físicos. A tecnologia RFID é implementada por meio de etiquetas (*tags*), que funcionam como transmissores, e leitores, que funcionam como os receptores. A etiqueta é um microchip conectado a antena que pode ser anexada a um objeto, servindo como identificador. O leitor se comunica com a etiqueta por ondas de rádio (JIA *et al.*, 2012).

Want (2006) discute que as etiquetas RFID podem ser divididas em duas classes: ativas e passivas. *Tags* ativas requerem uma fonte de energia, sendo estas impraticáveis em algumas aplicações pelo seu custo, tamanho e vida útil. Já as *tags* passivas não requerem bateria ou manutenção, possuem tempo de vida útil maior do que as *tags* ativas e por não precisarem de alimentação, seus componentes ocupam pouco espaço, permitindo caber em uma etiqueta adesiva. Devido a redução no tamanho e menor custo, neste trabalho são utilizadas etiquetas passivas. Este tipo de etiqueta é consistida em três partes: uma antena, um *chip* semicondutor conectado à uma antena e alguma forma de encapsulamento. O leitor das *tags* se comunica com uma etiqueta por ondas de rádio, a antena da *tag* captura a energia e transfere os dados armazenados na *tag*. O encapsulamento mantém a integridade da etiqueta e protege a antena e o *chip* contra intempéries no ambiente ou algum reagente. Em resumo, a operação de uma etiqueta ou *tag* RFID é um *transponder* (transmissor de rádio), representado por um *chip*, que ao ser estimulado retorna um sinal ou transmite o seu próprio, enviando dados referentes ao objeto no qual o *chip* está aplicado por meio da rádio frequência.

Na Figura 2 é ilustrado um *kit* módulo RFID MFRC522 Mifare, na qual o cartão branco e o chaveiro são exemplos de *tags* passivas, a antena RFID (leitor) em azul.

A tecnologia RFID pode ser aplicada em diversas áreas, tais como: lojas de roupas, nas quais as etiquetas das roupas possuem *tags* adesivas para identificação; em produtos alimentícios; pagamento de pedágio; logística; aplicações médicas como, por exemplo, as pulseiras utilizadas para identificação do paciente, contendo as informações necessárias para o atendimento, entre

Figura 2 – *Kit* Módulo RFID



Fonte: (BAUDAELETRONICA, 2020)

outras.

Segundo Deng *et al.* (2018), a tecnologia RFID quando comparada a outras tecnologias de identificação, tal como o código de barras, se sobressai pelo fato de ser reutilizável e não requerer uma linha de visão direta. Kamaludin, Mahdin e Abawajy (2018) apresentam várias aplicações em que o RFID substitui o código de barras como, por exemplo, transporte, operações portuárias, gerenciamento de cadeia de suprimento, monitoramento do nível de água e Internet das Coisas.

A tecnologia RFID com etiquetas passivas é aplicada neste trabalho para identificar os usuários pertencentes ao laboratório de pesquisa GPSiCS. Cada usuário possuirá uma *tag* associada ao seu cadastro no sistema, que irá permitir liberar o acesso ao ambiente físico do laboratório.

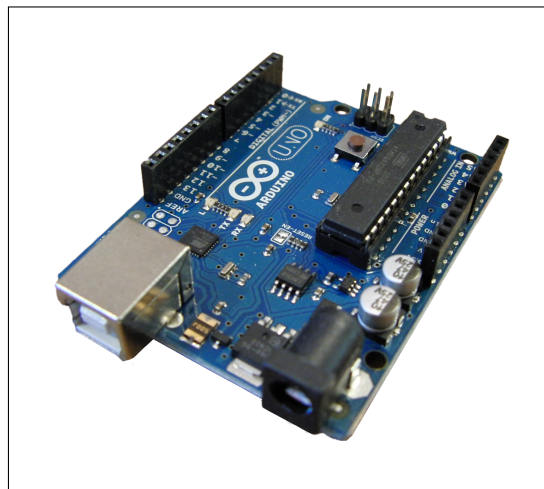
2.2 ARDUINO

Desde 2003, a plataforma Arduino é considerada uma ferramenta popular em projetos diversos que envolvem microcontroladores. A aplicação do Arduino nas mais diversas áreas tem aumento significativo por ter um custo acessível e uma curva de aprendizado bastante rápida, sendo cogitado como uma plataforma padrão para o ensino de sistemas embarcados e afins (DOLINAY; DOSTÁLEK; VAŠEK, 2016).

Arduino é um microcomputador programável no qual é possível processar entradas e saídas entre dispositivos/componentes conectados a ele. É uma plataforma de computação embarcada, e pode ser considerado um dispositivo que interage com o ambiente por meio de *hardware* e *software* (MCROBERTS, 2011).

Na Figura 3 é ilustrado um Arduino UNO R3, que tem como algumas de suas características: possuir como núcleo de processamento o microcontrolador ATmega328, operar em 5 Volts de tensão, possuir 14 portas digitais e 6 portas analógicas.

Figura 3 – Arduino UNO R3



Fonte: (WIKIPEDIA, 2020)

A plataforma Arduino foi escolhida para ser utilizada neste trabalho pelo fato de ser de rápida prototipação e pelo domínio prévio de programação da plataforma, por parte do autor deste trabalho.

2.3 NODEMCU - ESP8266

O módulo ESP8266 é um *transceptor* que envia dados pela rede Wi-Fi e pela comunicação serial, portanto, não há necessidade de conexão física com outros microcontroladores para recebimento e/ou envio de dados. O NodeMCU é um microcontrolador que possui o ESP8266 integrado (FERNANDES *et al.*, 2017). O NodeMCU pode ser usado como módulo para o Arduino ou como uma plataforma completa. A escolha do modo de usar depende do escopo da aplicação.

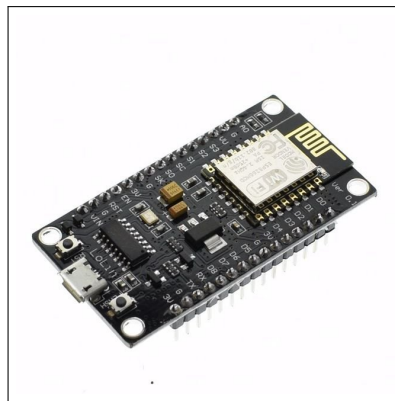
O NodeMCU, além de ser um módulo de transmissão Wi-Fi integrado, ainda é um microcontrolador, permitindo à comunicação por meio de GPIOs (*General Purpose Input/Output*),

portas programáveis para entrada e saída de dados, com conexão e transmissão de dados a Internet. Pode-se citar como vantagens, além de englobar a comunicação Wi-Fi, ser uma plataforma de baixo custo e baixo consumo de potência quando comparado a outros microcontroladores (BAJRAMI; MURTURI, 2018) .

Na Figura 4 é ilustrado um NodeMCU ESP8266 no modelo Lolin versão 3. Algumas de suas configurações, segundo Eletrogate (2020), são:

- a) Chip USB Serial CH340;
- b) Tensão de operação: 5V - 9V;
- c) Corrente de operação: 70mA (média) (picos de 200mA);
- d) Conexão Wi-Fi padrão 802.11 b/g/n e antena embutida;
- e) Alcance da Antena: 90m;
- f) Memória RAM: 20 KB;
- g) Memória FLASH: 4MB;
- h) Modos de operação: *Access Point*, *Station*, *Access Point* e *Station*;

Figura 4 – NodeMCU ESP8266 Lolin V3



Fonte: (ELETROGATE, 2020)

A escolha pela utilização do NodeMCU se deu pelo fato de ter fácil integração com a plataforma Arduino, como também possuir um *transceptor* Wi-Fi embutido.

2.4 SISTEMAS EMBARCADOS

Os sistemas embarcados podem ser definidos, de uma maneira geral, como sistemas que possuem interface com o mundo real por meio de sensores, que possuem microcontroladores para processo de leitura a partir desses sensores e podem ou não conter algum tipo de atuador.

Atualmente os sistemas embarcados podem ser encontrados desde residências até indústrias, na maioria das atividades cotidianas (POURSAFAEI *et al.*, 2018).

Os sistemas embarcados são adequados para resolver problemas específicos por meio da utilização de um *hardware* dedicado. Pode-se citar como exemplos comuns de sistemas embarcados: os *smartphones*, instrumentos para monitoramento do ambiente, a urna eletrônica, videogames, calculadoras, entre outros (KOULAMAS; LAZARESCU, 2018).

A presença de sistemas embarcados nas atividades cotidianas tem se expandido gradativamente e há previsão de crescimento nos próximos anos. Pode-se citar a fabricação de bilhões de processadores, por ano, especialmente para esse tipo de sistema. Sistemas embarcados estão sendo contemplados, cada vez mais, por aplicações de *software* sofisticadas e complexas, visando garantir sistemas implementados com qualidade, impactando diretamente nos seus requisitos (OSSADA; MARTINS, 2014).

Objetos conectados possuindo diversas capacidades computacionais, de acordo com as funcionalidades desejadas, fazem parte da rede de sistemas embarcados. Estes sistemas possuem menor consumo de energia, memória e capacidade de processamento, pois são desenvolvidos para um conjunto de necessidades específicas, ou seja, sistemas computacionais específicos. Neste contexto, mudanças realizadas através do tempo projetaram novos sistemas embarcados que fossem capazes de processar, armazenar, enviar e receber informações (VASCONCELOS, 2017).

Sistemas embarcados podem ser encontrado em mais de diversos segmentos do mercado, dentre eles, o automotivo, o médico e o hospitalar. A maioria das aplicações oferecem suporte aos sistemas embarcados, visto o seu constante crescimento (SILVA, 2011).

A partir destas definições, o conceito de sistema embarcado foi utilizado para implementação do *hardware* de identificação via RFID de usuários de um laboratório de pesquisa.

3 TRABALHOS RELACIONADOS

Neste capítulo são apresentados trabalhos relacionados ao sistema descrito neste documento.

3.1 RFID-INITIATED WORKFLOW CONTROL TO FACILITATE PATIENT SAFETY AND UTILIZATION EFFICIENCY IN OPERATION THEATER

Liu *et al.* (2011) descrevem um sistema que tem como objetivo controlar o fluxo dos pacientes em estado cirúrgico por meio da identificação por radiofrequência, desenvolvendo assim um sistema de monitoramento de avanço do paciente na sala de operações. Foi desenvolvido um sistema *web* que monitora todo o fluxo de trabalho com pacientes em estados cirúrgicos. O RFID é usado para indicar nas telas do computador a chegada do paciente em qualquer ponto de verificação do caminho, bem como alguns dados do paciente identificado. Isso ajuda a gerenciar o progresso das operações, localização do paciente, identificar o paciente e realizar cuidados no período operatório. Sendo assim, esse monitoramento fornece o compartilhamento instantâneo de informações para os profissionais de saúde com o intuito de aprimorar a eficiência do gerenciamento.

