VÍCTOR CARDOSO SENA MAIA

WESLLEY RIBEIRO CAMILO

UMA SOLUÇÃO INTEGRADA DE CONTROLE E MONITORAMENTO DE ACESSO FÍSICO PARA O CAMPUS DA UFLA

LAVRAS – MG

2022

VÍCTOR CARDOSO SENA MAIA
WESLLEY RIBEIRO CAMILO

UMA SOLUÇÃO INTEGRADA DE CONTROLE E MONITORAMENTO DE ACESSO FÍSICO PARA O CAMPUS DA UFLA

Trabalho de conclusão de curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Engenharia de Controle e Automação, para obtenção do título Bacharel.

Prof. Dr. Neumar Costa Malheiros
Orientador

LAVRAS – MG
2022

VÍCTOR CARDOSO SENA MAIA
WESLLEY RIBEIRO CAMILO

UMA SOLUÇÃO INTEGRADA DE CONTROLE E MONITORAMENTO DE ACESSO FÍSICO PARA O CAMPUS DA UFLA

Trabalho de conclusão de curso apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Engenharia de Controle e Automação, para obtenção do título Bacharel.

APROVADA em 16 de Setembro de 2022.

Prof. Dr. Danilo Alves de Lima	UFLA
MSc. Anderson Bernardo dos Santos	UFLA

Prof. Dr. Neumar Costa Malheiros
Orientador

LAVRAS – MG
2022

Nós dedicamos este trabalho a Deus e a nossa família. Somente o conhecimento acadêmico não seria suficiente para a finalização deste trabalho, se chegamos aqui foi porque recebemos seu amor, suporte e conselho, nossa eterna gratidão.

AGRADECIMENTOS

Nosso agradecimento é direcionado primeiramente ao Anderson Bernardo dos Santos que nos deu a oportunidade de desenvolver esse projeto e aplicá-lo na Universidade. Nosso muito obrigado pela confiança e contribuição com a nossa formação acadêmica. Também, nosso segundo agradecimento é direcionado ao Professor Dr. Neumar Costa Malheiros que aceitou de bom grado o desafio de nos orientar no desenvolvimento deste trabalho acadêmico, seu apoio e dedicação foram fundamentais para nos manter motivados e conseguir concluir este trabalho. Por fim o último agradecimento é dedicado a todos os professores que contribuíram com a nossa formação, por meio do conhecimento e experiências compartilhadas nos tornamos capazes de finalizar esse processo.

RESUMO

Este trabalho apresenta uma solução de controle e monitoramento de acesso físico desenvolvido para a Universidade Federal de Lavras. O sistema utiliza a tecnologia RFID para a identificação de pessoas e também se comunica com uma aplicação Web desenvolvida para permitir o monitoramento e cadastro de pessoas em tempo real por meio de requisições HTTP e registro de acesso em banco de dados. No trabalho, é descrito o projeto do hardware e software do dispositivo para o controle de acesso físico e também uma apresentação da aplicação Web com as suas funcionalidades. São apresentados os testes realizados para validação da solução, incluindo teste de bancada, teste em ambiente controlado e, por fim, teste em ambiente relevante.

Palavras-chave: Sistemas Embarcados. RFID. Controle de Acesso Físico Automatizado.

ABSTRACT

This work presents a physical access control and monitoring system developed for the Federal University of Lavras. The system uses RFID technology to identify people and also communicates with a Web application developed to allow real-time monitoring and registration of people through HTTP requests. The work describes the hardware and software design of the device for access control and also a presentation of the Web application with its functionalities. The tests performed to validate the solution are presented, including bench testing, testing in a controlled environment and, finally, testing in a relevant environment.

Keywords: Embedded systems. RFID. Access control.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os sistemas de controle de acesso tem como objetivo restringir o acesso a ambientes físicos ou virtuais. Em ambos os contextos, a ideia é identificar o indivíduo de modo a permitir ou bloquear o acesso ao ambiente protegido. A fim de comprovar a identidade do usuário, existem duas principais opções: identificar o usuário por aquilo que somente ele sabe ou por meio do que apenas ele possui.

Identificar o usuário por aquilo que somente ele sabe é a forma mais utilizada de controle de acesso a ambientes virtuais. Para isso, são utilizadas diferentes informações como uso de senhas numéricas, alfanuméricas, desenhos, informações pessoais, dentre outras. A outra maneira de identificar o usuário é por aquilo que somente ele tem, seja pelas características únicas do indivíduo, como por exemplo fisionomia, timbre da voz e digital ou por objetos que somente ele possui como por exemplo chave, cartão e telefone celular.

Especificamente para o sistema de controle de acesso físico, existe ainda a necessidade de atuar na porta/portão de modo a bloquear ou a permitir que o usuário acesse ao local controlado. Esse processo pode ser feito integrando ao porta/portão sistemas mecânicos, elétricos ou eletromecânicos. Nos sistemas mecânicos, um conjunto de engrenagens é responsável por movimentar uma trava que irá bloquear a porta. Nos sistemas elétricos, um eletroímã é usado para segurar a porta usando a força eletromagnética e nos eletromecânicos, podem ser usados motores ou eletroímãs para mover a trava.

A Universidade Federal de Lavras possui diversas salas e laboratórios para a realização de atividades acadêmicas. Em ambos os ambientes, existem equipamentos para dar suporte à execução das atividades. Por exemplo, nas salas de aula, são disponibilizados aos professores aparelho projetor e computador. Nos laboratórios, os equipamentos variam de acordo com as áreas do conhecimento, se tratando principalmente de produtos químicos, computadores, equipamentos de medição e teste.

Existem diferentes estratégias com a finalidade de se manter a integridade dos equipamentos, assim como evitar roubo ou furto desses. No caso das salas de aula, elas permanecem abertas durante o horário de funcionamento da Universidade e depois são fechadas pelos seguranças. Por esse motivo, os equipamentos disponibilizados ao professor são mantidos em um pequeno armário trancado com cadeado. Assim, para ter acesso aos equipamentos, o professor deve se dirigir a um local específico onde são entregues as chaves dos armários. Nesse local, trabalham técnicos da Universidade responsáveis pelo controle das chaves. Eles verificam se o professor tem direito à chave e registram o empréstimo das chaves, como uma forma de monitorar o uso dos ambientes e equipamentos, com a identificação dos responsáveis.

Em relação aos laboratórios, há um técnico responsável por um ou por vários deles, e é responsabilidade desse técnico monitorar o ambiente. Quando um estudante precisa ter acesso ao laboratório fora do horário de trabalho do técnico, um procedimento parecido com o das salas de aula é realizado. A chave é emprestada ao aluno que se torna responsável pelo laboratório durante o período que detêm a chave.

Sobre essa abordagem para controle das salas, pode-se fazer algumas considerações:

- São necessários vários funcionários para realizar o controle das chaves dos armários das salas de aula.
- Em todos os dias letivos, a equipe de vigilantes é responsável por abrir e fechar todas as salas dos pavilhões de aulas.
- Os professores precisam se deslocar até a sala de empréstimo de chaves, em muitos casos, muito distante da sala que irão lecionar a aula.
- Como as salas de aula ficam destrancadas, é comum que alunos movam cadeiras ou mesas de uma sala para outra. Essa ação gera dois principais

problemas. O primeiro deles é a má alocação de cadeiras, excesso ou falta delas em salas de aula, uma vez que não são devolvidas para o mesmo local. Segundo, dificulta o processo de controle de patrimônio da Universidade. Isso se deve ao fato de que a mudança não autorizada de bens entre os locais gera inconsistências no sistema de controle de patrimônio.

Em relação ao controle de laboratórios, outras considerações são também relevantes:

- Grande parte dos laboratórios possuem equipamentos de custo elevado, tornando um investimento em um sistema de controle de acesso atrativo.
- Existem equipamentos dentro dos laboratórios que devem ser usados apenas por pessoas qualificadas de modo a preservar a integridade do equipamento e do usuário.
- Existe a necessidade do uso dos laboratórios fora do horário comercial para execução de atividades de disciplinas, projetos de pesquisa e extensão.

1.1 Objetivos

A fim de contornar as dificuldades apresentadas na seção anterior, o objetivo deste trabalho é implementar um sistema de controle de acesso para atender as necessidades da Universidade. Esse sistema irá utilizar um recurso disponível a todos os membros da instituição para o processo de identificação, que é o cartão RFID. Além disso para se adaptar as mudanças na lista de pessoas autorizadas a acessar cada ambiente, o sistema irá permitir o cadastro de pessoas em tempo real e de maneira remota. Com o objetivo de aumentar a segurança de cada ambiente será armazenado o histórico de acesso de cada ambiente de maneira remota. A representação desse sistema é mostrada na Figura 1.1.

O sistema possui três diferentes ambientes. O primeiro deles, representado ao lado esquerdo, é o Ambiente do espaço controlado. Nesse ambiente, é

Figura 1.1 – Visão geral da proposta de sistema de controle.

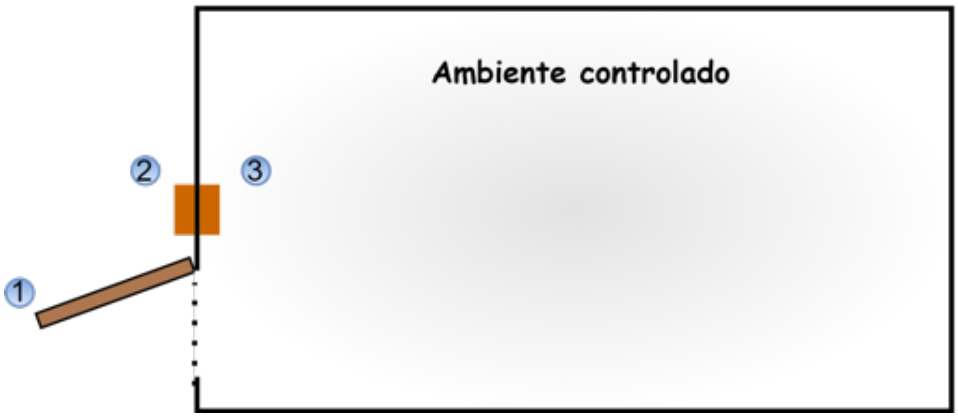
Fonte: Dos autores (2022).

instalado o dispositivo físico (2) que identifica o usuário (1) pelo seu cartão RFID (Identificação por radiofrequência) e destrava a porta, por meio de comandos ao atuador (3). Esse sistema também recebe atualizações de usuários que têm acesso a esse ambiente. Do lado direito da figura, está representado o Ambiente Gerencial. Nele, o gestor da aplicação (4) inclui ou exclui o cadastro de usuários com acesso autorizado aos ambientes controlados. Também nesse mesmo ambiente, o gestor consegue acompanhar, em tempo real, o histórico de acessos a cada ambiente. O elemento central desse sistema é o Servidor que estabelece a integração com esses dois ambientes. É por meio desse servidor que o dispositivo consegue receber as atualizações dos usuários e o gestor obtém o histórico de acesso.

A Figura1.2 representa em mais detalhes o ambiente do espaço controlado. Como pode ser observado, existem dois leitores de cartão: a) o exterior(2), usado para destravar a porta (1) e entrar no ambiente; b) e o interior(3), usado para sair do ambiente. Dessa forma, por esses dois sensores, é possível determinar quanto tempo o usuário permaneceu no local.

A partir do objetivo geral deste trabalho estabelecesse como objetivo específico projetar e desenvolver um protótipo funcional que possa ser testado em ambiente relevante onde deverá identificar o usuário por meio do cartão de mem-

Figura 1.2 – Visão superior do ambiente controlado, onde em (2) e em (3) tem-se os leitores interno e externo respectivamente,e em (1) a porta.



Fonte: Dos autores (2022).

bro da Universidade e liberar ou bloquear a porta de acordo com a permissão do usuário. Além disso, esse sistema deverá ser capaz de atualizar essa lista de usuários de maneira remota sempre que houver uma solicitações do gestor da aplicação. É dever deste protótipo enviar ao gestor os registros de acesso a medida que forem acontecendo. Também é objetivo desse trabalho, o desenvolvimento de uma aplicação para receber os dados enviados pelo protótipo e receber as solicitações do gestor.

1.2 Organização do Texto

Este trabalho seguiu a estrutura de projeto de Concepção Básica, na qual foi encontrado um ponto de melhoria, desenvolvido uma solução para melhorar o processo e, por fim, realizou-se uma análise da melhoria proposta.

O trabalho é composto por cinco capítulos, a saber: Introdução, Referencial Teórico, Solução Proposta, Discussão dos Resultados e Considerações Finais. O Capítulo 2 aborda os termos chaves deste trabalho, de modo a contribuir para a compreensão da solução proposta. A solução proposta por sua vez é apresentada em detalhes no Capítulo 3. É descrito o processo de desenvolvimento desse

sistema, considerando-se seus diversos elementos: hardware, software embarcado e, por fim, a aplicação Web. No Capítulo 4, são discutidos os resultados desse trabalho, com apresentação dos testes realizados para validação da aplicação, incluindo os testes de bancada e a aplicação desse sistema em um ambiente real na Universidade. Como última parte, é feita uma comparação entre o sistema desenvolvido e algumas soluções disponíveis no mercado. As considerações finais, no Capítulo 5, apresentam uma comparação entre o resultado esperado e o obtido, bem como possíveis avanços no projeto.

2 REFERENCIAL TEÓRICO

Neste capítulo, são apresentados termos e tecnologias necessários para o entendimento da solução proposta. Incluindo uma descrição do conceito de Sistemas embarcados, bobina eletromagnética, o protocolo de comunicação SPI e uma sobre a tecnologia RFID.