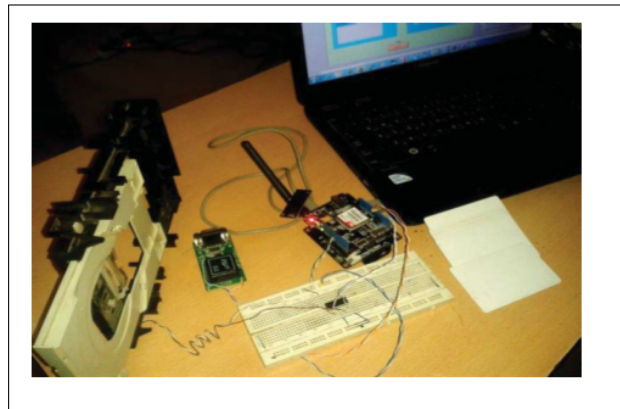
3.2 RFID BASED ACCESS CONTROL AND REGISTRATION SYSTEM

ALLAH *et al.* (2018) descrevem um sistema que usa tecnologia RFID para registro, monitoramento e controle de acesso para fins de segurança. Projetado para uso nas instalações da Comissão de Energia Atômica do Sudão, ajudando os responsáveis a monitorar e registrar as informações para o gerenciamento quando há necessidade. A proposta consiste em um circuito que controla a entrada de um portão e um *software* que monitora, exibe e registra informações do usuário juntamente com o *status* do sistema, obtendo a capacidade de ler e exibir o número do cartão do usuário, nome, a hora de chegada, a quantidade de vezes que ele foi usado e então salvar todos os dados em um arquivo de texto em uma Interface Gráfica do Utilizador (GUI) projetada e configurada utilizando o *software* LabView. Este sistema também faz o envio de mensagens SMS (*Short Message Service*) através do módulo GSM (*Global System for Mobile*) para o telefone celular de controle (mestre) em caso de invasores ou acesso não autorizado. Neste trabalho foi explicado que o desempenho do sistema mostra um registro de dados autenticado e

eficaz para os períodos de longo prazo como um sistema de registro monitorado.

O sistema se constituiu em duas partes principais: a parte de controle, que representa o *hardware*, e a parte de monitoramento e alerta que representa o *software*. Como são ilustrados na Figura 5, os principais componentes de *hardware* usados para o *design* do sistema consistem na placa Arduino *Freakduinoboard*, leitor RFID (RREAD-mRW), módulo GSM para a manipulação de SMS, um motor DC e *driver* de motor DC e um computador. O módulo RFID pode ler e gravar as identificações EM4100, T5557, EM4205/EM4305, HITAGS e FDX-B, equipado com um *driver* RS232 e um conector DB-9 para conexão direta com o computador, alimentado por uma fonte de 5 Volts.

Figura 5 – Proposta de Sistema



Fonte: (ALLAH *et al.*, 2018)

3.3 A DIGITAL SECURITY SYSTEM WITH DOOR LOCK SYSTEM USING RFID TECHNOLOGY.

Verma e Tripathi (2010) tiveram como objetivo implementar um sistema de segurança digital que possa ser implantado em uma zona segura, em que apenas uma pessoa cadastrada possa acessar. Uma trava de porta pode ser ativada por uma *tag* passiva RFID, após a *tag* ser autenticada, destrancando a porta em tempo real e obtendo um acesso seguro. Um sistema centralizado gerencia a tarefa de controle e operação, criando também um *log* contendo entrada e saída de cada usuário, juntamente com suas informações básicas.

A proposta de sistema consiste em 5 etapas. A primeira é a etapa em que o leitor RFID recupera as informações contidas na etiqueta. A segunda é a etapa após receber as informações da etiqueta, em que o leitor envia essas informações ao banco de dados para verificação, e a

terceira etapa em que o servidor central consulta o banco de dados e recupera as informações correspondentes. Na quarta etapa o leitor calcula o registro de data e hora após receber a resposta do servidor, criando um *log*. Na quinta e última etapa, uma vez verificadas as informações da *tag*, o sistema gera um sinal de controle através da porta paralela que controla a abertura e fechamento da trava por meio de um motor.

3.4 RFID BASED SECURITY AND ACCESS CONTROL SYSTEM

Farooq *et al.* (2014) discutem sobre um sistema de segurança e controle de acesso baseado em RFID para o uso em albergues dentro das instalações da Universidade de Punjab. O uso combinado de RFID e biometria realiza a tarefa de identificação do usuário. O leitor RFID instalado na entrada do albergue detecta o número da *tag* passiva. O sistema faz a captura da imagem do usuário e verifica se há correspondência no banco de dados. Caso o acesso seja concedido, o usuário vai ter passagem liberada, caso contrário, o sistema vai soar um alarme e fará uma chamada de emergência para a segurança da Universidade através do módulo GSM.

Os componentes utilizados para o sistema foram: a *tag* passiva RFID IPC80, com operação de frequência de 125kHz, que transmite informações ao leitor; o leitor RFID IP10 com distância de leitura de até 4 polegadas, sendo instalado três leitores para a segurança do albergue: portão de entrada, de saída e portão de entrada da bagunça; o módulo GSM; o microcontrolador AT89C52; a RAM não volátil 256K Nonvolatile RAM (NV-Ram) DS1230Y-85 utilizada para armazenar senhas contra números RFID registrados, travas de portas e alarmes.

3.5 CONTRIBUIÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO

A partir da análise dos trabalhos relacionados apresentados neste capítulo, é possível observar que RFID é considerado importante tanto na área da saúde como também para o controle e gerenciamento de acesso, visto sua aplicabilidade tanto em universidades, como em indústrias e hospitais, priorizando a segurança e a agilidade de troca de informações.

O sistema de controle de acesso utilizando a tecnologia RFID, desenvolvido neste trabalho de conclusão de curso, utiliza tecnologias relevantes para a solução da problemática apresentada. Diferentemente dos trabalhos apresentados, o sistema proposto trará a vantagem de utilizar o conceito de comunicação de um sistema embarcado integrado a um sistema *web* para manutenção e gerenciamento de dados de acesso ao ambiente.

4 METODOLOGIA

O protótipo desenvolvido neste trabalho é um sistema modular, composto da seguinte forma:

- a) Módulo Gerencial (principal): no qual se tem o gerenciamento do ambiente cadastrado, conforme o serviço fornecido, como por exemplo, o gerenciamento do acesso dos usuários;
- b) Módulo de Sensoriamento: no qual ocorre o monitoramento do ambiente por meio dos dispositivos, com a identificação por radiofrequência (RFID);
- c) Módulo de Atuação: composto pelos equipamentos de atuação, como, por exemplo, travas elétricas, lâmpadas, ar-condicionado, computadores e *datashows*.

De uma maneira geral, o sistema GPACCESS desenvolvido neste trabalho pode ser dividido no sistema *web*, que representa o módulo gerencial, e no sistema embarcado, que implementa os módulos de sensoriamento e atuação. Nas seções a seguir são apresentados os passos principais para desenvolvimento tanto do sistema *web* quanto do sistema embarcado.

4.1 SISTEMA WEB

A primeira etapa para o desenvolvimento do sistema *web* foi a de levantamento de requisitos, considerado o ponto de partida de qualquer projeto de *software*. Dentro dos resultados obtidos nesta etapa, foi possível mapear as funcionalidades e características necessárias para desenvolvimento do projeto. Neste processo de compreensão e identificação das necessidades do usuário, define-se todo os requisitos pertinentes ao *software*.

Os requisitos de um sistema podem ser subdivididos em requisitos funcionais e requisitos não funcionais. Os requisitos funcionais são as funcionalidades necessárias para o sistema, como, por exemplo: cadastrar, consultar e excluir dados referentes a uma determinada entidade representada no sistema. Já os requisitos não funcionais se referem a recursos que são considerados características do sistema, como por exemplo: restrições, segurança e confiabilidade. A etapa de levantamento de requisitos do sistema de acesso desenvolvido foi realizada por meio de consulta aos coordenadores do laboratório do GPSiCS, utilizando uma entrevista informal. A seguir são detalhados todos os requisitos funcionais e não-funcionais para o sistema GPACCESS.

4.1.1 Requisitos Funcionais

Estes requisitos são as funcionalidades que o *software* deve atender em relação as necessidades do usuário. Os requisitos funcionais deste sistema estão descritos na Tabela 1 e na Tabela 2.

Tabela 1 – Requisitos Funcionais do Administrador

Código	Descrição
RF01	O sistema deve permitir que o administrador possa realizar autenticação no sistema.
RF02	O sistema deve permitir que o administrador possa deslogar do sistema.
RF03	O sistema deve permitir que o administrador associar <i>tags</i> aos usuários.
RF04	O sistema deve permitir que o administrador possa remover usuário.
RF05	O sistema deve permitir que o administrador possa listar os acessos.
RF06	O sistema deve permitir que o administrador possa listar usuários.
RF07	O sistema deve permitir que o administrador possa consultar as informações de cada acesso.
RF08	O sistema deve permitir que o administrador gere relatórios de acessos.
RF09	O sistema deve permitir que o administrador atualize seus dados.
RF10	O sistema deve permitir que o administrador recupere sua senha.

Fonte: (AUTORIA PRÓPRIA, 2020)

Tabela 2 – Requisitos Funcionais do Usuário

Código	Descrição
RF11	O sistema deve permitir cadastro de novos usuários.

Fonte: (AUTORIA PRÓPRIA, 2020)

4.1.2 Requisitos Não-Funcionais

Os requisitos não funcionais do sistema estão descritos na Tabela 3.

Tabela 3 – Requisitos Não-Funcionais

Código	Descrição
RNF01	O sistema deve ser desenvolvido usando a linguagem de programação Node.js para <i>backend</i> e React.js para <i>frontend</i> .
RNF02	O sistema deve utilizar o PostgreSQL, como Sistema de Gerenciamento de Banco de Dados.
RNF03	O sistema deve ser utilizado em plataforma <i>web</i> .
RNF04	O sistema deve ser seguro.

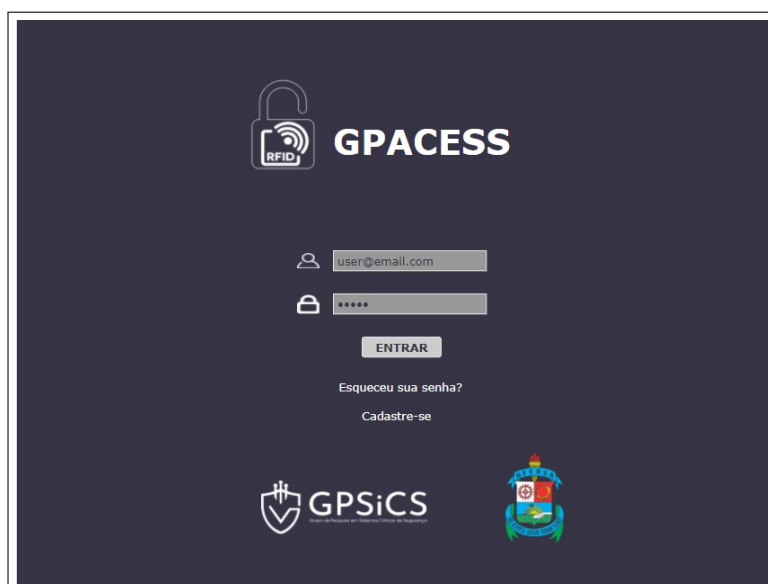
Fonte: (AUTORIA PRÓPRIA, 2020)

4.1.3 Protótipação de Telas

Nesta seção são ilustradas as telas inicialmente prototipadas, disponibilizadas aos usuários do sistema para aprovação. As telas foram prototipadas na ferramenta *Justinmind Prototyper*¹ que é gratuita e fácil de utilizar. Os protótipos foram utilizados como base para a implementação do sistema real.

Na Figura 6 é ilustrada a tela inicial do sistema *web*. Os dados escolhidos para entrar no sistema foram e-mail e senha. Os usuários que podem acessar o sistema são, apenas, os coordenadores, que encontram-se previamente cadastrados no banco de dados.