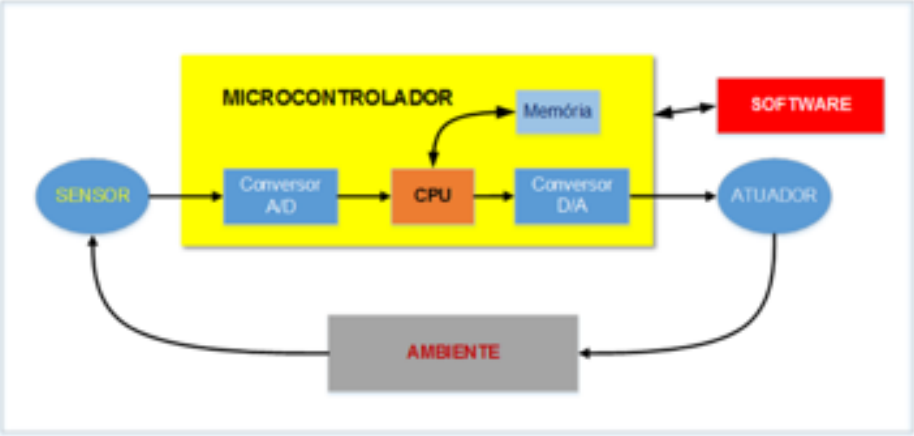
2.1 Sistemas Embarcados

Sistemas embarcados são sistemas eletrônicos com microcontroladores desenvolvidos para atender a uma função específica e, geralmente, possuem restrições de recursos como memória, velocidade de processamento ou número de interfaces de entrada e saída de dados. Outras características de um sistema embarcado são: ser de tamanho reduzido, possuir baixo consumo de energia e ser robusto (ALMEIDA; MORAES; SERAPHIM, 2017).

Tais sistemas possuem diversas aplicações, principalmente em automação industrial, residencial, eletrodomésticos, entre outros. Basicamente, conforme pode ser visto na Figura 2.1, um sistema embarcado é composto por um microcontrolador, interfaces de entrada e saída para interação com o usuário, fonte de alimentação e módulos periféricos que implementam funcionalidades extras ao microcontrolador.

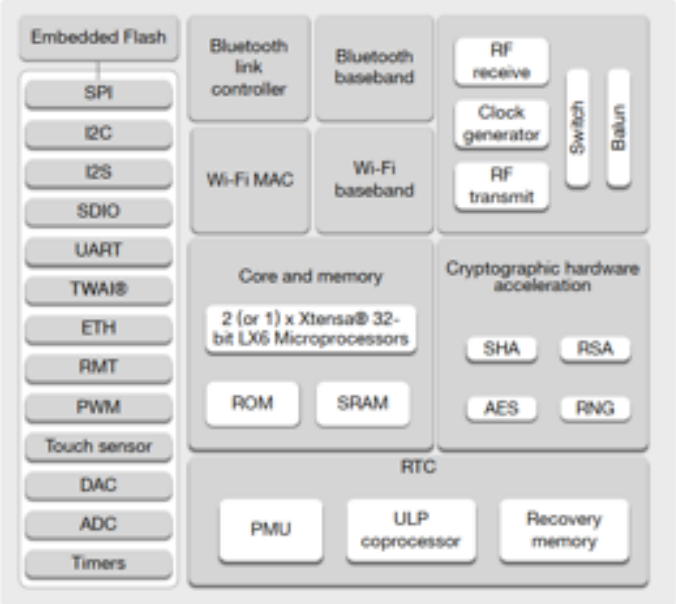
Diferente de um microprocessador, conforme pode ser observado na Figura 2.2, o circuito integrado de um microcontrolador é composto por todos os periféricos básicos necessários para o seu funcionamento, como memórias, barramentos, conversores de sinais analógico/digital, temporizadores e portas de comunicação. Devido a essas características, a programação de um microcontrolador é diferente da convencional, que executa sob o controle e suporte de um sistema operacional. Assim, na programação de microcontroladores, é necessário que o programador tenha conhecimento das relações básicas entre os componentes e o código seja compilado especificamente para o modelo do chip embarcado.

Figura 2.1 – Diagrama ilustrativo de um sistema embarcado.



Fonte: (TEIXEIRA; CAMPOS, 2019)

Figura 2.2 – Diagrama representando os componentes interno de um ESP32.



Fonte:(SYSTEMS, 2015)

A programação do microcontrolador pode ser realizada de diversas maneiras, com o uso de IDE para compilação e a disponibilidade do kit de desenvolvimento de software (SDK). Geralmente a linguagem de programação utilizada é

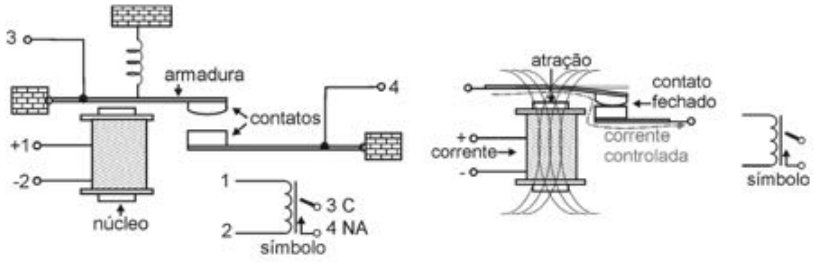
C/C++ devido à caraterística de produzir softwares otimizados para o microprocesador, com a vantagem de melhor acesso aos recursos de hardware, flexibilidade, performance e implementar os conceitos de Orientação a Objeto, os quais facilitam a manutenção e o reuso do código (CURVELLO et al., 2015).

2.2 Bobina Eletromagnética

O eletroímã é um dispositivo eletromecânico capaz de gerar campo magnético quando uma corrente elétrica passa em suas bobinas. Ele é composto por um núcleo de ferro e uma solenoide, conforme ilustrado na Figura 2.4.

O relé eletromecânico é utilizado como interface de acionamento de cargas, separando o circuito de potência do circuito de acionamento. Seu funcionamento é semelhante ao do eletroímã e de acordo com a Figura 2.3, o relé possui cinco terminais, sendo dois para acionamento da bobina e os terminais normalmente aberto (NA), normalmente fechado (NF) e o comum. Ao aplicar uma tensão na bobina, o núcleo móvel realiza a comutação dos contatos.

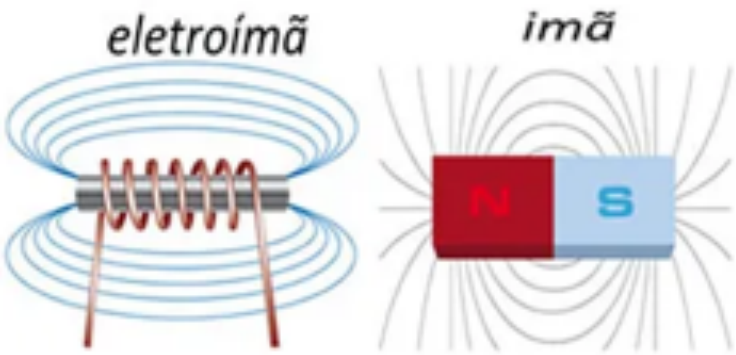
Figura 2.3 – Funcionamento do relé para acionamento de carga.



Fonte:Adaptado (BRAGA, 2009)

Ao aplicar uma tensão nos terminais da solenoide, uma corrente é induzida no circuito devido à diferença de potencial, gerando um campo magnético semelhante ao produzido por ímãs permanentes. Em uma fechadura eletromagnética ao ser acionada, é o fluxo magnético que atrai placa de armadura e realizar a ação de bloqueio.

Figura 2.4 – Linhas de campo magnético produzidas no eletroimã.



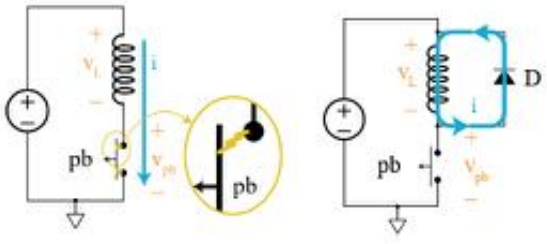
Fonte:Adaptado (FERREIRA, 2021)

Do ponto de vista elétrico a solenoide é representada por um indutor e possui uma indutância (L). E, conforme representado na Figura 2.5, a tensão no indutor (v) é proporcional ao valor de indutância e a variação da corrente ao longo do tempo.

Isso causa o aparecimento de valores de tensões elevadas no momento em que o relé ou a fechadura eletromecânica é desenergizado e pode queimar o transistor de acionamento em circuito eletrônico. A solução, neste caso, é inserir no circuito um diodo de roda livre em paralelo com o indutor, permitindo que a corrente flua pelo circuito até ser dissipada pela resistência dos componentes.

Figura 2.5 – Comportamento do indutor no circuito.

$$v = \mathrm{L}\frac{di}{dt}$$



Fonte:Adaptado (Khan Academy, 2016)

2.3 Protocolo de Comunicação SPI

Os protocolos de comunicação são utilizados nos sistemas embarcados para transporte de dados e comunicação dos dispositivos. Os protocolos podem ser subdivididos entre síncrono e assíncronos. A principal diferença entre eles é a presença de um sinal de *clock* para sincronia durante a troca de dados. Para este trabalho, o protocolo síncrono SPI (*Serial Peripheral Interface*) se torna relevante, pois é utilizado para comunicação entre o módulo embarcado e o leitor RFID.

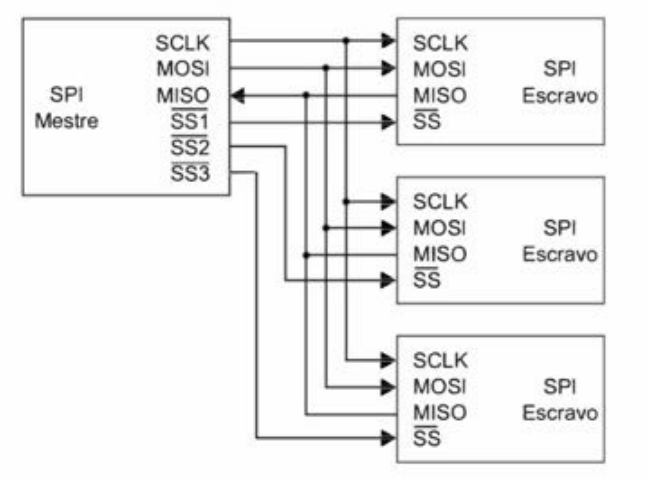
O protocolo *SPI* é baseado no conceito de mestre e escravo, sendo o microcontrolador do sistema embarcado atuando como mestre e os demais periféricos ligado ao barramento SPI são escravos. O protocolo utiliza obrigatoriamente um barramento de pelo menos 4 vias, sendo elas:

- *clock (CLK)*: utilizado para sincronizar a transmissão de dados entre os dispositivos. Este sinal somente pode ser gerado pelo mestre e a frequência do sinal deve ser compatível com o *clock* dos periféricos ligado ao barramento.
- *Master OUT Slave IN (MOSI)*: utilizado para envio de dados do mestre para o escravo.
- *Master IN Slave OUT (MISO)*: utilizado para envio de dados do escravo para os mestre.
- *Select (SS)*: utilizado para selecionar o dispositivo escravo para troca de dados e é ativo em nível lógico baixo.

Conforme representado na Figura 2.6, no protocolo SPI, as vias CLK, MOSI e MISO do barramento podem ser compartilhadas entre os dispositivos, mas é necessário uma via para cada dispositivo escravo ligado ao barramento.

Uma característica do protocolo SPI é a comunicação *full-duplex* entre mestre e escravo, realizando o envio e recebimento de dados com mesmo *clock*. Isso é possível devido aos barramentos de envio e recebimento de dados serem

Figura 2.6 – Ligação entre dispositivos com barramento SPI.



Fonte:(CURVELLO et al., 2015)

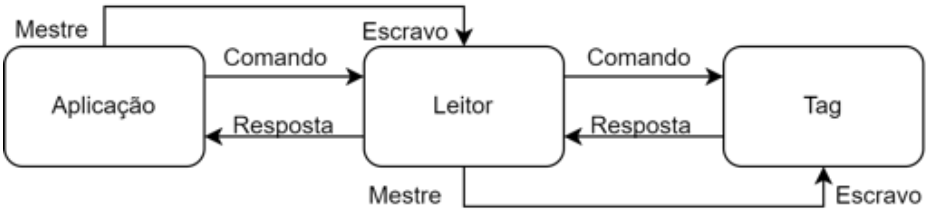
separados, permitindo uma comunicação mais rápida entre os dispositivos e podendo atingir uma taxa de até 2 Mbps (SACCO, 2014) e durante a troca de dados, os dispositivos ligados ao barramento e que estão com nível lógico alto no pino SS, devem manter o canal MISO no estado de alta impedância e não processar os dados recebidos no canal MOSI.

Dentre as limitações do protocolo SPI, podemos citar a ausência de verificação de erro (teste de paridade) nos dados transmitidos e de detecção dos dispositivos ligado ao barramento, sendo necessário implementar via *software*.

2.4 RFID

O acrônimo RFID (Radio Frequency Identification) tem sua origem na língua inglesa e pode ser traduzido como identificação por radiofrequência. Esse termo resume o objetivo da tecnologia, que é de conseguir identificar objetos por meio de ondas eletromagnéticas. De modo geral, os sistemas RFID são compostos por três principais componentes: a Tag, o Leitor e a Aplicação. A Figura 2.7 ilustra a função de cada componente e seu comportamento no sistema.

Figura 2.7 – Representação geral de um sistema RFID.



Fonte: Adaptado (JIA et al., 2012)

O primeiro elemento, representado ao lado direito da Figura 2.7, é a Tag[1]. Ela é o elemento chave do sistema RFID. Suas características e componentes dependem de cada aplicação, mas todas as aplicações possuem 2 elementos comuns: uma memória e uma antena. Essa Tag é fixada a algum objeto de modo que informações referentes ao objeto possam ser armazenadas nela. Assim, por meio de sua antena, ela é capaz de transmitir essas informações para o leitor.

A função do Leitor é se comunicar via radiofrequência com a Tag, de modo a extrair as informações armazenadas nela e transmiti-las para a aplicação via outro protocolo. Como pode ser observado na Figura 2.7, do ponto de vista de rede de comunicação, o par Leitor-Tag mantém uma relação de metre e escravo, na qual o Leitor, como mestre, detém o controle da comunicação. Assim, é do Leitor a responsabilidade pela integridade dos dados, aplicando para isso algoritmos de tratamento de colisões, criptografia e paridade.

O último elemento mostrado na Figura 2.7 é a aplicação. Ela representa o elemento do sistema que vai usufruir da informação armazenada na Tag. Geralmente, a aplicação pode ser um computador, celular, servidor ou um sistema embarcado. Em alguns casos, o leitor e a aplicação podem estar em um mesmo dispositivo.

[1] Alguns autores preferem traduzir o termo e utilizar a palavra etiqueta para se referir a ela. Porém, como o termo *tag* é mais comumente utilizado, ele foi adotado como padrão neste trabalho.

2.4.1 Classificação por Frequência

Os sistemas que usam a tecnologia RFID podem ser classificados segundo diversas características. Neste trabalho, seguiu-se o modelo proposto em (FENNANI; HAMAM; DAHMANE, 2011), que considera como critérios de classificação a frequência utilizada para transmissão do sinal.

Sabe-se que a frequência de transmissão de um sinal afeta diretamente algumas características importante do mesmo, como alcance, interferência com outros materiais e taxa de transmissão. De maneira geral e simplificada, sabe-se que quanto maior a frequência de um sinal menor é o tamanho da antena para emissão do sinal, menor a interferência com outros materiais e maior a velocidade de transmissão. Portanto, esse fator impacta diretamente onde o sistema será aplicado. Nesse contexto, os sistemas RFID são divididos em três grandes grupos: baixa frequência (LF – *Low Frequence*), alta frequência (HF – *High frequence*) e ultra alta frequência (UHF – *Ultra High Frequence*).

Baixa frequência (LF)

Os sistemas de baixa frequência estão compreendidos entre as faixas de 125 KHz e 134,2 KHz. Em especial, seu uso é aconselhável em ambientes com grande presença de água ou metal, uma vez que os dois outros grupos tem um pior desempenho nesses ambientes. A utilização do sistema em baixas frequências o torna mais suscetível a interferência com outros sinais de rádio, uma vez que existem uma série de outros equipamentos que compartilham dessa mesma faixa de frequência. Além disso, outro ponto negativo é que o comprimento de onda maior implica em uma antena maior, impactando no tamanho da *tag* e, consequentemente, no seu custo.

Ultra alta frequência (UHF)

Dentre as frequências de 300 MHz e 3GHz, estão compreendidos os dispositivos que operam em UHF. Estes apresentam as maiores velocidades de leitura e gravação das *tags*, sendo possível ler múltiplas tags ao mesmo tempo. Além disso, possuem maior alcance, em torno de 18 metros, e também tem tags menores e mais em conta, consequência do uso de frequências com baixo comprimento de onda.

Apesar dos pontos positivos apresentados, existem algumas limitações ao se utilizar essa faixa de frequência. A primeira é que ondas com essas frequências são facilmente absorvidas por seres vivos. Como ainda são incertas as consequências a longo prazo dessa exposição, existe uma legislação específica que define a potência máxima do sinal e também os lugares onde essas antenas podem ser instaladas, sendo que essa legislação varia entre os países.

Outro ponto é que, diferentemente da LF e HF, seu acoplamento não é indutivo, mas sim capacitivo. Nesse tipo de acoplamento, as ondas não são uniformemente distribuídas e pontos nulos de campo no espaço são formados, gerando regiões onde a *tag* não pode ser lida. Assim, para essa faixa de frequência, o posicionamento da antena é extremamente relevante, sendo, em alguns casos, necessário colocar mais de uma antena para cobrir todo o espaço.

Alta Frequência (HF)

Os dispositivos de alta frequência operam na faixa de 3MHz a 30MHz. Eles são os mais fabricados desde de 2001 uma vez que compartilham tanto benefícios dos LF quanto os dos UHF. Dentre esses benefícios, está uma velocidade de transmissão que permite a leitura de múltiplas tags e suporte a recursos de criptografia. Tem uma tolerância razoável a meios com a presença de metal e água, não possui regiões de campo nulo e tem um alcance de até 90 cm. A junção dessas

características faz com que as tags HF sejam as mais recomendadas para a grande maioria das aplicações.

2.5 Controle de Acesso Físico

Atualmente, existem diversas tecnologias disponíveis no mercado para realizar a identificação de pessoas e o controle de acesso em ambientes físicos de forma automatizada, tais como: o uso de senha, cartão de RFID, leitores biométricos e leitores faciais (MARCONDES, 2021). Alguns exemplos de soluções comerciais são apresentados na Figura 2.8.

Figura 2.8 – Identificação e controle de acesso físico.

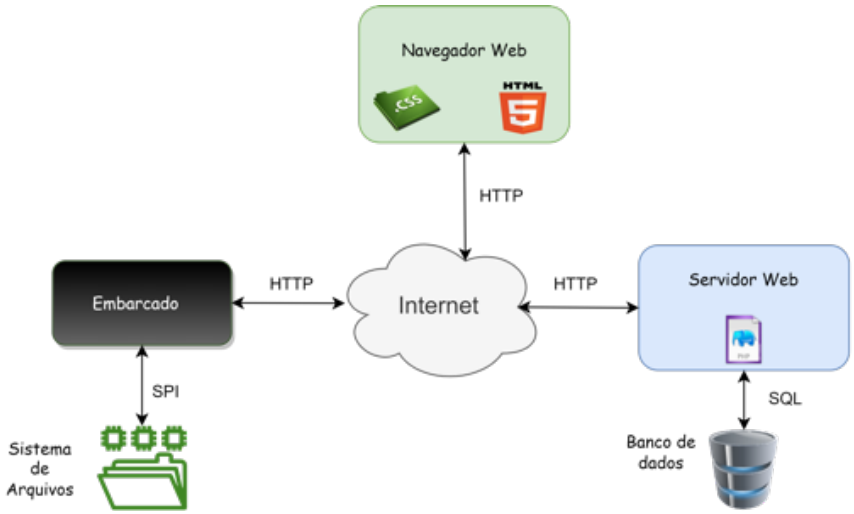
Fonte:(MARCONDES, 2021)

Sendo que existe modelos de sistemas que são monitoráveis sendo possível gerenciar, controlar e monitorar os acessos registrados. A escolha da tecnologia a ser adotada deve ser planejada de acordo com ambiente em que o sistema será instalado, número estimado de usuários e tipo de barreira física.

3 SOLUÇÃO PROPOSTA

Apresenta-se a seguir uma visão geral do projeto, que mostra os elementos que compõem o Sistema de Controle de Acesso, suas funções, e seus relacionamentos. Conforme representado na Figura 3.1, os componentes do Sistema de Controle de Acesso estão representados nos retângulos, sendo eles: o sistema embarcado, o navegador Web e o Servidor Web.

Figura 3.1 – Visão geral do sistema.



Fonte: Dos Autores (2022)

Com o objetivo de gerar uma maior praticidade para os gestores do Sistema, foi desenvolvida uma aplicação Web de modo a permitir a interação com o sistema por meio de qualquer dispositivo conectado à Internet. Na Figura 3.1, essa aplicação está representada por meio do Navegador Web e do Servidor Web. Por meio de um Navegador Web, o gestor da aplicação é capaz de visualizar as páginas HTML implementadas, e assim enviar as requisições para o servidor Web. O servidor Web portanto recebe as requisições Web vindas do Navegador, processa-as por meio do código PHP e envia a resposta novamente para o administrador. Como mostra a Figura 3.1, no servidor web também está armazenado o Banco de Dados

relacional desenvolvido para armazenar o histórico de acesso e a lista de usuários autorizada de cada ambiente.

O sistema embarcado, representado do lado esquerdo inferior na Figura3.1, é o dispositivo instalado no ambiente que realiza o controle de acesso. Também pelo diagrama, é possível notar que sistema embarcado possui um sistema de arquivos, no qual consegue armazenar os dados de maneira persistente.

Por fim, ainda em relação à Figura 3.1, é possível notar que a comunicação entre os elementos acontece por meio do protocolo HTTP. Esse protocolo, apesar de não ser o mais leve, é o mais utilizado, e, portanto, torna mais simples o processo de manutenção e integração da aplicação. Por usar, na camada de transporte, o protocolo TCP e seguir a arquitetura cliente servidor, sempre a comunicação entre o embarcado e o Servidor Web é iniciada pelo cliente, neste caso, o embarcado.

3.1 Projeto do Sistema Embarcado

Para o desenvolvimento do sistema embarcado, foram necessárias diversas etapas de estudo, projeto, prototipação e testes para validar o modelo proposto. Essas etapas envolveram também a pesquisa e aquisição dos componentes, simulação e montagem do circuito em *protoboard*, desenvolvimento dos algoritmos de teste e integração, confecção da placa de circuito impresso, teste de estabilidade do sistema, confecção da estrutura para o sistema embarcado em impressora 3D, desenvolvimento da aplicação web e implementação do código embarcado. Afim de melhorar o entendimento do sistema como um todo e evitar que os assuntos fiquem desconexos, algumas dessas etapas serão descritas em conjunto em uma mesma seção, ou de maneira implícita em outras, de modo a mostrar a progressão do desenvolvimento do projeto como um todo.

Para o projeto do sistema embarcado, primeiramente foi necessário definir seus elementos internos e a interface dele com os usuários. Os componentes escolhidos estão apresentados na Figura 3.2. Dentre eles, o eletroímã é o atua-

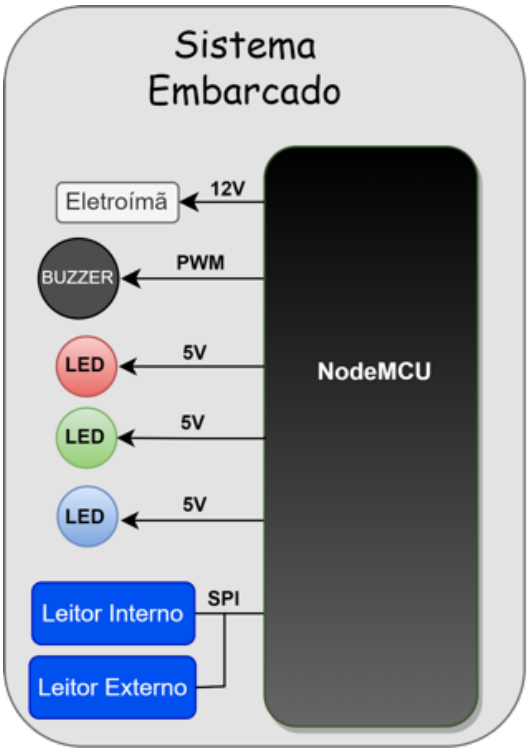
dor do sistema que tem a função de manter a porta travada e destrava-la quando solicitado. A escolha por um eletroímã, especificamente, foi devido ao seu comportamento em caso de falhas na alimentação do sistema. Essas falhas podem ser causadas pela falta de energia elétrica ou oscilações muito bruscas na rede elétrica. Diferentemente de outros atuadores, o eletroímã, em caso de falha, irá desbloquear a porta, requisito fundamental de segurança, uma vez que manter as pessoas trancadas dentro de um ambiente pode gerar uma situação de risco.

Obviamente, diversas outras abordagens poderiam ser utilizadas para que o sistema pudesse funcionar mesmo desconectado da rede elétrica. Porém, para essa aplicação em específico, considerou-se baixo o impacto causado por essa falha e foi decidido utilizar essa configuração de modo a reduzir a complexidade do sistema e o custo do projeto.

Ainda em relação à Figura3.2, os outros elementos dispostos abaixo do eletroímã representam a interface com o usuário. Os dois últimos, apresentados no diagrama como leitores, são os elementos utilizados para identificação do usuário. Esses elementos leem os dados armazenados no cartão do usuário e usam o ID para associa-los. A escolha por esse método de identificação foi motivada pelo fato de todos os membros da universidade (estudantes, técnicos, servidores e terceirizados) já possuírem um cartão com essa tecnologia e estarem cadastrados no banco de dados da universidade. Além disso, o uso de cartões RFID evita a formação de ilhas tecnológicas na instituição, permite que a solução proposta tenha mais viabilidade econômica e reduz despesas com manutenção. O leitor interno foi incluído com a finalidade principal de permitir ao sistema, em alguns casos, monitorar quanto tempo uma pessoa permaneceu dentro do ambiente e, consequentemente, um meio de motivá-la a conservar o patrimônio existente no ambiente.

Acima dos leitores, está o *LED* azul. Ele tem a função de informar ao usuário se o dispositivo está operando online ou offline. Essa informação é muito

Figura 3.2 – Componentes do Sistema Embarcado.