Figura 6 – Tela de *Login*



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 7 é ilustrada a tela de cadastro de usuários, de acordo com as funcionalidades requisitadas. Os coordenadores do grupo, previamente cadastrados no banco de dados, podem entrar no sistema e cadastrar novos usuários pesquisadores, com a *tag*, nome completo e e-mail, para que estes possam utilizar seus crachás (*tag*) na entrada do laboratório.

¹ <https://www.justinmind.com/>

Figura 7 – Tela de Cadastro

Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 8 é ilustrada a tela de recuperação de senha para os usuários coordenadores, utilizando o e-mail cadastrado no banco de dados.

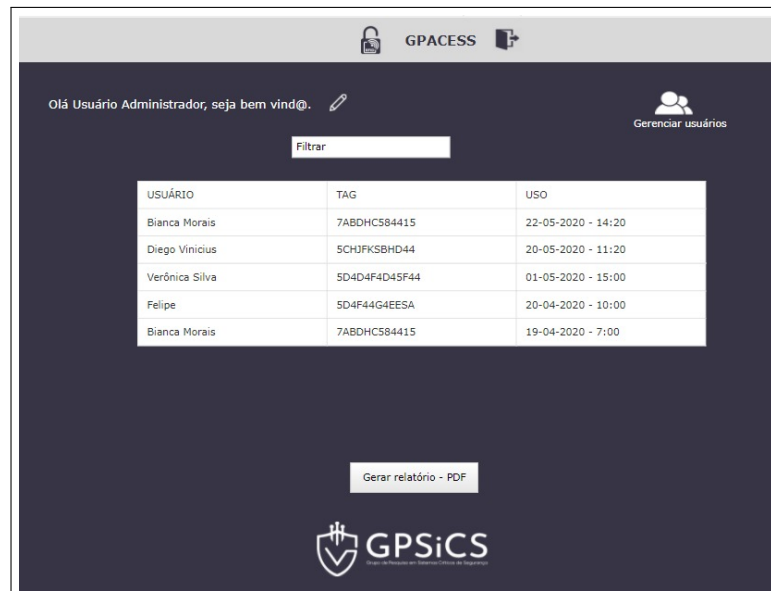
Figura 8 – Tela de Recuperação de senha

Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 9 é ilustrada a tela após entrar no sistema, tendo o menu inicial, no qual são exibidos dados de uso das *tags* e seus respectivos usuários. Pode-se observar também um ícone em formato de lápis ao lado do nome do usuário que esta logado, este redireciona para uma página na qual é possível editar os seus dados e sua senha. O ícone em formato de boneco

permite redirecionar para o módulo de gerenciamento de usuários, apresentado na Figura 10. Também é possível gerar um relatório em formato PDF (*Portable Document Format*) dos acessos, com direito a filtragem de dados pelo campo de busca.

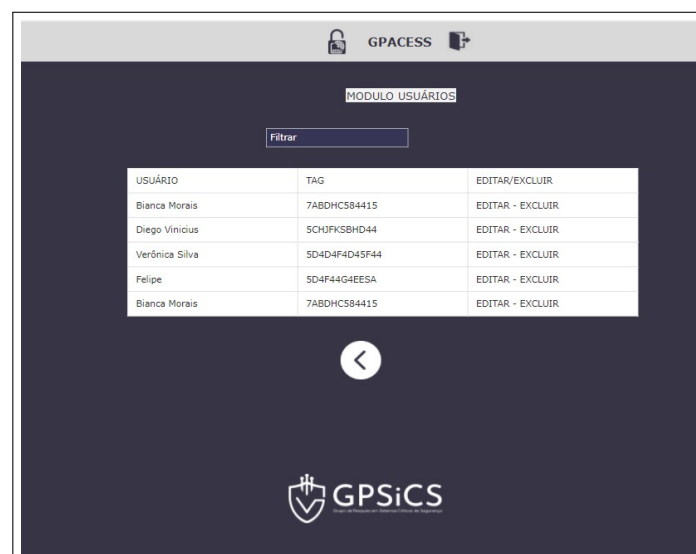
Figura 9 – Menu Inicial



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 10 é ilustrada a tela de gerenciamento de usuários, na qual os dados podem ser editados ou excluídos, individualmente, também com a opção de filtragem de dados pelo campo de busca.

Figura 10 – Módulo de Gerenciamento de Usuários



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 11 é ilustrada a tela de edição de dados do usuário logado no sistema, na qual este pode editar seus dados ou alterar sua senha.

Figura 11 – Tela de Edição de Dados

Fonte: (AUTORIA PRÓPRIA, 2020)

4.1.4 Banco de Dados

Nesta seção é apresentada a modelagem e a ferramenta de gerenciamento do banco de dados do sistema *web* GPACCESS.

O uso de banco de dados se faz necessário para o armazenamento de dados importantes de um sistema. Para criação e gerenciamento do bando de dados do GPACCESS foi utilizado o PostgreSQL², que é um sistema de gerenciamento de banco de dados objeto relacional, de código aberto, que pode ser utilizado em inúmeras plataformas, dentre estas, a PostBird³ que funciona monitorando o banco, no formato de interface gráfica do usuário, a fim de visualizar dados com facilidade.

O banco foi hospedado *online* visando melhor integração com o servidor de hospedagem do sistema *web*. O banco de dados é de fundamental importância para manter os dados, como para consultas, dentre estas, a autenticação no sistema e a listagem de dados do uso do laboratório pelos usuários cadastrados.

A visualização do funcionamento do banco de dados do GPACCESS se dá pelo mapeamento ilustrado na Figura 12, que é disposto no modelo lógico, criado no brModelo⁴, explicado

² <https://www.postgresql.org/>

³ <https://www.electronjs.org/apps/postbird>

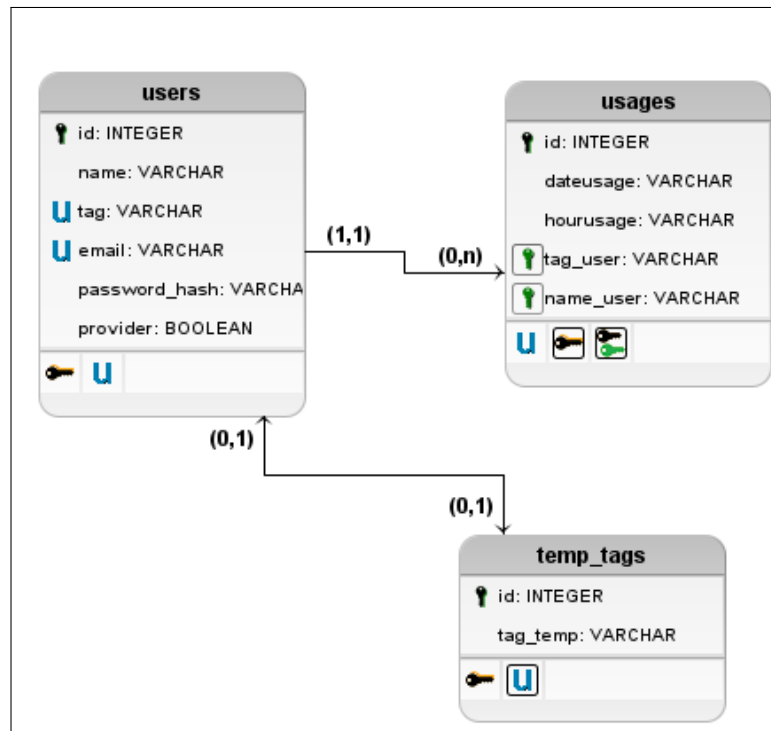
⁴ <http://www.sis4.com/brModelo/>

a seguir:

- a) *users*: é a tabela de dados dos usuários, na qual seus campos de informação são:
- *id* que identifica cada usuário do sistema e é chave primária;
 - *name* é o nome do usuário;
 - *tag* é o número de identificação do cartão ou chaveiro;
 - *email* é o *email* do usuário;
 - *password_hash* é a senha encriptada, na qual na tabela é exibido apenas um campo codificado.
- b) *usages*: é a tabela de dados de acesso ao laboratório, na qual seus campos de informação são:
- *id* que identifica de forma única o acesso de um usuário, ou seja, é chave primária;
 - *dateusage* é a data de uso do cartão;
 - *hourusage* é a hora de uso do cartão;
 - *tag_user* é o cartão associado a tabela *users* como chave estrangeira, sendo o número de identificação do usuário;
 - *name_user* é o nome do usuário associado ao cartão, é uma chave estrangeira da tabela *users*.
- c) *temp_tags*: é a tabela de *tags* temporárias, utilizadas no cadastro de *tags* para novos usuários:
- *id* que identifica unicamente uma tag a ser atribuída a um novo usuário, ou seja, é chave primária;
 - *tag_temp* é a *tag* temporária;

A cardinalidade das tabelas vem do nível de relacionamento das tabelas apresentadas na Figura 12 que é ilustrado pelas setas entre elas, na qual o mesmo funciona da seguinte forma: o usuário pode ter no mínimo nenhum e no máximo vários acessos, ou seja, (0,N), e a tabela de acessos pode ter no mínimo um e no máximo um usuário por acesso, ou seja, (1,1). Em relação a tabela “temp_tags” e a tabela “users”, uma *tag* da tabela de *tags* temporárias pode ser associada a nenhum ou um usuário, ou seja, (0,1), e a tabela de usuários pode ter uma ou nenhuma *tag* que estava na tabela de *tags* temporárias, ou seja, (0,1).

Figura 12 – Modelo Lógico do Banco de Dados do GPACCESS



Fonte: (AUTORIA PRÓPRIA, 2020)

4.2 SISTEMA EMBARCADO

Nesta seção é apresentada a metodologia para construção do sistema embarcado do GPACCESS.