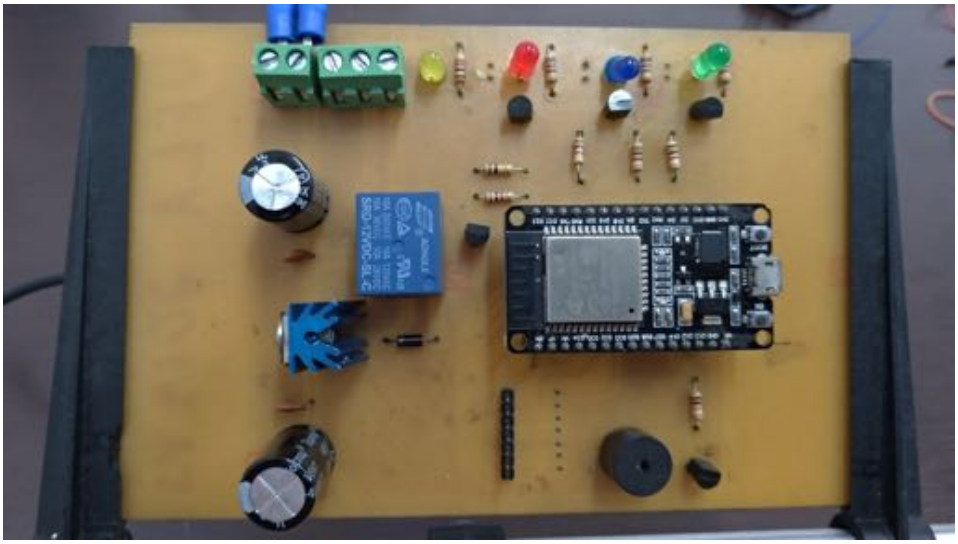
Fonte: Dos autores (2022).

importante no processo de identificação de possíveis falhas de comunicação com o servidor. Quando aceso, o *LED* indica que o sistema embarcado tem acesso à Internet e, quando apagado, indica que não tem acesso à Internet. Os elementos acima do *LED* azul tem funções semelhantes: avisar ao usuário se ele tem acesso ao ambiente ou não. Se o usuário está cadastrado, o *LED* verde acende e o *Buzzer* emite dois sinais sonoros curtos. Caso contrário, o *LED* vermelho acende e o *Buzzer* emite apenas um sinal contínuo. Essa configuração, com dois tipos diferentes de avisos (visual e sonoro), foi escolhida propositalmente, afim de que pessoas com deficiência visual ou auditiva também pudessem usar o sistema sem dificuldades. Para controlar todos os elementos mencionados anteriormente e ainda realizar

a comunicação com o Servidor foi escolhida a placa NodeMCU-ESP32 como microprocessador do sistema embarcado.

Uma vez finalizadas as etapas de dimensionamento dos componentes, teste de funcionamento na *protoboard* e validação do modelo, foi confeccionada a placa de circuito impresso (PCI), conforme ilustrada Figura 3.3. Posteriormente, foram realizados testes de integração e estabilidade do sistema.

Figura 3.3 – Placa de circuito do sistema de controle de acesso.



Fonte: Dos autores (2022).

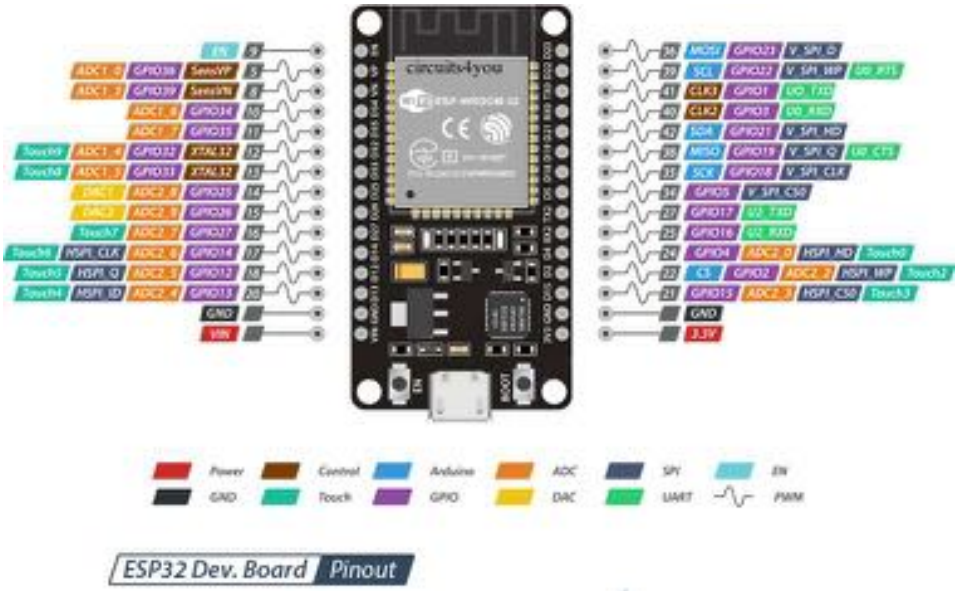
Para facilitar a montagem e a manutenção do sistema, nas conexões dos cabos de alimentação e do eletroimã foram utilizados bornes de fixação. Já para o barramento do módulo RFID, foi utilizada uma barra de pinos. Desse modo, no momento da montagem ou em caso de necessidade de troca do módulo, não será necessário refazer a solda na placa. Os componentes utilizados e suas funcionalidades estão detalhados nas subseções seguintes.

3.1.1 Especificação do NodeMCU32

A placa de desenvolvimento NodeMCU é baseada no módulo ESP32. Ela é destinada à prototipagem e ao desenvolvimento de baixo custo. O diagrama

funcional da placa NodeMCU32 é ilustrado na Figura 3.4. O NodeMCU32 é um módulo com o processador Xtensa 32-Bit LX6 Dual Core, de baixo consumo de energia, e com interface de rede *wireless* integrada no padrão 802.11 b/g/n: 2.4 à 2.5 GHz. Além disso, ele possui, integrada na placa, uma memória flash de 32bit com capacidade de 4MB, 3 interfaces UART para comunicação serial, 3 interfaces SPI e 2 interfaces I2C, para comunicação com dispositivos periféricos, e 36 interfaces I/O digital com tensão de saída de 3.3V e corrente máxima de 12mA (SYSTEMS, 2015).

Figura 3.4 – Diagrama funcional do NodeMCU com o chip ESP32.



Fonte:(THAKUR, 2018)

O uso da placa NodeMCU32 se justifica nas etapas de desenvolvimento porque, em uma única placa, estão disponíveis: uma interface serial-USB tipo B utilizada para programação, rede sem fio com antena integrada na placa de circuito impresso, interfaces I/O e módulo de memória flash. Além disso, a placa possui um tamanho reduzido quando comparada a outros módulos disponíveis no mercado.

3.1.2 Leitores RFID

O módulo RFID-RC522 foi escolhido para ler a Tag passiva do cartão RFID. Ele possui o chip MFRC522 da empresa NXP e implementa o protocolo ISO/IEC 14443 Type, compatível com cartões de 13,56MHz. Assim, é possível a leitura de cartões Mifare1 S50, S70, UltraLight, Pro, Desfire. Para comunicação do módulo com o sistema embarcado foi utilizado o protocolo de comunicação SPI.

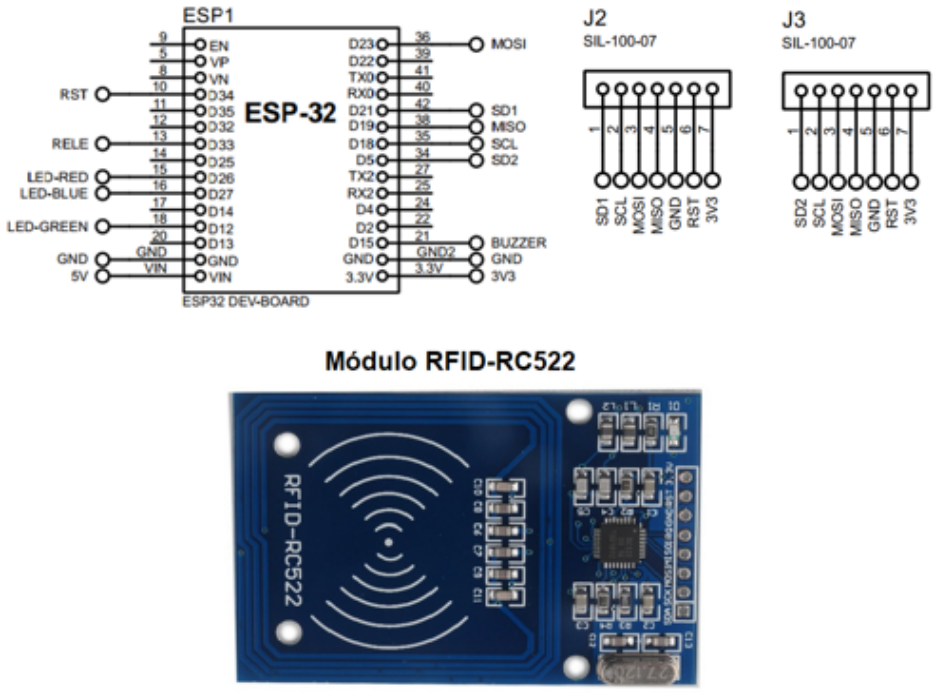
O protótipo possui dois leitores de cartão RFID. Sendo o primeiro posicionado junto a Central de Controle de Acesso e o segundo no lado externo do ambiente monitorado. Conforme pode ser observado na Figura 3.5 , o módulo de controle de acesso possui dois conectores J2 e J3 para conexão cabo de leitura dos módulos de leitura RFID. Também é possível observar que apenas o primeiro primeiro pino dos conectores J2 e J3 não é compartilhado, sendo esse utilizado para selecionar qual módulo pode trocar dados com o microcontrolador.

3.1.3 Acionamento do Eletroímã

Um dos desafios no desenvolvimento do módulo de controle de acesso foi a implementação de um circuito eletrônico de acionamento para o elemento mecânico de bloqueio da porta. Isso devido à disponibilidade, no mercado, de diversas fechaduras magnéticas com característica diferentes como força de tração, tensão de acionamento e consumo de corrente. Neste caso, o uso de relé se apresenta como uma boa opção pois é compatível com uma ampla faixa de dispositivos de bloqueio. O modelo de relé utilizado é acionado com 12V em corrente contínua e suporta 7A de corrente nominal para acionamento de cargas. Deve-se atentar que a corrente fornecida pela fonte de alimentação deve ser suficiente para energizar o eletroímã e os demais componentes.

O circuito apresentado na Figura 3.6 implementa a eletrônica necessária para que o microcontrolador consiga controlar cargas com valores de tensão e cor-

Figura 3.5 – Módulo de RFID e esquema de ligação com o módulo.

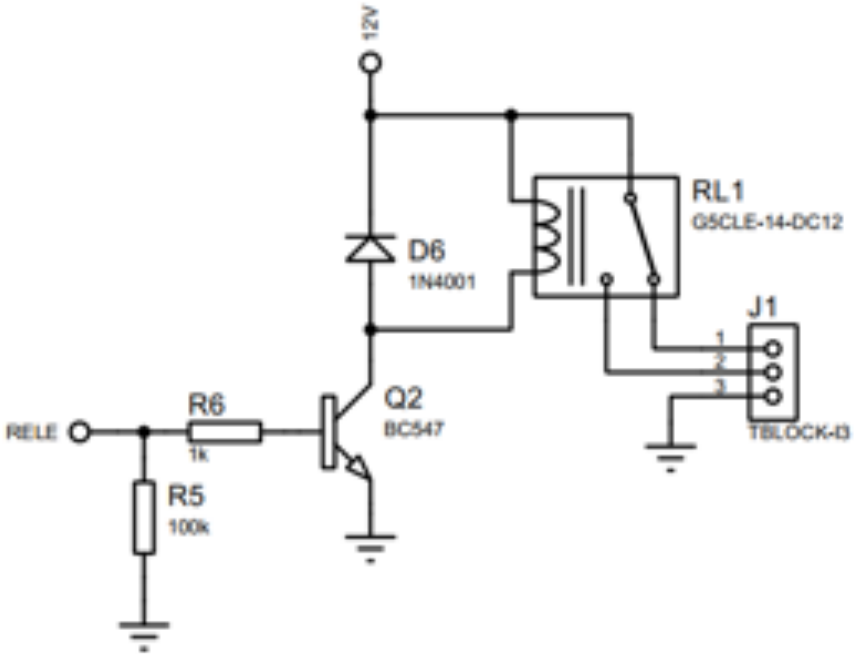


Fonte: Dos autores (2022).

rente maiores do que as que ele possui em sua saída. O transistor Q2 é responsável por amplificar a corrente fornecida e realizar o acionamento do relé, ou seja, por meio de uma corrente pequena aplicada na base do transistor pelo pino de saída do microcontrolador obtém-se uma corrente de cerca de 300mA necessária para acionar a bobina do relé.

Além disso, foi utilizado o diodo D6 com a função de proteção do transistor Q2. A justificativa para isso é que, quando o relé é desligado devido à energia magnética armazenada em sua bobina, é produzida uma corrente contra eletromotriz com valores de tensão elevados. Neste caso, o diodo de roda livre é utilizado como proteção, sendo responsável por permitir que a corrente circule na bobina até ser dissipada evitando a queima do transistor.

Figura 3.6 – Circuito de acionamento do eletroímã.



Fonte: Dos autores (2022).