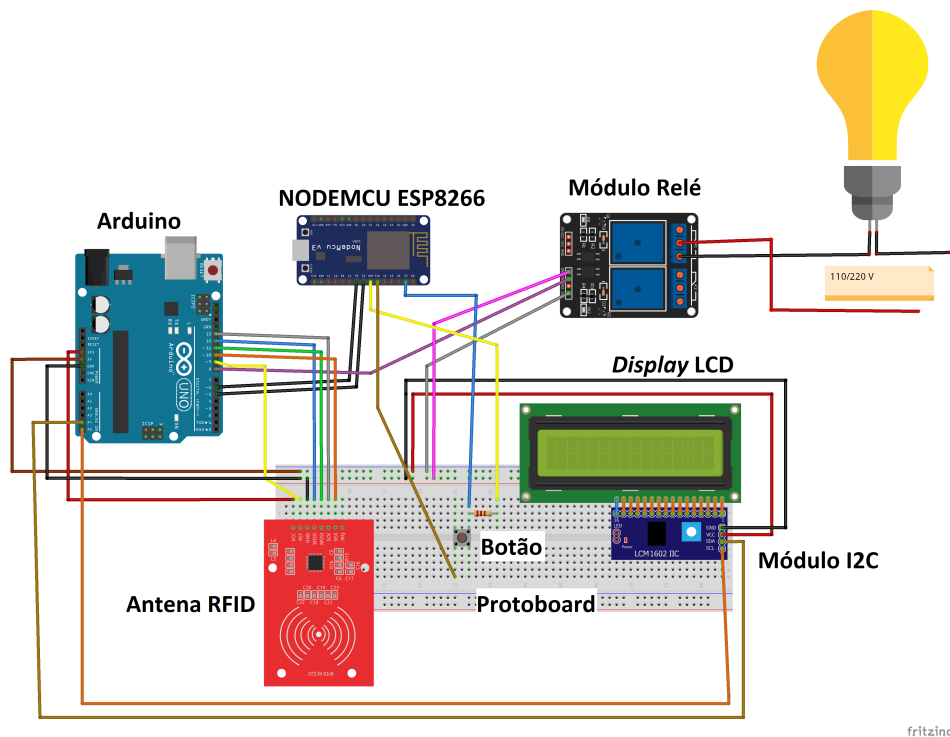
Para o desenvolvimento do sistema embarcado do GPACCESS, responsável pela identificação via RFID dos usuários e liberação do acesso ao laboratório, se fez necessário o uso dos seguintes componentes:

- Placa de Arduino UNO R3;
- Display* LCD;
- Módulo I2C;
- Protoboard*;
- Leitor RFID;
- Módulo Relé;
- Módulo Wi-Fi NodeMCU ESP8266;

O Arduino é conectado ao *display* LCD, ao módulo relé e ao leitor RFID, por meio de interconexão com a *protoboard*, no qual o *display* LCD exibe as informações do usuário do cartão ao ser passado no leitor RFID. O Arduino recebe os dados lidos pelo leitor RFID e envia,

por conexão serial, ao módulo Wi-Fi que comunica-se com o servidor. No servidor é verificado a existência do cadastro no banco de dados da *tag*, caso seja positivo, é enviado a confirmação ao módulo Wi-Fi, que devolve para o Arduino e este ativa o módulo relé que aciona a lâmpada, simbolizando a fechadura elétrica, portanto, destrancando a porta. No *hardware* há também um botão que funciona criando uma interrupção: caso esteja pressionado, troca o funcionamento do módulo Wi-Fi para comunicar-se com o banco de cadastro de *tags* temporárias, inserindo uma nova *tag* que fica disponível para ser associada a um novo usuário, caso ela não esteja associada a nenhum. Na Figura 13 é ilustrado o *sketch* do protótipo do sistema embarcado (*hardware*), exemplificando o uso do material descrito nesta seção.

Figura 13 – *Sketch* do *Hardware*



Fonte: (AUTORIA PRÓPRIA, 2020)

O módulo I2C é utilizado para a redução do uso de portas do LCD para o Arduino, ajustando a intensidade da luz do visor automaticamente ou por meio das portas do próprio módulo. A lâmpada exemplifica uma carga qualquer, como, por exemplo, uma trava elétrica ou um equipamento elétrico.

5 RESULTADOS E DISCUSSÕES

Neste capítulo serão apresentados os resultados obtidos neste trabalho com a implementação do sistema embarcado e o sistema *web* (*software*).

5.1 SISTEMA WEB

Nesta seção é apresentada a versão final do sistema *web* desenvolvido. A hospedagem do sistema foi realizada temporariamente no Heroku ⁵, uma plataforma que contém serviço grátis e suporta várias linguagens de programação, dentre elas o Node.js e o React.js. O Heroku também permite hospedagem de banco de dados PostgreSQL *online* integrada, sendo possível operar atividades básicas de um sistema hospedado. Desta forma, atendendo aos requisitos necessários para hospedagem do sistema desenvolvido.

O *backend* e *frontend* estão disponíveis no GitHub ⁶, uma plataforma de hospedagem de código fonte, com o adicional de controle de versão. Os códigos e o site do sistema deste trabalho estão disponíveis nos seguintes endereços:

- a) *backend*: <https://github.com/biancasgmorais/gpaccessbackend>
- b) *frontend*: <https://github.com/biancasgmorais/gpaccessfrontend>
- c) Hospedagem: <https://gpaccess.herokuapp.com/>

5.1.1 Modelo Final GPACCESS

O resultado final do sistema *web* é apresentado a seguir. A partir das telas prototipadas, foram realizadas melhorias tanto visuais, como funcionais.

Na Figura 14 é ilustrada a tela de *login*, na qual os dados de entrada são e-mail e senha. Também é possível visualizar os *links* para a página de recuperação de senha e cadastro de novos usuários. O logo do GPSiCS e o brasão da universidade fazem referência a vinculação do ambiente no qual o serviço é oferecido, estes também redirecionam para as páginas dos referenciados.

⁵ www.heroku.com

⁶ <https://github.com/>

Figura 14 – Tela de *Login* (Versão Final)

The login screen features a dark blue background. At the top center is a logo with a hand holding a device emitting an RFID signal, labeled 'RFID GPACCESS'. Below the logo are two input fields: 'Email' with an envelope icon and 'Password' with a lock icon. A white 'Entrar' button is positioned below the password field. Underneath the button are two links: 'Esqueceu sua senha?' and 'Cadastre-se'. At the bottom, there are two logos: 'GPSiCS' on the left and a university crest on the right.

Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 15 é ilustrada a tela de cadastro, os dados são nome completo e e-mail. Esses dados foram escolhidos, pois a utilização dessa funcionalidade é feita por usuários que vão se cadastrar no banco e, logo depois, os usuários administradores farão a liberação do acesso, associando uma *tag* a esse usuário.

Figura 15 – Tela de Cadastro (Versão Final)

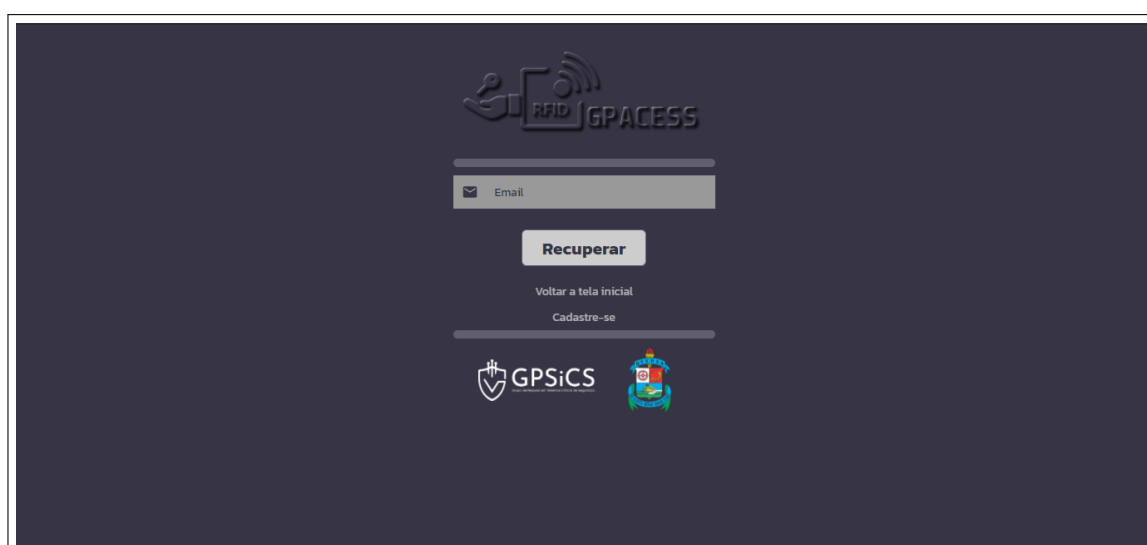
The registration screen has a dark blue background. At the top center is the same 'RFID GPACCESS' logo as in the login screen. Below it are two input fields: 'Nome completo' with a person icon and 'Email' with an envelope icon. A white 'Criar conta' button is located below the email field. Underneath the button is a link: 'Já tenho login'. At the bottom, there are two logos: 'GPSiCS' on the left and a university crest on the right.

Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 16 é ilustrada a tela da recuperação de senha, feita com o e-mail. Essa funcionalidade só pode ser feita por usuários administradores, que estão previamente cadastrados no banco, pois a estes são associados senha, provendo o acesso a todas as funcionalidades do

sistema. Dentro dessa funcionalidade, o e-mail inserido é verificado se corresponde a um e-mail de um usuário administrador cadastrado no banco. Em caso positivo, um e-mail é enviado para o e-mail cadastrado no banco. O protocolo de envio de e-mail é feito com o Google⁷ API (*Application Programming Interface*), na qual um e-mail foi criado e autorizado juntamente com o protocolo OAuth2 que permite a autenticação da aplicação nos serviços do Google. Ambos protocolos utilizam o SMTP (*Simple Mail Transfer Protocol*), ou protocolo de transferência de correio simples, que, resumidamente, é um protocolo de envio de mensagem por e-mail.

Figura 16 – Tela de Recuperação de Senha (Versão Final)

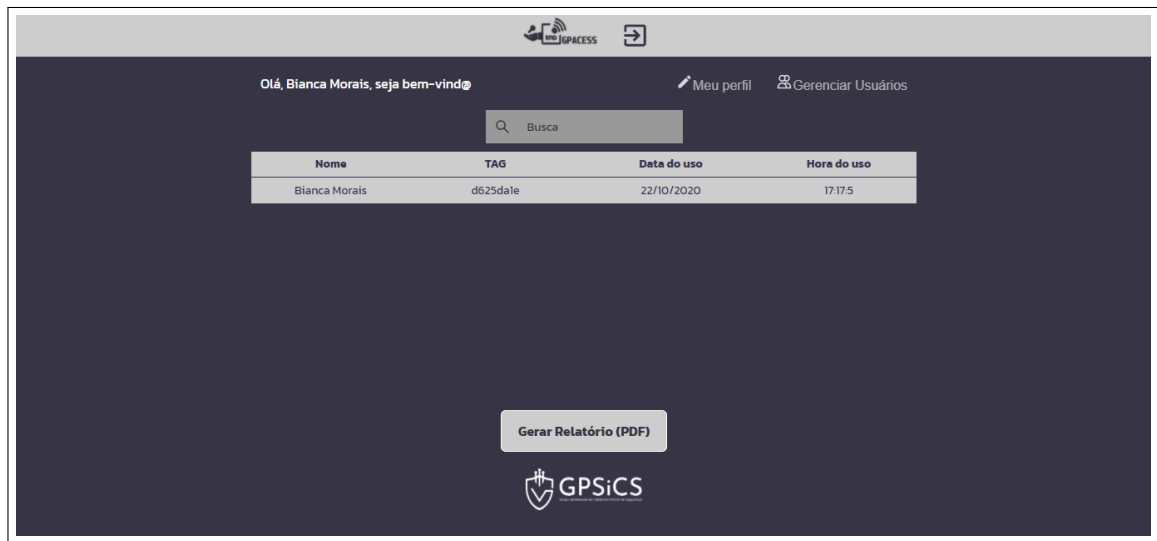


Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 17 é ilustrada a tela inicial, após a autenticação no sistema, esta funcionalidade só pode ser acessada pelos coordenadores do grupo de pesquisa (usuários administradores), previamente cadastrados no banco. Nesta tela, são exibidos os dados de controle do ambiente, na qual em uma tabela são dispostos nome, *tag*, data de uso e hora de uso. Na tabela são exibidas informações que podem ser filtradas no campo busca e também pode-se gerar um relatório no formato de arquivo PDF, podendo este ser gerado apenas com os dados filtrados, ou a tabela completa. A opção “Meu Perfil” redireciona a tela de edição de senha do usuário logado e a opção “Gerenciar Usários” redireciona a tela de dados dos usuários cadastrados no banco de dados.