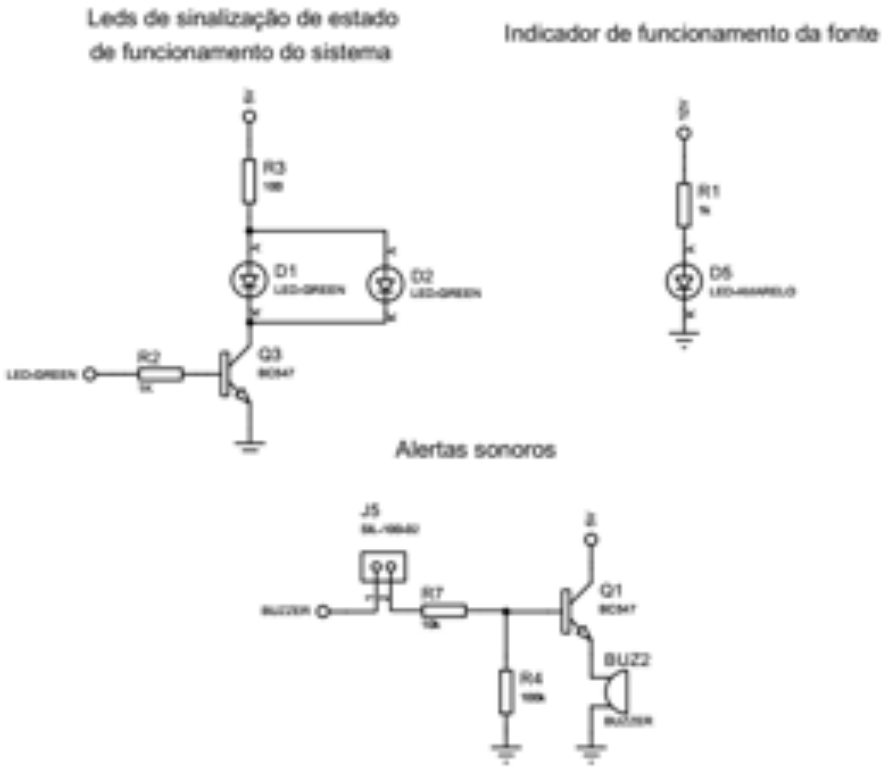
3.1.4 Interface com o Usuário

Qualquer sistema embarcado necessita de uma interface para interagir com o usuário e diversas tecnologias podem ser utilizadas para atingir esse objetivo. Dentre as opções disponíveis, pode-se citar *display LCD*, telas capacitivas sensíveis ao toque, *LED* e sistemas sonoros. Como um dos objetivos deste trabalho foi a redução de custo, foi utilizada uma interface mais simples, mas que não deixa de atender aos requisitos definidos no escopo do projeto. Portanto, foram utilizados *LEDs* de cores diferentes e um *buzzer* para gerar o sinal sonoro, conforme representado na Figura 3.2

Para o acionamento dos *LEDs* e do *buzzer* é necessário um drive de corrente, pois a corrente fornecida pelo microcontrolador não é suficiente para ligar os dispositivos. O drive implementado, conforme a Figura 3.7, é responsável por

fornecer a corrente e a tensão de acionamento adequadas para os dispositivos a partir do sinal de controle gerado pelo microcontrolador.

Figura 3.7 – Interface da central de alarme com o usuário.



Fonte: Dos autores (2022).

3.1.5 Projeto Estrutural

No desenvolvimento da estrutura do sistema embarcado, foi realizado um estudo para planejar o posicionamento e fixação dos componentes. Para isso, foi utilizando um software do tipo CAM *(Computer Aided Manufacturing)* no qual foram modeladas as caixas personalizadas para o sistema de controle de acesso. O modelo especificado contempla as estruturas de fixação do módulo RFID e a placa placa de circuito impresso.

A partir da desenvolvimento do modelo obtido foi possível gerar o arquivo utilizado pela impressora 3D e ajustar os parâmetros de impressão. O filamento utilizado para a impressão das caixas de montagem foi o poliácido láctico (PLA), que tem maior resistência mecânica quando comparado ao filamento de acrilonitrila butadieno estireno (ABS). Além disso, possui menor coeficiente de expansão térmica, reduzindo efeitos como o empenamento durante o processo de fabricação (SANTANA et al., 2018). Devido às dimensões da caixa, o processo de impressão foi demorado, levando cerca de 16 horas para a confecção da caixa de montagem interna e 3 horas para a caixa externa. O resultado obtido é apresentado na Figura 3.8.

3.2 Software Embarcado

O software embarcado no módulo ESP32 foi desenvolvido por meio da Arduíno IDE, uma vez que ela já possui uma grande quantidade de bibliotecas disponíveis, uma comunidade de desenvolvedores grande e ativa, o que possibilita uma constante evolução nas bibliotecas e mais facilidade na resolução de problemas. Além disso, a IDE possui ferramentas que auxiliam o desenvolvedor na configuração do chip, monitoramento de falhas e auxílio para a gravação do código na memória do microcontrolador.

No contexto do projeto de software, optou-se por utilizar ao máximo os recursos disponíveis no módulo ESP32, dentre eles, seu armazenamento interno e dois de seus núcleos de processamento independentes. Nesta seção, serão discutidos ambos os recursos e como eles foram aplicados ao projeto.

3.2.1 Armazenamento Interno

Na solução proposta neste trabalho, foi necessário armazenar algumas informações internamente no Sistema Embarcado para que ele não ficasse dependente da comunicação com o Servidor no processo de autorização e registro dos

Figura 3.8 – Caixa de montagem impressa para o módulo de controle de acesso.

Fonte: Dos autores (2022).

acessos. Uma alternativa seria a utilização de um cartão SD (Secure Digital) externo. No entanto, esse cartão ficaria subutilizado, uma vez que cartões SD possuem uma capacidade de armazenamento na escala de gigabytes, muito superior à necessidade do projeto. Essa capacidade de armazenamento subutilizada traria um custo desnecessário ao projeto. Além disso, outro problema é em relação à segurança dos dados. Como o cartão SD é removível e pode ser facilmente lido

por outros dispositivos, qualquer pessoa que tivesse acesso ao dispositivo poderia manipular os dados do cartão.

Diferentes estratégias poderiam ser adotadas para contornar o problema, inclusive o uso de criptografia dos dados e implementação de uma rotina de sincronização com o servidor. Porém, afim de reduzir o custo computacional e a complexidade do projeto, uma outra alternativa foi utilizada. O módulo ESP32 possui uma memória Flash de 4MB externa ao microcontrolador, que se comunica com ele por meio do protocolo SPI(*Serial Peripheral Interface*). O FreeRTOS, sistema operacional de tempo real, instalado no ESP32, permite configurar essa memória de diferentes formas, dentre elas, a mais interessante para este projeto, seria liberar 2 dos 4MB para armazenamento interno. Esta alternativa foi a escolhida para o projeto, uma vez que não apresenta os problemas do cartão SD. No entanto, devido à pouca quantidade de memória, foi necessário desenvolver algumas estratégias para otimizar seu uso, armazenando-se nela somente o necessário para garantir a independência em relação ao servidor.

Para gerenciar a memória flash, foi gravado no chip o sistema de arquivos SPIFFS (*SPI FLash File System*). Essa abordagem permite manipular dados na memória com um sistema de arquivos simples no qual todos os arquivos se encontram na raiz (sem uma estrutura em diretórios). Essa simplicidade permite um uso reduzido da memória para informações de cabeçalho e do próprio armazenamento do sistema de arquivos, o que deixa disponível um espaço maior para a gravação dos dados úteis. Devido aos poucos métodos disponibilizados na API (Application Programming Interface) do SPIFFS, foi necessário desenvolver uma classe específica para lidar com as operações envolvendo o uso da memória flash, incluindo métodos para manipular os dados, gerenciar o espaço, e tratar erros.

Em relação as informações armazenadas na memória interna, para identificar o usuário, foi necessário armazenar seu ID disponível no cartão. Para a função de registro de acesso, os dados armazenados são o ID do usuário e a informação de

qual sensor foi utilizado, o interno ou externo. Essa informação permite saber se o usuário entrou ou saiu do ambiente. Desse modo, foi proposta a seguinte configuração: um arquivo chamado `usuarios`, que contém uma lista com todos os ID's dos usuários cadastrados, e um arquivo chamado `acessos`, no qual são registrados o ID do usuário e o sensor correspondente (que realizou a leitura do cartão) para um dado acesso. Afim de simplificar a manipulação dos dados, escolheu-se trabalhar com arquivos de texto em vez de arquivos binários. Nesse formato, o ID do usuário, que é um número hexadecimal de onze dígitos único para cada usuário, foi armazenado como 11 caracteres. A informação de qual sensor realizou a leitura do cartão foi armazenada por um caractere na qual o valor 1 significa o sensor externo e 0 o sensor interno.

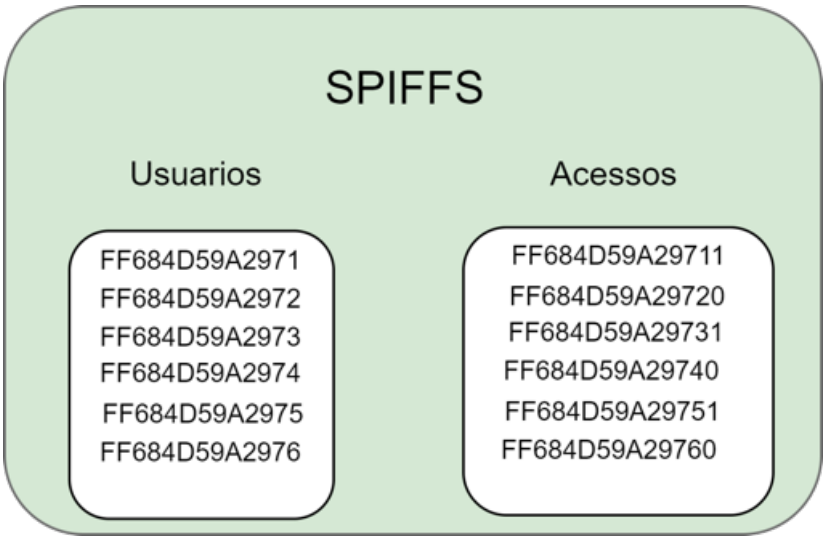
No arquivo `usuarios`, cada ID foi separado por um caractere de quebra de linha, já no arquivo `acessos`, o ID do usuário foi concatenado ao caractere do sensor, formando um único registro. Cada registro foi separado com um caractere de quebra de linha. O uso dessa estrutura foi pensado de modo que as funções desenvolvidas para manipulação dos dados fossem minimamente afetadas em aplicações futuras caso fossem armazenadas outras informações. Uma representação visual é apresentada na Figura 3.9 para ilustrar o formato final do sistema de arquivos.

3.2.2 Processamento Paralelo

Afim de reduzir o tempo de resposta do sistema e com isso melhor a experiência do usuário, foram utilizadas técnicas de programação paralela na implementação do software embarcado. O módulo ESP32 possui dois microprocessadores Xtensa 32-bit LX6, identificados como *core* 0 e *core* 1. Por meio do *FreeRTOS*, seu sistema operacional de tempo real, é possível criar tarefas [1], assim como escolher o núcleo do microprocessador que irá executa-la.

[1] O termo tarefas, *task* do inglês, refere-se a um fluxo sequencial de instruções construído para atender uma finalidade específica.

Figura 3.9 – Representação do sistema de arquivos.



Fonte: Dos Autores (2022)

Simplificadamente, quando se trabalha com processamento paralelo, procura-se dividir as tarefas de modo que cada núcleo fique a maior parte do tempo executando instruções, porém em duas principais situações o núcleo fica em estado de espera. A primeira é quando uma tarefa depende do resultado de outra para realizar alguma instrução. A segunda é quando ambas as tarefas compartilham um mesmo recurso de hardware, por exemplo, um barramento de comunicação.

Na prática, evitar estes cenários não é simples, visto que a demanda de cada núcleo é dinâmica e influenciada por condições externas ao sistema, no caso deste trabalho, o fluxo de pessoas e a velocidade da transmissão de dados pela rede. Desse modo, optou-se por utilizar uma divisão bastante comum em aplicações IoT. Nessa abordagem, um núcleo fica responsável por processar a tarefa com a atividade principal do dispositivo (neste caso, o controle de acesso) e o segundo núcleo executa a tarefa que realiza a comunicação com o servidor.

Por padrão, usando a Arduíno IDE, todo o código dentro das funções `void setup()` e `void loop()` é processado no núcleo 1. Assim, dentro dessas funções foi definida a tarefa associada ao controle de acesso. Foi criada outra para executar

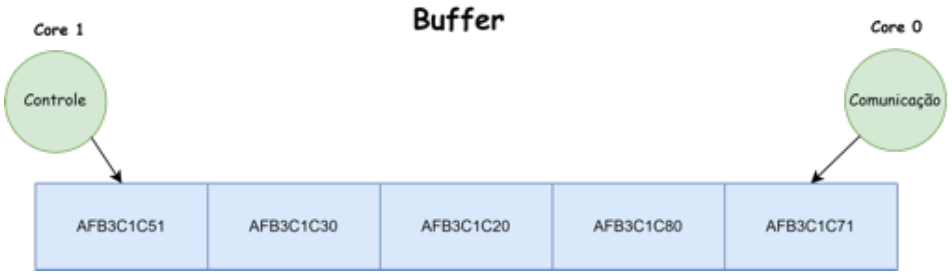
as instruções relacionadas à comunicação com o servidor e atribuída ao núcleo 0. A fim de facilitar o entendimento, neste trabalho, a tarefa executada pelo núcleo 0 foi nomeada como `controle` e a executada pelo núcleo 1, como `comunicação`.

Mesmo utilizando-se esse padrão para divisão de tarefas, ainda assim ambas compartilhariam recursos em comum, uma vez que precisam acessar os arquivos armazenados na memória flash. Nesse caso, tem-se dois cenários diferentes. O primeiro acontece quando a tarefa `comunicação` precisa excluir algum ID no arquivo `usuarios`, enquanto a `controle` lê os dados afim de verificar se o usuário está cadastrado. Nesse momento, vários erros poderiam ocorrer dependendo do exato momento no qual os dois eventos acontecerem. Para evitar essa situação, o sistema operacional *FreeRTOS* disponibiliza mutex, semáforos e filas. Como nesse caso existiam duas diferentes tarefas, optou-se por usar o semáforo binário. Assim, no momento que uma tarefa estiver utilizando o arquivo, ela bloqueia a outra de acessá-lo ao mesmo tempo.

O segundo cenário acontece quando a tarefa `controle` armazena dados no arquivo `acessos` enquanto a tarefa `comunicação` retira esses dados. Assim como no cenário anterior, há o problema de compartilhamento de recursos. Porém, diferentemente do primeiro cenário que raramente acontece, o segundo acontece sempre que há um novo acesso ao ambiente controlado. Portanto, usar somente a estratégia do semáforo não seria a melhor opção. O cenário 2 é um exemplo do tradicional problema do produtor e consumidor, ou também conhecido como *Bounded Buffer Problem* abordado em sistemas operacionais. Nele, uma entidade se comporta como o produtor que gera dados, no caso a tarefa `controle`, que gera os registros de acesso, e uma entidade que se comporta como consumidor, que consome os dados, no caso, a `comunicação`, que retira o registro do arquivo e o envia para o servidor. Para esse cenário, é indicado usar um *buffer*, que tem a função de armazenar os dados produzidos pela `controle` e que poderão ser consumidos pela `comunicação`. Desse modo, a tarefa `controle` não precisa esperar a tarefa

`comunicação` pegar o registro para que ela possa grava-lo e aguardar por uma nova leitura. Para implementar o *buffer*, foi utilizado a estrutura de fila disponibilizada pelo FreeRTOS. A Figura 3.10 mostra a estrutura do *buffer* e a interação com as tarefas. Seguindo o comportamento esperado de uma estrutura de dado do tipo fila FIFO, o primeiro elemento que entra, no caso inserido pela tarefa `controle`, é o primeiro que sai, no caso retirada pela tarefa `comunicação`.

Figura 3.10 – Representação do uso do *buffer*.

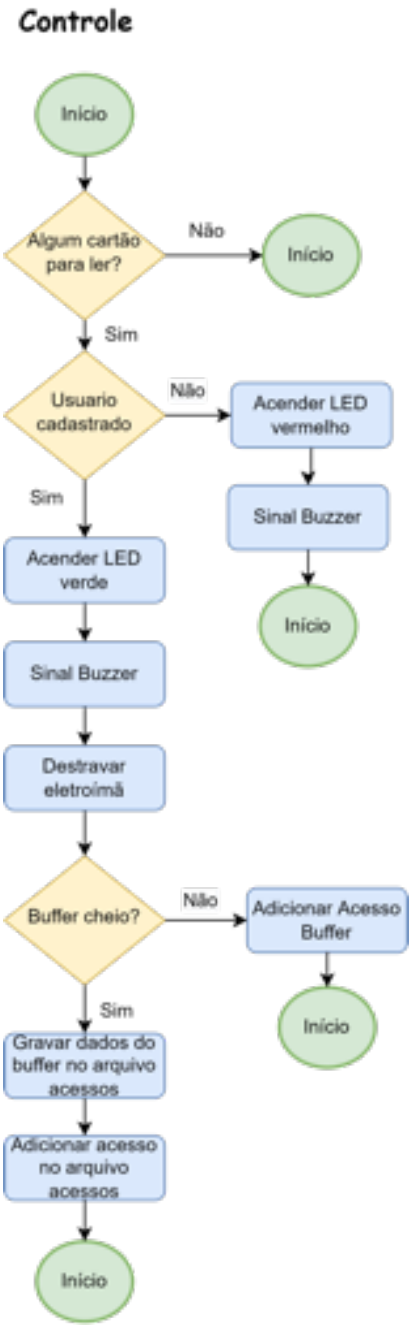


Fonte: Dos autores (2022).

A fila disponibilizada pelo FreeRTOS é do tipo circular, ou seja, tem um tamanho definido, e a sua posição de começo e fim variam à medida que os registros são adicionados e retirados dela. A partir de testes realizados em bancada, variando-se o fluxo da leitura e a estabilidade da conexão com a internet, constatou-se que o tamanho de 5 registros seria suficiente. Porém, em futuras aplicações nas quais o fluxo de pessoas seja muito grande, recomenda-se aumentar o tamanho do *buffer*.

A Figura 3.11 apresenta um fluxograma simplificado com as ações feitas pela tarefa `controle`. Como pode ser observado, a tarefa `controle` inicia sua execução esperando por um novo cartão para ser lido, ela permanece nessa posição até que o evento aconteça. Após isso, ela busca o ID lido do cartão no arquivo `usuários`. Caso o ID não seja encontrado, significa que o usuário não está cadastrado, portanto o *LED* vermelho é aceso e um sinal sonoro contínuo é emitido pelo*Buzzer*, indicando ao usuário que ele não está cadastrado. Por outro lado, caso

Figura 3.11 – Descrição da *tasks* controle.



Fonte: Dos autores (2022).

o ID seja encontrado no arquivo `usuários`, o *LED* verde é acionado, dois sinais sonoros são emitidos e o eletroímã é então destravado, para desbloquear a porta para o usuário.

Para registrar o acesso, primeiramente, a tarefa verifica se o *buffer* está cheio, situação que irá acontecer caso o sistema perca a comunicação com o servidor. Se estiver, ela primeiro esvazia o *buffer* gravando seus dados no arquivo `acessos` e, logo após, adiciona o registro também no arquivo. Caso o *buffer* não se encontre cheio, o registro é gravado diretamente nele.

A Figura 3.12 apresenta a sequência de ações realizadas pela tarefa `comunicação`. Como a função da `comunicação` é realizar a interface com o servidor e, para isso, ela precisa de estar conectada à rede, sua primeira ação é verificar se ela se encontra conectada. Caso não esteja, ela fica em um loop tentando se conectar e aumentando esse período entre novas tentativas, até que a conexão seja estabelecida. Caso já esteja conectada, o primeiro passo é verificar se existe algum dado no arquivo `acessos`. Ela prioriza a verificação do arquivo, uma vez que os registros são mais antigos, de modo a preservar a ordem dos acessos. Então, se o arquivo `acessos` tiver algum dado, ele será enviado para a aplicação Web na próxima instrução. Como segunda etapa, a tarefa verifica se existe algum registro no *buffer*. Caso tenha, ele também é enviado para a aplicação web.

Os próximos passos estão relacionados com as solicitações de cadastro ou exclusão de algum usuário vindas do servidor. A fim de verificar possíveis atualizações nos registros dos usuários, a cada tempo definido pelo gestor da aplicação, o sistema verifica com o servidor se existe alguma nova atualização para aquele ambiente. Caso não haja, ele retorna para o início das instruções, mas, se houver, a tarefa primeiro atualiza o arquivo `usuarios`, seja excluindo ou cadastrando um novo usuário, e após isso envia o status dessa atualização para o servidor, se foi bem sucedida ou se aconteceu algum erro que impediu a atualização.

Figura 3.12 – Descrição da *tasks*Comunicação.

Fonte: Dos autores (2022).

3.3 Aplicação Web

Como pode ser observado na Figura 3.1, além do sistema embarcado, que foi descrito nos tópicos anteriores, há ainda o servidor. Esse servidor hospeda a aplicação Web e o banco de dados no qual estão armazenados de forma permanente o cadastro de usuários e registros de acesso aos ambientes controlados. Para o ambiente de desenvolvimento foi configurado um servidor web Apache local, já para os testes em campo o servidor foi provisionado no próprio Data Center da Diretoria de Gestão de Tecnologia da Informação da Universidade.

É importante mencionar mais uma vez que a Universidade possui requisitos, padrões de projetos e tecnologias próprias para as aplicações Web internas. Portanto, todo esforço colocado nessa etapa não seria aproveitado. Desse modo, buscou-se construir uma interface que fosse suficiente para validar o funcionamento do sistema, de forma que não houve preocupação com o layout das páginas, padrões de projeto, segurança de dados, entre outros.

A aplicação web foi desenvolvida utilizando-se a linguagem PHP, com o desenho das telas foi definido com as linguagens HTML e CSS. A aplicação Web desempenha algumas funções específicas, listadas a seguir:

- Disponibiliza ao administrador do sistema uma interface na qual ele possa habilitar ou bloquear o acesso dos usuários aos ambientes controlados.

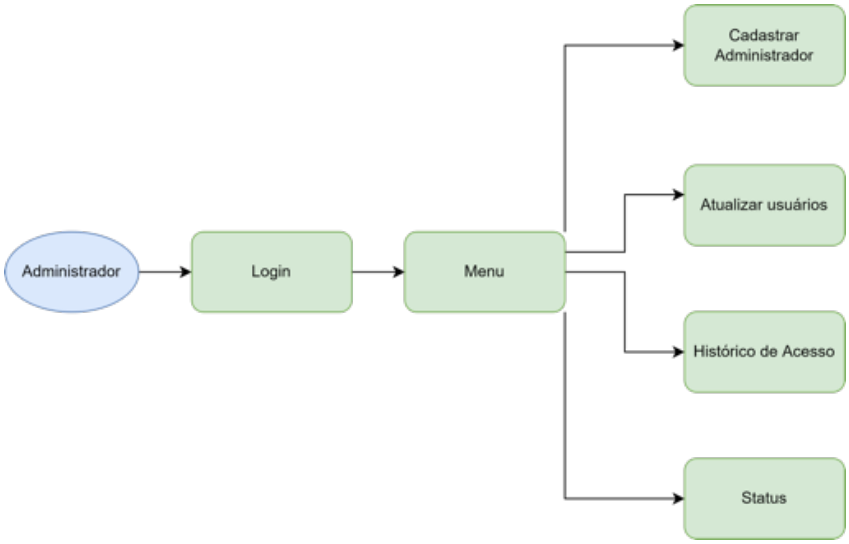
- Disponibiliza ao administrador do sistema o histórico de acessos aos ambientes cadastrados.

- Reporta ao administrador do sistema mensagens de erro, vindas do sistema embarcado.

- Entrega aos devidos sistemas embarcados, as solicitações feitas pelo administrador.

Para direcionar a explicação, foi criado um mapa de navegação, apresentado na Figura 3.13, com a estrutura das páginas disponíveis. Esse mapa está referenciado nos próximos subtópico, nos quais é apresentada a função de cada página , seu layout e os componentes presentes nela, como discutido em (MOURA; FERREIRA; PAINE, 1998).

Figura 3.13 – Mapa de navegação.



Fonte: Dos autores (2022).

3.3.1 Login

Assim como mostra a Figura 3.13, a primeira página disponível para o administrador é a página de login. Uma vez que a aplicação Web pode ser acessada de qualquer dispositivo com acesso à Internet dentro da rede da Universidade, foi necessário desenvolver uma página de login para autenticar o administrador, para que ele pudesse ter acesso as outras funcionalidades do sistema somente depois de autenticado.

Como pode ser observado na Figura 3.14, a página de login tem um formulário no qual o administrador insere seu email e senha cadastrados e aperta o

Figura 3.14 – Página de login.

Fonte: Dos autores (2022).

botão login para disparar o mecanismo de autenticação e ter acesso à página de menu.

3.3.2 Menu Principal

Após a autenticação, o usuário é direcionado para a página de menu. Esta página tem a função de exibir ao administrador os recursos disponíveis e direcioná-lo à página responsável pela funcionalidade escolhida. Assim como mostra a 3.15, os recursos são exibidos no texto que também são hiperlinks nos quais, ao clicar, o administrador é direcionado a página específica.

Figura 3.15 – Página de Menu.

Fonte: Dos autores (2022).

3.3.3 Cadastrar Administrador

Como é mostrado na Figura 3.15, o primeiro link da página Menu, direciona para a página Cadastrar Administrador. Assim como expresso pelo nome, essa página tem a função de cadastrar novas pessoas que terão acesso à aplicação Web.

Figura 3.16 – Página de Cadastro do Administrador.

Fonte: Dos autores (2022).

A Figura 3.16 exibe a página Cadastro do Administrador. Existem no total quatro informações necessárias para realizar o cadastro, sendo elas: o nome e email do administrador, o departamento, que representa o departamento onde está a sala que ele deseja administrar, e o campo sala, onde deve ser colocado o número de identificação da mesma. Após clicar no botão confirmar, o administrador já está apto a utilizar o sistema.

3.3.4 Atualizar Usuários

O segundo link da página de menu direciona para a página Atualizar Usuários. É por meio dessa página que o administrador irá manipular o arquivo `usuarios` que fica armazenado na memória interna do sistema embarcado. Caso o administrador cadastre um novo usuário, esse ID será adicionado no arquivo `usuarios`. De forma análoga, o usuário é excluído do arquivo se o Administrador assim o fizer.