⁷ <https://www.google.com.br/>

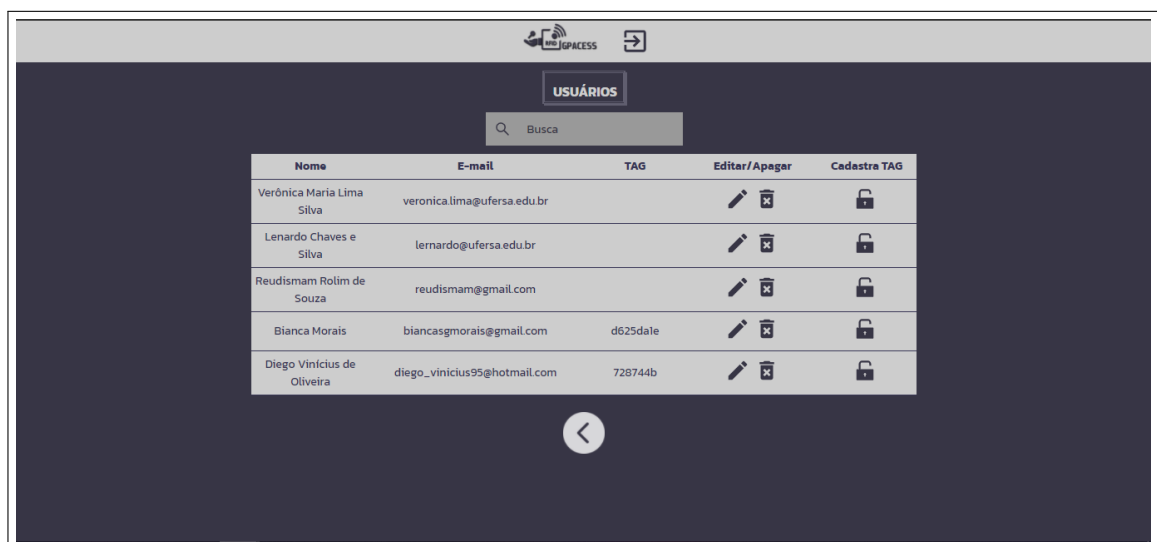
Figura 17 – Tela Inicial (Versão Final)



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 18 é ilustrada a tela do menu “Gerenciar Usuários”. Nesta tela são listados os dados dos usuários, que são nome, e-mail e o número da *tag*. Estes dados podem ser editados ou apagados do sistema. A opção editar redireciona para uma tela onde os dados podem ser modificados. A opção “Cadastra TAG” redireciona para uma tela na qual uma *tag* temporária fica disponível para ser associada a um usuário. O campo busca filtra os dados de qualquer campo da tabela. O botão voltar, representado por uma seta para a esquerda, redireciona à tela inicial, como também ao clicar no logo do GPACCESS no cabeçalho da página.

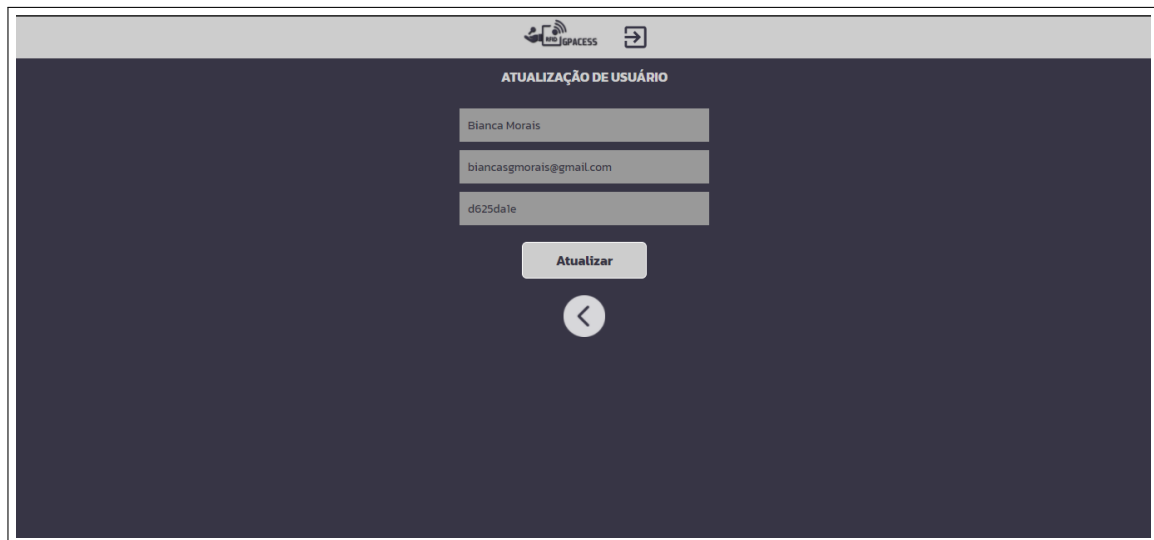
Figura 18 – Tela de Gerenciamento de Usuários (Versão Final)



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 19 é ilustrada a tela de atualização de dados do usuário, os campos já são inicialmente preenchidos pelos dados que estão na tabela, a fim de facilitar sua usabilidade. O botão voltar redireciona a tela de gerenciamento de usuários.

Figura 19 – Tela de Atualização de Dados (Versão Final)

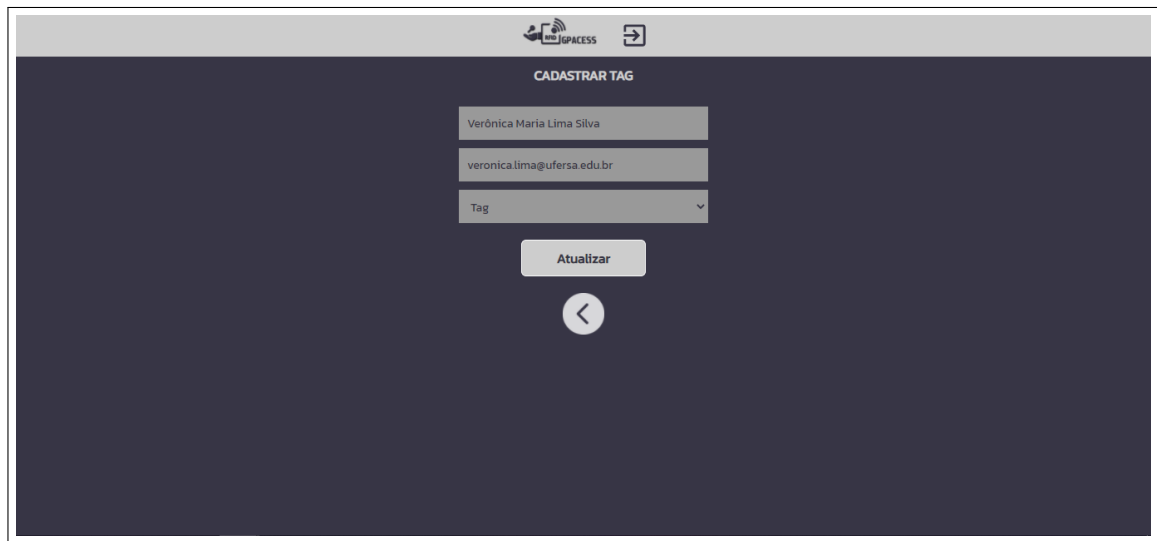


A captura de tela mostra uma interface de usuário com o título "ATUALIZAÇÃO DE USUÁRIO" no topo. Abaixo do título, há três campos de entrada de texto empilhados verticalmente. O primeiro campo contém o nome "Bianca Morais", o segundo contém o e-mail "biancasgmorais@gmail.com" e o terceiro contém a senha "d625dale". Abaixo dos campos, há um botão retangular com o texto "Atualizar". Logo abaixo do botão, há um botão circular com uma seta para trás, indicando uma função de voltar.

Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 20 é ilustrada a tela do cadastro de *tag* para um usuário que ainda não tenha ou necessite trocar. O campo “Tag” é uma caixa de seleção que exibe uma *tag* que esteja cadastrada na tabela de *tags* temporárias, no banco de dados. Esta caixa de seleção exibe uma *tag* durante um minuto, caso nenhum usuário seja associado a ela durante esse tempo, ela é apagada do banco, pois assim fica disponível para posteriormente ser cadastrada a outra pessoa. No caso da *tag* ser cadastrada, ela, também, é apagada da tabela temporária e fica, apenas, na tabela principal associada ao usuário, não permitindo ser cadastrada novamente na tabela de *tags* temporárias, muito menos, na tabela principal.

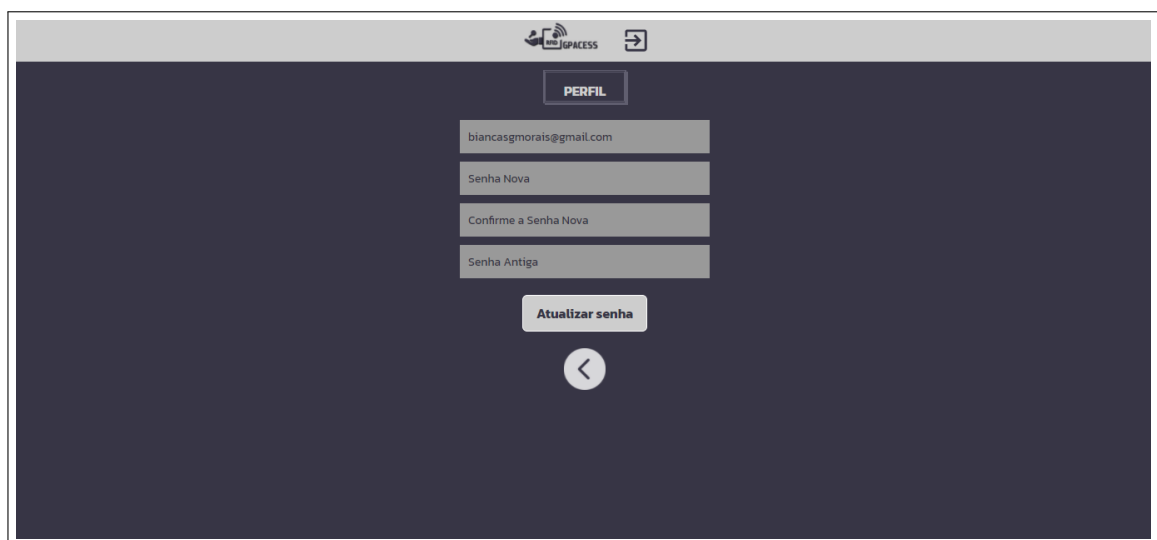
Figura 20 – Tela de Cadastro de TAG (Versão Final)



Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 21 é ilustrada a tela de edição de dados do usuário logado, na qual o e-mail deste é previamente exibido numa caixa de texto, os campos “Senha Nova” e “Confirme a Senha Nova” servem para verificação de senha e o campo “Senha Antiga”, refere-se a senha atual do usuário.