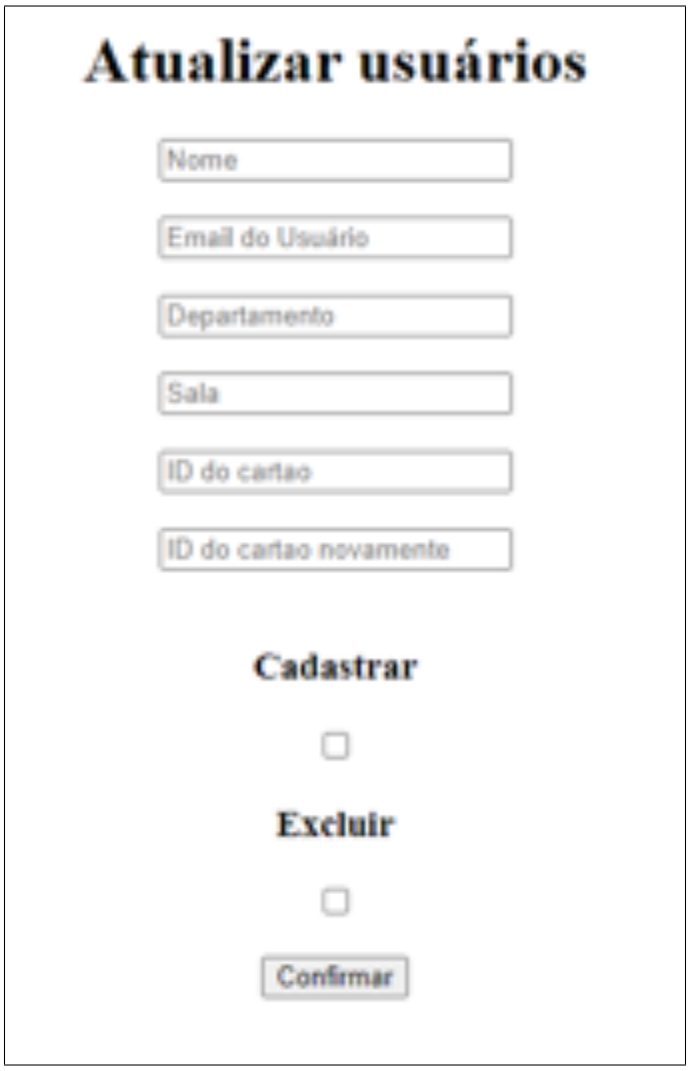
Como fica evidente na Figura 3.17, existem ao todo 6 campos, sendo que os 4 primeiros são exatamente iguais aos da página Cadastro Administrador, exceto que os campos Departamento e Sala especificam o local onde o usuário terá ou perderá o acesso. Os dois campos inferiores, contém o número de identificação do usuário (ID) armazenado no cartão funcional. Esse campo foi incluído para viabilizar a etapa de validação da solução, porém espera-se que o ID seja obtido diretamente do banco de dados da UFLA por meio do e-mail do usuário, uma vez que está informação já essa disponível lá.

Por fim, existem duas caixas de escolha que permitem ao administrador selecionar se ele quer cadastrar o usuário, ou seja, autorizá-lo a entrar no ambiente, ou excluí-lo, de modo que o usuário perca a permissão de acessar o ambiente controlado. É importante ressaltar que a atualização somente acontece após o recebimento de um e-mail de confirmação enviado pela aplicação Web, uma vez que a atualização precisa ser feita no armazenamento interno do sistema embarcado, podendo acontecer erros e atrasos nesse processo.

3.3.5 Histórico de Acesso

A próxima página disponível é a de histórico de acessos. Essa página lê os dados armazenados no banco de dados e exibe-os para o administrador. Os dados são apresentados em formato de tabela contendo as informações do nome da pessoa que acessou o ambiente, a localização do ambiente (departamento e sala),

Figura 3.17 – Página para Atualização de usuários.



Fonte: Dos autores (2022).

a hora que o cartão foi detectado pelo leitor e por último se a pessoa entrou no ambiente ou saiu. A Figura 3.18 apresenta o formato da tabela com o uso de dados fictícios.

Figura 3.18 – Página de histórico de acesso.

Registro de Acesso

Nome	Departamento	Sala	Data/Hora	Saiu/Entrou
Marcos	DCC	03	2020-06-08 08:47:10	entrou
Jairo	DEG	03	2020-06-08 08:56:53	entrou
Marcos	DEG	05	2020-06-08 10:09:59	saiu
Weslley	DCC	01	2020-06-08 10:31:00	entrou
Victor	DEG	05	2020-06-08 10:36:55	entrou
Victor	DFI	03	2020-06-08 10:40:60	saiu
Pedro	DFI	04	2020-06-08 10:50:07	entrou
Marcos	DEG	04	2020-06-08 10:50:21	entrou
Marcos	DEG	05	2020-06-08 11:24:45	saiu
Jairo	DFI	01	2020-06-08 11:36:22	saiu
Victor	DFI	01	2020-06-08 12:06:14	entrou
Jairo	DFI	03	2020-06-08 12:46:47	entrou
Jairo	DEG	05	2020-06-08 13:28:29	saiu
Marcos	DEG	03	2020-06-08 14:25:32	entrou
Marcos	DCC	01	2020-06-08 14:28:00	saiu
Weslley	DCC	04	2020-06-08 14:32:40	saiu
Weslley	DCC	05	2020-06-08 14:34:38	entrou
Victor	DFI	01	2020-06-08 15:39:19	saiu
Pedro	DFI	05	2020-06-08 16:03:36	saiu
Pedro	DFI	05	2020-06-08 17:27:42	entrou
Marcos	DCC	05	2020-06-08 17:38:27	entrou
Weslley	DCC	01	2020-06-08 17:40:47	saiu
Marcos	DEG	05	2020-06-08 17:42:42	saiu

Fonte: Dos autores (2022).

3.3.6 Status

A última página da aplicação web é a de Status. Ela lê as mensagens de erro enviadas por cada sistema embarcado e exibe-as ao administrador. A partir

dessa página, o administrador consegue monitorar se os dispositivos estão funcionando de forma adequada e, se necessário, realizar uma ação corretiva.

Sua estrutura é semelhante à de Registro, porém sem as colunas “nomes” e “saiu/entrou” e com a coluna “Mensagem”. Os dois primeiros campos indicam a localização do dispositivo que enviou a mensagem, o campo Data/Hora indica o momento em que o erro foi recebido e a mensagem indica qual o erro.

Figura 3.19 – Página Status dos Dispositivos.

Fonte: Dos autores (2022).

3.4 Análise Econômica

Para a análise de viabilidade econômica, foi realizada uma pesquisa dos equipamentos comerciais que atendem aos mesmos requisitos da solução proposta. Em particular, considerou-se principalmente os seguintes itens: central de controle de acesso compatível com cartão RFID 13,56 MHz ISO 14443A, saída para acionamento de fechadura eletromagnética, registro de histórico de acesso em banco de dados e conexão sem fio compatível com o protocolo IEEE 802.11 b/g/n.

Foram avaliados os custos de duas soluções comerciais. Os custos[2] dos sistemas para controle de acesso fornecidos pela Intelbras e Hikvision estão descritos na Tabela 3.1 e na Tabela 3.2, respectivamente. Considerando o sistema proposto neste trabalho, a lista de componentes para o desenvolvimento do protótipo e da solução para o controle de acesso físico monitorável encontra-se na Tabela 3.3.

Tabela 3.1 – Solução para controle de acesso físico e monitorável da Intelbras.

Componente	Descrição	Preço
Controlador de acesso SS 3430 MF BIO	Métodos de autenticação:leitura de cartão de proximidade RFID 13,56MHz, biometria digital e senha. Interface de comunicação TCP/IP e WiFi IEEE 802.11 b/g/n Software de gerenciamento de controle de acesso. Armazenamento de 30.000 usuários, 3.000 biometrias e 150.000 eventos. 1x Saída para acionamento de fechadura 1x Entrada para botão de saída	R$ 1.254,75
Fonte de alimentação	Fonte de alimentação 12V 2A	R$17,14
Fechadura Eletromagnética	Intelbras FE 20150 150 Kgf	R$327,60
Botoeira	Acionador de Fechadura	R$59,85
	Total	R$1.659,34

Fonte: Dos autores (2022).

Entre os equipamentos comercias encontrados, as centrais de controle de acesso apresentadas da Intelbras e Hikvision (Tabelas 3.1 e 3.2) foram as que atendem aos requisitos deste trabalho e com características semelhantes às do protótipo desenvolvido. Por outro lado, possuem algumas funcionalidades adicionais, como

[2] Os custos foram obtidos em <https://www.netalarmes.com.br/> e <https://www.inpower.com.br/>.

Tabela 3.2 – Solução para controle de acesso físico e monitorável da Hikvision.

Componente	Descrição	Preço
Controle de Acesso Hikvision DS-K1T804BMF	Métodos de autenticação:leitura de cartão de proximidade RFID 13,56MHz, biometria digital e senha. Interface de comunicação TCP/IP e WiFi IEEE 802.11 b/g/n 3.000 impressões digitais, 3.000 cartões e armazenamento de 100.000 eventos Interface De Entrada: Botão Sair, Sensor de Porta e Entrada de Alarme Interface De Saída: Relé (saída de bloqueio) e saída de alarme Gerenciamento via *software* IVMS 4200	R$ 944,00
Fonte de alimentação	Fonte de alimentação 12V 2A	R$ 21,75
Fechadura Eletromagnética	Fechadura Hikvision Ds-k4h258s	R$ 326,63
Botoeira	Botão De Acesso de Aluminio Hikvision Ds-K7P02	R$ 91,73
	Total	R$ 1.384,11

Fonte: Dos autores (2022).

Tabela 3.3 – Solução para controle de acesso proposta.

Componente	**Unidade**	**Quantidade**	**Total Parcial**
Fechadura Eletromagnética Eletroímã - 150 kgf	UND	1	R$311,22
Fonte de alimentação 12V 2A	UND	1	R$40,00
Kit Leitor RFID 13,56Mhz Cartao E Chaveiro	UND	2	R$43,98
Módulo NodeMCU ESP32 - D0WDQ6	UND	1	R$72,90
Filamento PLA Cinza	Kg	0,25	R$24,50
Cabo Manga Sem Blindagem	METRO	2,5	R$18,77
Conector prensa cabo pvc	UND	1	R$4,14
Transistor 2n2222A	UND	5	R$1,80
Terminal Modu	UND	40	R$6,00
Conector Alojamento passo 2.54mm	UND	40	R$10,40
Borne	UND	2	R$1,78
Relé 12V 1 Polo 2 Posicoes 5 Terminais	UND	1	R$3,70
Regulador de Tensão	UND	1	R$1,70
Capacitores	UND	5	R$1,00
Buzzer 5V com oscilador interno	UND	1	R$1,42
Led 3mm	UND	7	R$1,54
Resistor 1k 1/4W	UND	11	R$0,66
Diodo 1N4007	UND	2	R$0,44
		Total	R$R545,95

Fonte: Dos autores (2022).

opções de acesso com senha e biometria. Outras soluções também foram analisadas e atendiam ao requisitos levantados. Porém, tais soluções possuem tela *touch screen* e reconhecimento facial, o que implica em um preço cerca de cinco vezes maior que as demais soluções.

Fazendo um comparativo entre os custos de implementação envolvendo as 3 soluções apresentadas, observa-se que o protótipo desenvolvido possui um custo, aproximadamente, 2,5 vezes menor que a solução comercial de menor custo. Além disso, dado que todo o sistema foi desenvolvido utilizando tecnologias *open-source*, é possível um total acesso ao *firmware* do sistema embarcado, permitindo a implementação de novas funcionalidades no futuro.

4 DISCUSSÃO DOS RESULTADOS

Neste capítulo, são abordadas as etapas de validação do Sistema de Controle de Acesso, incluindo os testes de bancada, testes em ambientes controlados e, por fim, o teste em ambiente relevante. Também será apresentada uma avaliação de confiabilidade do sistema.

4.1 Testes em Bancada

O processo de validação e teste do sistema foi realizado em várias etapas. Primeiramente, foram realizados os testes de cada nova funcionalidade de forma isolada. Aprovada nos testes, a nova funcionalidade era incorporada com o restante do sistema e novos testes eram aplicados para validação da integração da nova funcionalidade. Ambos os testes foram realizados em bancada.

Essa segunda fase (de testes das funcionalidades integradas) demandou mais tempo, uma vez que a maior parte dos erros aconteceu durante esta fase. Dentre as maiores dificuldades encontradas nesta etapa destacam-se:

- Estabilidade na conexão com o servidor. Foram necessários diversos testes e ajustes, tanto do módulo NodeMCU, quanto do servidor Apache, para que a conexão entre eles se mantivesse estável.

- Problemas na integração entre os módulos. Os módulos foram testados individualmente e, após validados, integrados a uma placa de prototipagem para formar o sistema embarcado. Nessa fase, diferentes erros ocorreram. Após diversos testes, descobriu-se que os erros eram decorrentes das conexões com a placa de desenvolvimento. Assim, após a alteração dos testes da placa de prototipagem para a placa de circuito impresso, os erros foram solucionados.

4.2 Testes em Ambiente Controlado

Após finalizar o desenvolvimento e a integração de todas as funcionalidades, o dispositivo foi testado em um ambiente controlado. Para esse teste, o Sistema de Controle de Acesso foi instalado em uma sala na Coordenadoria de Campus Inteligente da Pró-Reitoria de Infraestrutura.

Nesta etapa, o sistema permaneceu em fase de teste por um período de seis meses no qual três pessoas faziam o uso diário da sala. Nesse período, foi possível avaliar o comportamento do sistema quando submetido à variação de temperatura, quedas de energia elétrica e quedas de conexão com a Internet. Em todas essas condições, o sistema permaneceu estável com o comportamento padrão.

4.3 Teste em Ambiente Relevante

Conforme o sucesso dos testes com o sistema em ambiente controlado, submetido a condições próximas das reais, foi elaborada uma nova etapa de testes, na qual o Sistema de Controle de Acesso foi submetido a um ambiente relevante. Nesta etapa, foi escolhido um laboratório de informática localizado no Pavilhão 6 da Universidade Federal de Lavras (UFLA) - Campus Sede. A escolha deste laboratório se deu por este possuir uma câmera, a qual poderia ser utilizada como forma de monitoramento da interação das pessoas com o Sistema de Controle de Acesso, além de auxiliar na identificação de possíveis falhas.