Figura 21 – Tela de Perfil (Versão Final)

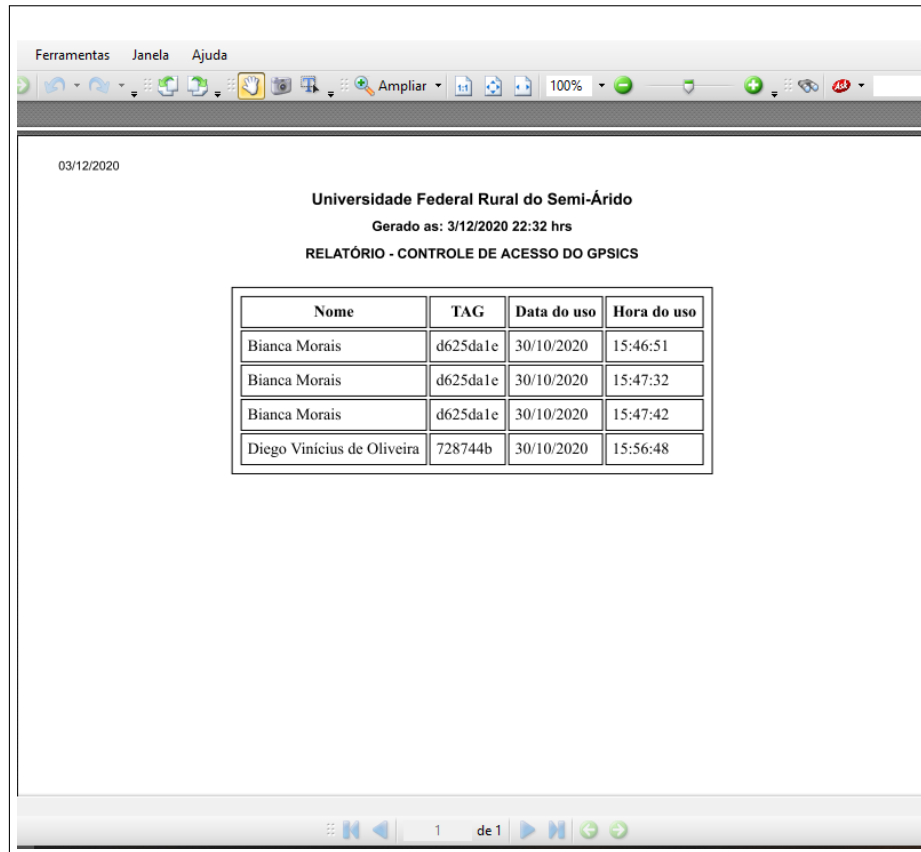


Fonte: (AUTORIA PRÓPRIA, 2020)

Na Figura 22 é ilustrada a página de impressão de relatório, caso o botão de “Gerar Relatório (PDF)” da tela inicial seja pressionado, de acordo com o descrito na Figura 17. O relatório pode ser salvo no formato de arquivo PDF e suas informações são as mesmas da tabela,

seja ela filtrada ou não, também informando a hora e data que foi gerado.

Figura 22 – Modelo de Relatório (Versão Final)



03/12/2020

Universidade Federal Rural do Semi-Árido
Gerado as: 3/12/2020 22:32 hrs
RELATÓRIO - CONTROLE DE ACESSO DO GPSICS

Nome	TAG	Data do uso	Hora do uso
Bianca Moraes	d625da1e	30/10/2020	15:46:51
Bianca Moraes	d625da1e	30/10/2020	15:47:32
Bianca Moraes	d625da1e	30/10/2020	15:47:42
Diego Vinicius de Oliveira	728744b	30/10/2020	15:56:48

Fonte: (AUTORIA PRÓPRIA, 2020)

5.2 SISTEMA EMBARCADO

Nesta sessão é abordado sobre a programação utilizada no Arduino e no NodeMCU ESP8266; o funcionamento do protótipo e o resultado final do sistema embarcado. Os fluxogramas, criados na plataforma Lucidchart⁸, são diagramas que ilustram o funcionamento interno do código de ambos os componentes. Os códigos da aplicação embarcada estão disponíveis no GitHub, no seguinte endereço:

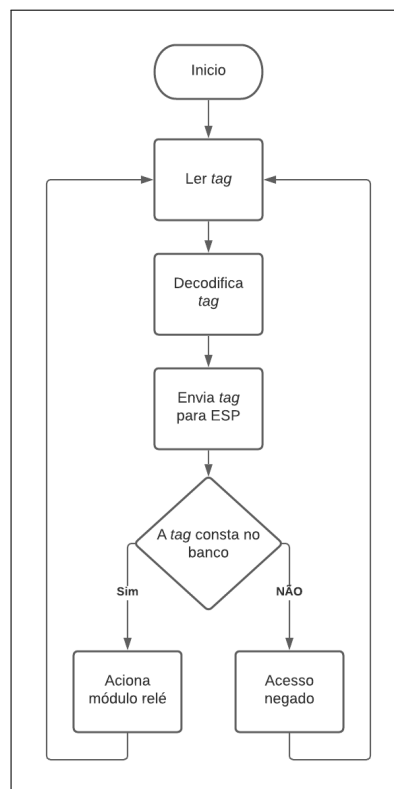
a) Aplicação Embarcada: <https://github.com/biancasgmorais/gpaccesshardware>

⁸ <https://lucid.app/>

5.2.1 Funcionamento do Arduino

O microcontrolador Arduino funciona, neste projeto, como o sistema principal de processamento e comunicação de *hardware*, fornecendo informações aos dispositivos que estão conectados a ele. Portanto, seu funcionamento acontece conforme fluxograma apresentado na Figura 23, na qual ao iniciar a aplicação embarcada é ativado o RFID e espera por uma *tag*, assim que a antena detecta a *tag*, a aplicação embarcada a decodifica e envia para o ESP8266. Em caso de resultado positivo da consulta ao banco de dados, o módulo relé é ativado ligando a lâmpada, ou seja, ativando a carga, que neste caso é uma fechadura elétrica.

Figura 23 – Fluxograma do Funcionamento do Arduino



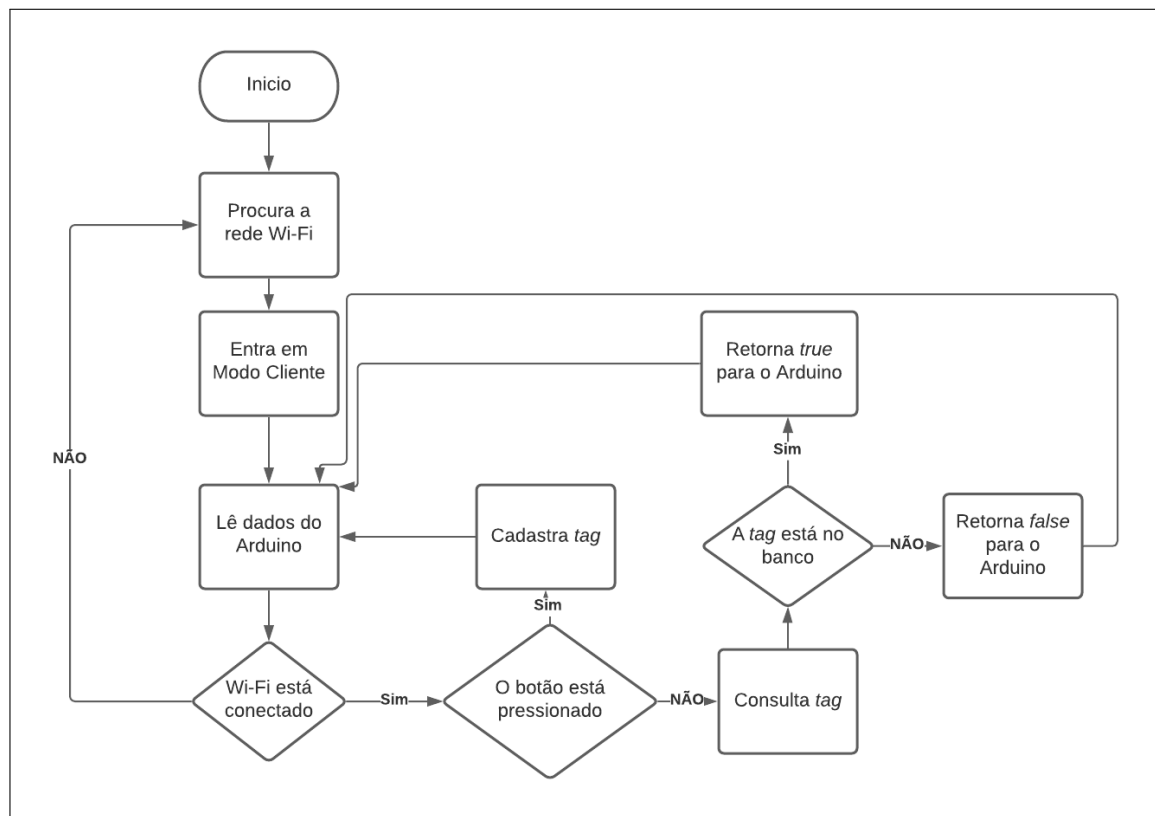
Fonte: (AUTORIA PRÓPRIA, 2020)

5.2.2 Funcionamento do ESP8266

O NodeMCU ESP8266 V3, além de ser um módulo Wi-Fi, também é um microcontrolador. No caso deste projeto, o único componente associado diretamente ao seu comando foi o botão. O ESP8266 se comunica com o Arduino por meio da comunicação serial, na qual a conexão foi feita por *jumpers*. Portanto, o seu funcionamento se dá como ilustra o fluxograma

na Figura 24, na qual ao iniciar a aplicação embarcada é recebido os dados da rede Wi-Fi no modo cliente, ou seja, ele envia dados pela rede. O módulo começa a ler dados pela porta serial conectada ao Arduino e verifica se a rede Wi-Fi está conectada; caso esteja, a verificação do botão é feita, se ele for 0 significa que ele não está pressionado, então entra na condição de consultar a *tag*, se ele for 1 significa que o botão está pressionado, iniciando assim a funcionalidade de cadastro de *tag* na tabela de *tags* temporárias e logo após voltar a consultar os dados enviados pelo Arduino. No caso do consulta de *tag*, o método *post* é acionado por meio de uma biblioteca chamada ESP8266HTTPClient⁹, inicializando assim o modo de cadastro de um acesso ao ambiente. Se a aplicação retornar o código 201, significa que a *tag* estava no banco e seu acesso foi cadastrado retornando o número 15 (escolhido de forma arbitrária) para o Arduino. Caso ele retorne o código 400, significa que a *tag* não está no banco, ou algum dado do acesso está incorreto, retornando não autorizado e escrevendo o número 10 (escolhido de forma arbitrária) na saída do Arduino, não liberando o acesso. Em ambos os casos, após percorrerem e receberem suas respostas, a aplicação volta para a leitura de dados do Arduino.

Figura 24 – Fluxograma do Funcionamento do ESP8266



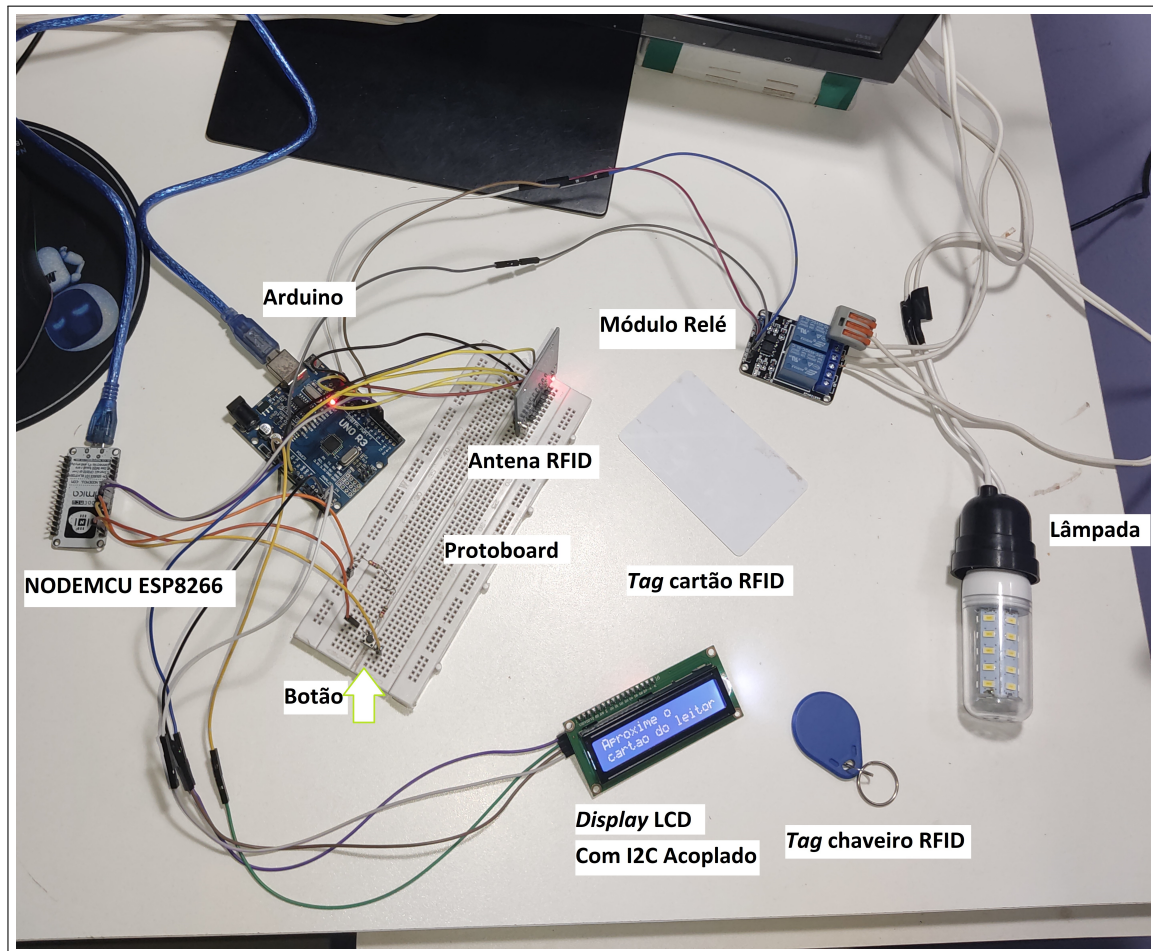
Fonte: (AUTORIA PRÓPRIA, 2020)

⁹ <https://github.com/esp8266/Arduino/tree/master/libraries/ESP8266HTTPClient>

5.2.3 Protótipo Final

O protótipo experimental do sistema embarcado é apresentado na Figura 25, na qual ilustra a montagem real. O protótipo funcionou de acordo com os fluxogramas apresentados.

Figura 25 – Protótipo de *Hardware* Final



Fonte: (AUTORIA PRÓPRIA, 2020)

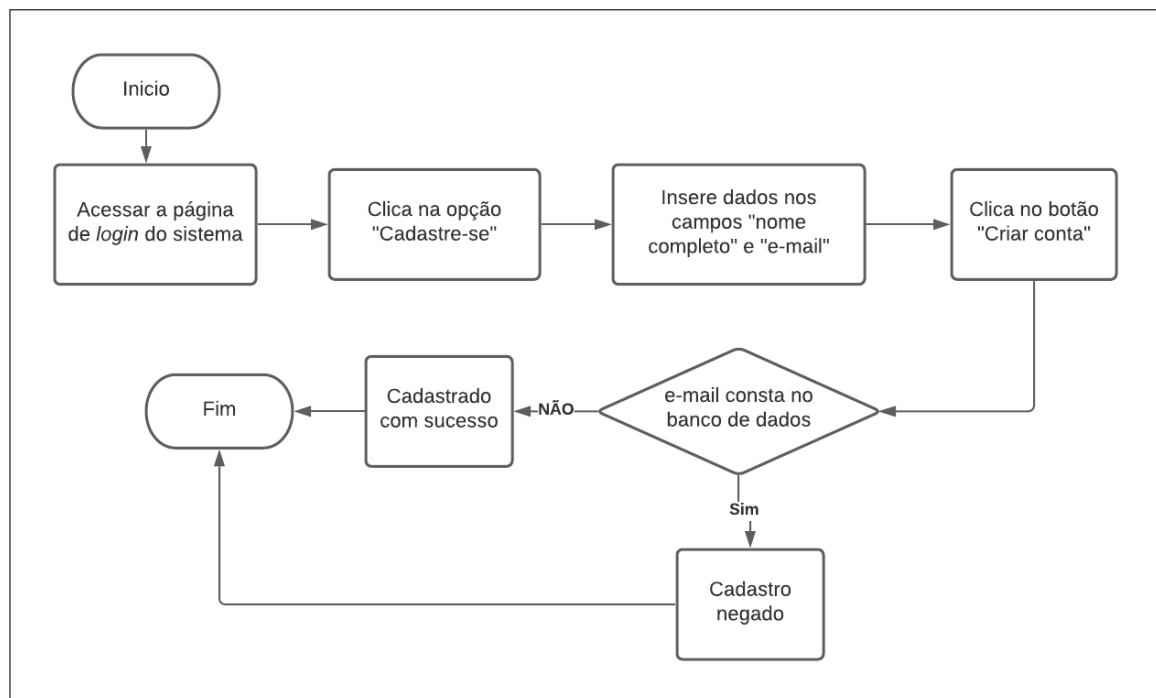
5.3 FUNCIONAMENTO DO SISTEMA

Nesta seção é descrito o funcionamento de alguns serviços fornecidos pelo sistema descrito neste trabalho, sendo estes, cadastro de usuários, cadastro de *tags* e gerar relatório, afim de exemplificar e ilustrar as ações necessitadas sua usabilidade.

5.3.1 Cadastro de Usuário

A funcionalidade de cadastramento de novos usuários é feita por pessoas associadas aos grupo de pesquisa, que não são coordenadores (administradores). Na Figura 26 são ilustradas as ações necessárias para o cadastro de usuários. Ao iniciar, o usuário acessa a página de *login* do sistema, onde são exibidos os dados ilustrados na Figura 14, dessa forma, ao clicar na opção de “Cadastre-se” o usuário é redirecionado para a tela de cadastro apresentada na Figura 15 e insere seus dados nos campos “nome completo” e “e-mail”, após clicar no botão “Criar conta” a aplicação faz a verificação dos dados, caso o e-mail não conste no banco de dados o usuário é cadastrado com sucesso, finalizando assim a ação. Analogamente, caso o e-mail conste no banco de dados, a solicitação é negada, finalizando assim a ação.

Figura 26 – Fluxograma do Cadastro de Usuários



Fonte: (AUTORIA PRÓPRIA, 2020)

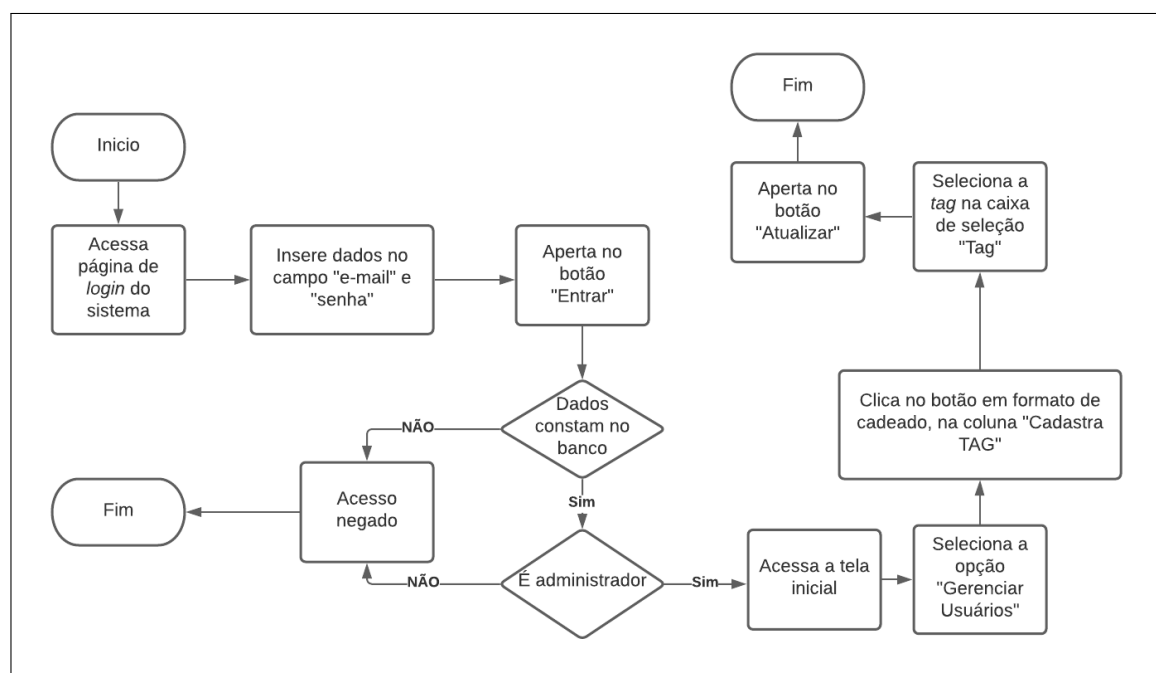
5.3.2 Cadastro de Tags

A funcionalidade de cadastro de *tags* foi projetada para a liberação do acesso dos usuários cadastrados da forma apresentada na subseção anterior. Essa ação só pode ser feita pelos coordenadores (administradores). Na Figura 27 são ilustradas as ações necessárias para o cadastro de *tags*, no qual ao iniciar, o usuário acessa a tela de *login* do sistema, insere seus dados

nos campos “e-mail” e “senha”. Ao pressionar o botão “Entrar” a aplicação verifica se os dados constam no banco, caso o resultado seja negativo, a solicitação é negada e a ação é finalizada. Caso o resultado da consulta seja positivo, a aplicação verifica se os dados são de um usuário administrador, se o resultado for positivo a tela inicial apresentada na Figura 17 é exibida, sendo assim, o usuário seleciona a opção “Gerenciar Usuários” onde a tela apresentada na Figura 18 é exibida. Portanto, ao clicar no ícone de cadeado, situado na coluna “Cadastra TAG” que é referente ao usuário no qual deseja-se associar uma nova *tag*, o usuário é redirecionado para a tela apresentada na Figura 20, selecionando a *tag* que fica disponível no campo de seleção “Tag”. Ao pressionar o botão “Atualizar” uma *tag* é associada ao usuário escolhido e a ação é finalizada. Entretanto, se o resultado da consulta de dados, na aplicação, informar que o usuário não é um administrador, sua solicitação é negada e a ação é finalizada.

As ações feitas pelo sistema embarcado para tornar a *tag* disponível para cadastro é apresentado na seção 5.2.

Figura 27 – Fluxograma do Cadastro de *Tag*



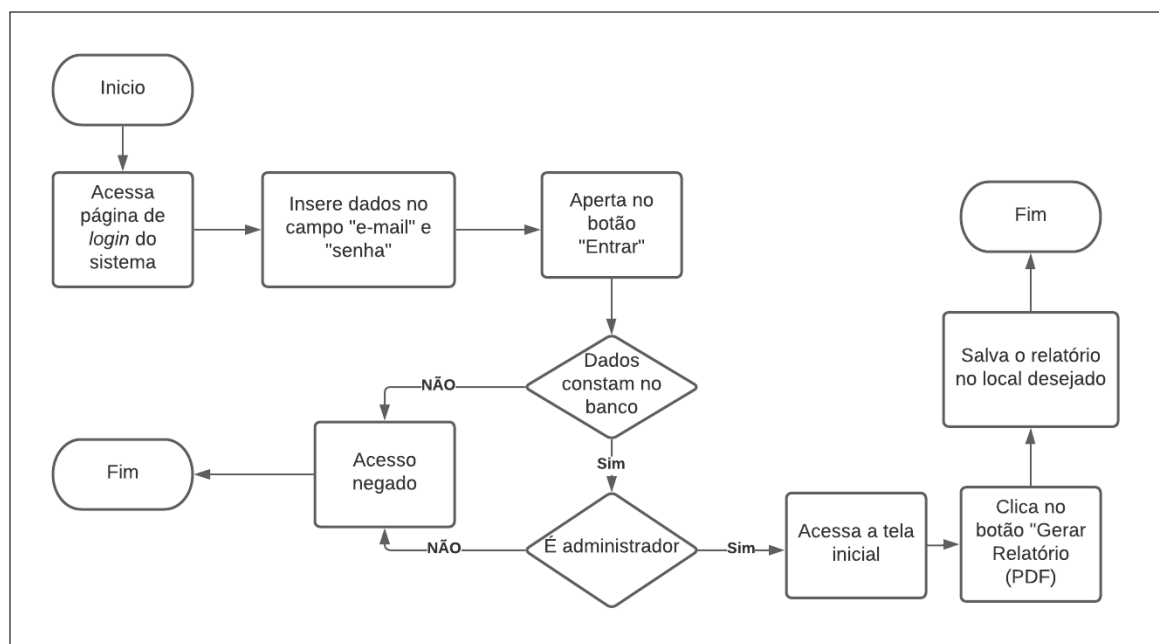
Fonte: (AUTORIA PRÓPRIA, 2020)

5.3.3 Gerar Relatório

A funcionalidade de gerar relatório foi projetada para disponibilizar os registros de acessos no formato impresso ou em formato PDF. Essa ação só pode ser feita pelos coordenadores

(administradores). Analogamente aos passos descritos na subseção anterior, na Figura 28 são ilustradas as ações necessárias para a geração de relatório, no qual ao iniciar, o usuário acessa a tela de *login* do sistema, apresentada na Figura 14, insere seus dados nos campos “e-mail” e “senha”. Ao pressionar o botão “Entrar” a aplicação verifica se os dados constam no banco, caso o resultado seja negativo, a solicitação é negada e a ação é finalizada. Caso o resultado da consulta seja positivo, a aplicação verifica se os dados são de um usuário administrador, se o resultado for positivo, a tela inicial apresentada na Figura 17 é exibida. O usuário clica no botão “Gerar Relatório (PDF)”, salva no local desejado e finaliza sua ação. Em caso de resultado negativo, ou seja, se a aplicação verificar que o usuário não é um administrador, sua solicitação é negada e a ação é finalizada.

Figura 28 – Fluxograma da Geração de Relatórios



Fonte: (AUTORIA PRÓPRIA, 2020)

6 CONCLUSÃO

Neste trabalho foi desenvolvido um sistema geral que conecta *hardware* e *software* para controle de acesso automático de ambientes utilizando a tecnologia RFID. O sistema foi desenvolvido para solucionar a problemática da ausência de registro e de controle de acesso ao laboratório do Grupo de Pesquisa em Sistemas Críticos de Segurança (GPSiCS), para um controle seguro e viável do ambiente e dos usuários. Porém, é importante destacar que o sistema desenvolvido pode ser aplicado a qualquer ambiente que necessite de controle de acesso automático.

O sistema GPACCESS foi criado para a plataforma *web* utilizando linguagens de programações atuais. O uso de dispositivos discretos como Arduino, RFID, ESP8266 proporcionaram a criação de um sistema prático e viável de ser aplicado e replicado, englobando automação, que pode ser aplicado a diversos contextos como a indústria 4.0. Dessa forma, pode-se destacar que o trabalho trouxe contribuições importantes a universidade e o grupo de pesquisa.

Os resultados do sistema embarcado cumpriu as funcionalidades projetadas, obtendo sucesso em todos os serviços. O sistema *web* cumpriu todos os requisitos levantados. A interface trouxe melhorias quando comparada as telas prototipadas, tais como uma nova logo, visual técnico aprimorado, retirada de algumas entradas de dados que não foram mais necessárias e a opção de cadastro de *tags* para novos usuários, tornando a parte visual uma ferramenta com melhor usabilidade.

A implementação física no laboratório do GPSiCS não ocorreu devido a pandemia da COVID-19, sendo assim, foi adiado até que fosse possível de ser implementada com segurança, dentro do retorno das atividades presenciais da universidade.

Algumas das dificuldades enfrentadas foram em relação montagem, devido a falta da estrutura física de laboratório, porém possível de ser superada com a aquisição dos componentes.

Como sugestão de trabalhos futuros, além da validação do sistema no espaço físico do GPSiCS, o sistema inicial pode ser melhorado tanto em relação a montagem física, como em relação a programação. Novas funcionalidades podem ser adicionadas como: o acionamento dos dispositivos eletrônicos do ambiente apenas quando o ambiente estiver sendo utilizado; a criação de um aplicativo *mobile* para que os usuários que não são coordenadores do grupo de pesquisa possam visualizar seus acessos.

REFERÊNCIAS

- ALLAH, O. A.; ABDALLA, S.; MEKKI, M.; AWADALLAH, A. Rfid based access control and registration system. In: **2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)**. [S.l.: s.n.], 2018. p. 1–4.
- BAJRAMI, X.; MURTURI, I. An efficient approach to monitoring environmental conditions using a wireless sensor network and NodeMCU. **e & i Elektrotechnik und Informationstechnik**, Springer Science and Business Media LLC, v. 135, n. 3, p. 294–301, abr. 2018. Disponível em: <<https://doi.org/10.1007/s00502-018-0612-9>>.
- BAUDAELETRONICA. **Kit RFID RC-522 / 13,56 MHz**. 2020. [Online; accessed 24-novembro-2020]. Disponível em: <<https://www.baudaeletronica.com.br/kit-rfid-rc-522-13-56-mhz.html>>.
- DENG, F.; HE, Y.; LI, B.; SONG, Y.; WU, X. Design of a slotted chipless RFID humidity sensor tag. **Sensors and Actuators B: Chemical**, Elsevier BV, v. 264, p. 255–262, jul. 2018. Disponível em: <<https://doi.org/10.1016/j.snb.2018.02.153>>.
- DOLINAY, J.; DOSTÁLEK, P.; VAŠEK, V. Arduino debugger. **IEEE Embedded Systems Letters**, v. 8, n. 4, p. 85–88, 2016.
- ELETROGATE. **NodeMCU v3 Lolin - Kit de Desenvolvimento com ESP8266 baseado em LUA**. 2020. [Online; accessed 24-novembro-2020]. Disponível em: <<https://www.eletrogate.com/nodemcu-v3-lolin-kit-de-desenvolvimento-com-esp8266-baseado-em-lua>>.
- FAROOQ, U.; HASAN, M. ul; AMAR, M.; HANIF, A.; ASAD, M. U. RFID based security and access control system. **International Journal of Engineering and Technology**, IACSIT Press, p. 309–314, 2014. Disponível em: <<https://doi.org/10.7763/ijet.2014.v6.718>>.
- FERNANDES, A. C.; MAGALHÃES, I. N. D. de; SOUZA, M. A.; JUNIOR, A. G. da C.; MOREIRA, C. S. Sistema de aquisição de sinais ECG processado pelo LabVIEW com comunicação wi-fi por meio do módulo ESP8266. **Revista Principia - Divulgação Científica e Tecnológica do IFPB**, Instituto Federal de Educacao, Ciencia e Tecnologia da Paraiba, v. 1, n. 34, p. 62, jun. 2017. Disponível em: <<https://doi.org/10.18265/1517-03062015v1n34p62-68>>.
- JIA, X.; FENG, Q.; FAN, T.; LEI, Q. RFID technology and its applications in internet of things (IoT). In: **2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)**. IEEE, 2012. Disponível em: <<https://doi.org/10.1109/cecn.2012.6201508>>.
- KAMALUDIN, H.; MAHDIN, H.; ABAWAJY, J. H. Clone tag detection in distributed RFID systems. **PLOS ONE**, Public Library of Science (PLoS), v. 13, n. 3, p. e0193951, mar. 2018. Disponível em: <<https://doi.org/10.1371/journal.pone.0193951>>.
- KOULAMAS, C.; LAZARESCU, M. Real-time embedded systems: Present and future. **Electronics**, MDPI AG, v. 7, n. 9, p. 205, set. 2018. Disponível em: <<https://doi.org/10.3390/electronics7090205>>.
- LIU, C. C.; CHANG, C.-H.; SU, M.-C.; CHU, H.-T.; HUNG, S.-H.; WONG, J.-M.; WANG, P.-C. RFID-initiated workflow control to facilitate patient safety and utilization efficiency in operation theater. **Computer Methods and Programs in Biomedicine**, Elsevier BV, v. 104, n. 3, p. 435–442, dez. 2011. Disponível em: <<https://doi.org/10.1016/j.cmpb.2010.08.017>>.

MCROBERTS, M. **Arduino Básico**. São Paulo: Novatec Editora: [s.n.], 2011. 456 p.

OSSADA, J. C.; MARTINS, L. E. G. **GERSE: Guia para Elicitação de Requisitos de Sistemas Embarcados**. Unpublished, 2014. Disponível em: <<http://rgdoi.net/10.13140/RG.2.2.33660.03203>>.

POURSAFAEI, F.; BAZZAZ, M.; KAFSHDOOZ, M. M.; EJLALI, A. Slack clustering for scheduling frame-based tasks on multicore embedded systems. **Microelectronics Journal**, Elsevier BV, v. 81, p. 144–153, nov. 2018. Disponível em: <<https://doi.org/10.1016/j.mejo.2018.09.002>>.

SILVA, D. S. da. **Técnica de Detecção de Falhas de Escalonamento de Tarefas em Sistemas Embarcados Baseados em Sistemas Operacionais de Tempo Real**. 77 f. Dissertação (Pós-Graduação em Engenharia Elétrica) — Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2011.

VASCONCELOS, M. D. **UMA ARQUITETURA DE SEGURANÇA PARA SISTEMAS EMBARCADOS VIRTUALIZADOS**. 79 f. Dissertação (Pós-Graduação em Ciência da Computação) — Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2017.

VERMA, G. K.; TRIPATHI, P. A digital security system with door lock system using RFID technology. **International Journal of Computer Applications**, Foundation of Computer Science, v. 5, n. 11, p. 6–8, ago. 2010. Disponível em: <<https://doi.org/10.5120/957-1334>>.

WANT, R. An introduction to RFID technology. **IEEE Pervasive Computing**, Institute of Electrical and Electronics Engineers (IEEE), v. 5, n. 1, p. 25–33, jan. 2006. Disponível em: <<https://doi.org/10.1109/mprv.2006.2>>.

WIKIPEDIA. **Arduino — Wikipédia, a enciclopédia livre**. 2020. [Online; Acessado em: 24 nov. 2020]. Disponível em: <<https://pt.wikipedia.org/w/index.php?title=Arduino&oldid=59579797>>.