A Figura 4.1 apresenta o posicionamento dos elementos no laboratório. Dentro da sala, foi instalada a central de controle de acesso com um dos leitores de cartão de RFID, Figura 4.1(d) e também foi fixado o eletroimã na parte superior da porta. Do lado externo, Figura4.1(b), o segundo leitor de cartão RFID foi instalado próximo à fechadura.

Como parte do teste, todos os usuários do laboratório tiveram que ser cadastrados pela interface Web, incluindo professores, equipe de limpeza, equipe de

Figura 4.1 – Laboratório de informática utilizado durante o período de teste.

Fonte: Dos autores (2022).

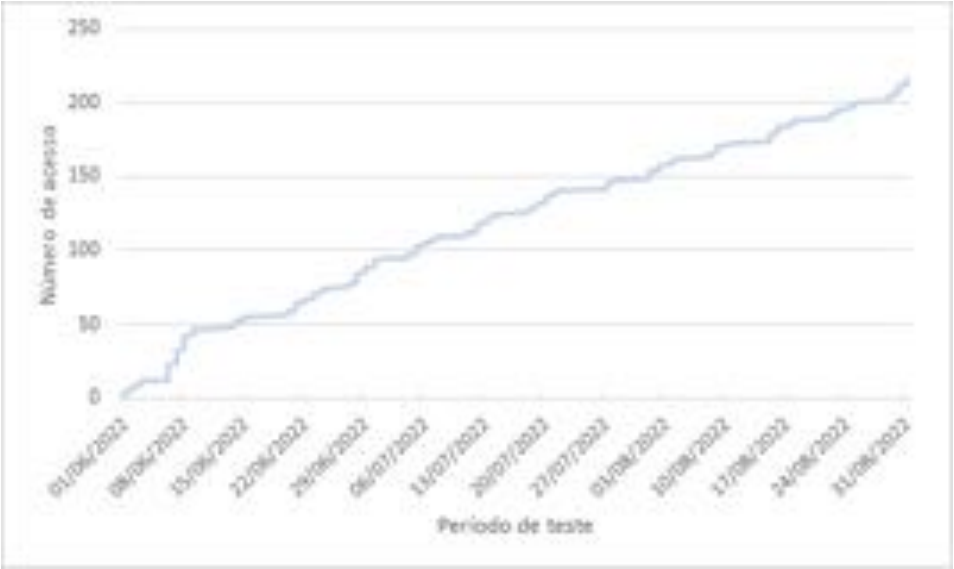
manutenção de computadores, equipe de vigilância e responsável pela manutenção do controle de acesso. Para validação e teste do sistema, foram analisadas as ocorrências e registros de acesso durante os meses de junho, julho e agosto de 2022.

4.3.1 Avaliação de Confiabilidade

Durante 3 meses, foram monitorados os acessos no laboratório. Na Figura 4.2, pode-se observar a evolução no número total acumulado de acessos durante o período de testes. Ao todo, foram registrados 216 acessos. Também foram identificados os perfis dos usuários que acessaram o laboratório. A Figura 4.3 mostra o total de acessos por perfil. Esses dados foram determinados a partir da

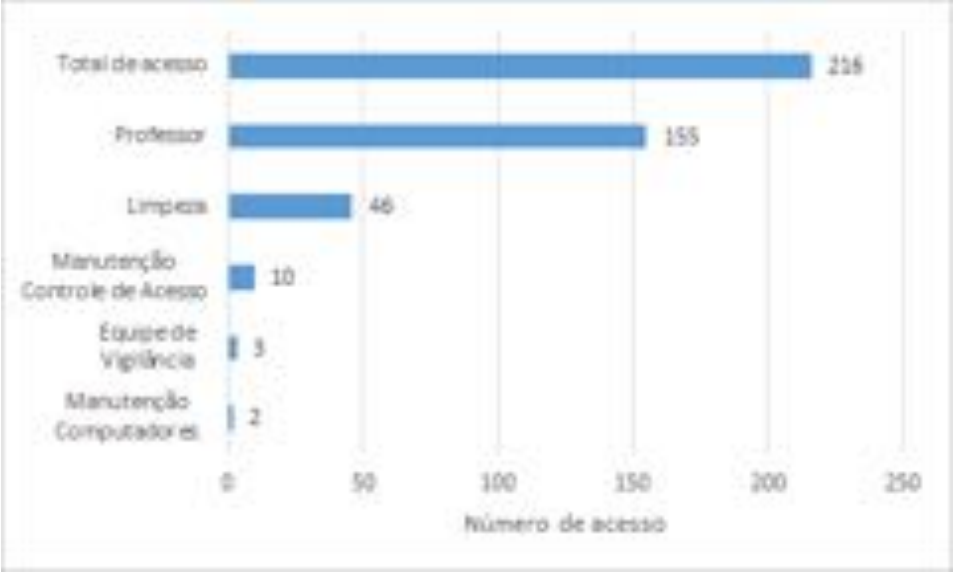
combinação dos registros de acesso com as informações de identificação dos cartões RFID armazenadas no banco de dados do sistema.

Figura 4.2 – Contagem de acessos ao laboratório de informática.



Fonte: Dos autores (2022).

Figura 4.3 – Perfil de usuário do laboratório de informática.



Fonte: Dos autores (2022).

Na Figura 4.4, é possível analisar a frequência diária de acessos ao laboratório durante a fase de testes. Percebe-se que não foi registrado qualquer acesso nos finais de semana. Este resultado é coerente com os horários de reservas efetuadas para realização de atividades no laboratório, conforme é apresentado n Figura 4.5. Além disso, a realização de atividades de limpeza e manutenção do laboratório aos fins de semana ocorre somente para os casos de atividades agendadas neste período.

Pela análise dos dados na Figura 4.4(a), não houve registro de acesso nos dias 16 e 17 de junho. Isso é devido ao feriado de Corpus Christi (16), seguindo de ponto facultativo (17). De forma análoga, os dados na Figura 4.4(b) mostram que no dia 26 de junho também não houve registro de acessos, em razão do feriado municipal.

Para identificar os horários em que o Sistema de Controle de Acesso foi utilizado com maior frequência, considerou-se os dois grupos mais representativos conforme número de acessos por perfil (na Figura 4.3). Também foram considerados os horários reservados desde o início do semestre letivo 2022/2 para realização de aula práticas pela Pró-Reitoria de Graduação (PROGRAD).

A partir dos dados apresentados na Figura 4.5, pode-se observar que o Sistema de Controle de Acesso foi utilizado com maior frequência nos primeiros dias da semana e entre as 6:30 e 22:30. Em relação ao acesso pela equipe de limpeza, identificou-se que a limpeza do laboratório ocorre com maior frequência no começo do dia. Em relação ao acesso pelos professores, observou-se alguns acessos fora dos horários reservados inicialmente pela Pró-reitoria de graduação. O acesso ao laboratório para atividades extras é permitido desde que reservado previamente, respeitando-se as prioridades de realização das atividades letivas obrigatórias.

Durante as primeiras semanas de teste, foi relatado que a equipe de limpeza não estava conseguindo acessar o laboratório. Após análise no local, verificou-se que o Sistema de Controle de Acesso estava funcionando normalmente, mas a

Figura 4.4 – Total de acessos por dia durante os meses de teste.

(a) Acesso por dia registrado em junho.

(b) Acesso por dia registrado em julho

(c) Acesso por dia registrado em agosto

Figura 4.5 – Acessos para uso do laboratório de informática.

Fonte: Dos autores (2022).

sala havia sido trancada com a chave. Como medida corretiva as cópias de chave do laboratório foram recolhidas e entregues para o setor de segurança.

No dia três de agosto, foi reportado pela equipe de vigilância que a porta do laboratório estava destravada. Após análise no local, verificou-se que o Sistema de Controle de Acesso encontrava-se desligado. A partir dos vídeos da câmera de monitoramento, observou-se que a fonte de alimentação havia sido retirada da tomada por um aluno para uso de outro dispositivo. Como ação corretiva foi realizado a alteração do local de instalação da fonte de alimentação do Sistema de Controle de Acesso, afim de evitar um desligamento acidental.

A partir da análise do histórico de acessos, percebeu-se que haviam alguns registros repetidos lidos pelo mesmo sensor. No primeiro momento, o evento foi

associado a uma mesma leitura para quando o usuário demorasse a retirar o cartão de perto do leitor. Após alguns testes e uma análise mais detalhada, percebeu-se que, como a porta do laboratório tinha a maçaneta do tipo bola, era comum o usuário gastar mais tempo para abri-la. Dessa forma, o eletroímã a bloqueava antes que o usuário abrisse porta. Com o problema identificado, o tempo que o usuário tem para abrir a porta foi aumentado para dez segundos e esta ocorrência não foi mais registrada, sendo esta uma solução válida para o cenário atual de teste, em que é necessário identificar apenas a pessoa responsável pelo uso do laboratório e não todos os alunos.

5 CONSIDERAÇÕES FINAIS

O uso da tecnologia RFID se mostrou uma boa opção no controle de acesso a ambientes físicos, isso porque possui um bom custo-benefício, segurança e também a capacidade de identificar o usuário. Quando conectado à Internet, o sistema de controle de acesso é capaz de se adequar aos mais complexos cenários nos quais seria necessária a interferência humana.

O desenvolvimento do sistema proposto neste trabalho gerou um melhor entendimento sobre o potencial do uso da tecnologia no controle de acesso a ambientes físicos. Também foi possível entender melhor os desafios e melhorias necessárias no sistema para aplicação em larga escala.

Os testes realizados mostraram que o sistema atingiu os objetivos do trabalho, uma vez que foi capaz de identificar o usuário por meio do cartão de membro da Universidade e liberar ou bloquear a porta de acordo com a permissão do usuário. Além disso, o sistema foi capaz de atualizar essa lista de usuários de maneira remota sempre que houver uma solicitações do gestor da aplicação. O protótipo desenvolvido também foi capaz de enviar ao gestor os registros de acesso a medida que eram detectados. Também foi desenvolvida uma aplicação Web que recebeu e armazenou os dados enviados pelo protótipo e também pelo gestor. Além de atingirem aos objetivos estabelecido o sistema desenvolvido, se aplicado às salas e laboratórios da Universidade, é capaz de melhorar o processo atual, uma vez que:

- Reduzirá o número de funcionários dedicados ao controle de acesso.
- Permitirá que as salas de aula permaneçam trancadas.
- Não será necessário o deslocamento dos professores até os locais de empréstimo de chaves.
- O controle de pessoas autorizadas aos laboratórios poderá ser realizado de maneira automatizada.

- O acesso aos ambientes poderá acontecer à qualquer dia e hora.

Além de conseguir trazer as melhorias citadas acima, o sistema ainda gera uma quantidades de dados relevantes para a Universidade. Desse modo, viabiliza a implantação futura de um sistema de análise de dados que permita à Universidade identificar espaços ociosos, caracterizar o fluxo de pessoas, gerar indicadores sobre uso dos espaços, entre outros.

Apesar do sistema ter sido testado em condições reais por um período considerável e nenhuma falha grave ter sido detectada, algumas melhorias e modificações podem ser implementadas no sistema nas próximas versões. Em relação aos componentes utilizados, o módulo de desenvolvimento NodeMCU poderia ser substituído por sua versão contendo apenas o módulo ESP32. Dessa forma, poderia-se reduzir o tamanho e o custo da placa, o que evitaria componentes que, apesar de serem importantes para a fase de testes, são desnecessários em um produto final.

Também em relação à redução do tamanho, pode-se usar componentes SMD (Surface Mounted Device), a fim de se aproveitar os dois lados da placa. Esta modificação poderia também reduzir o consumo de material para a produção da caixa interna do sistema embarcado e tornar a solução mais compacta e atrativa visualmente. Ainda em relação a placa de circuito, poderia-se aprimorar a eletrônica do regulador de tensão para suportar tensões compatíveis com carregadores de baterias de *nobreak*. Essa atualização traria uma maior robustez e controle das oscilação na rede elétrica.

As possibilidades de melhoria na Interface Web são muitas, entre as quais pode-se destacar: melhoria no *layout* das páginas, adicionando-se cores e mais elementos nas páginas para melhoras o aspecto visual e a interação com o usuário. Também é interessante o desenvolvimento de alarmes para alertar ao gestor da aplicação sobre falhas nos ambientes. Essa funcionalidade iria agilizar o processo de identificação de falhas. Por fim, outra possível melhoria seria a integração do

sistema com alguma ferramenta de análise de dados. Dessa forma, seria possível aproveitar de maneira mais profunda os dados produzidos pelo sistema, gerando relatórios e auxiliando a Universidade na tomada de decisão em relação ao uso dos espaços.

É também interessante que, em trabalhos futuros, sejam abordadas a segurança e a privacidade dos dados utilizados na aplicação, avaliando-se possíveis vulnerabilidades do sistema, tanto no que diz respeito ao sistema embarcado quanto à aplicação Web.

REFERÊNCIAS

ALMEIDA, R. M. A. de; MORAES, C. H. V. de; SERAPHIM, T. d. F. P. **Programação de Sistemas Embarcados: Desenvolvendo Software para Microcontroladores em Linguagem C**. [S.l.]: Elsevier Brasil, 2017.

BRAGA, N. C. **Tudo Sobre Relés (livro completo)**. 2009. Https://www.newtoncbraga.com.br/index.php/como-funciona/597-como-funcionam-os-reles. Acessado em: 17 ago. 2022.

CURVELLO, A. et al. **Linguagens de Programação para Sistemas Embarcados**. 2015. Https://embarcados.com.br/editorial-linguagens-para-sistemas-embarcados/. Acessado em: 16 ago. 2022.

FENNANI, B.; HAMAM, H.; DAHMANE, A. O. Rfid overview. In: **ICM 2011 Proceeding**. [S.l.: s.n.], 2011. p. 1–5.

FERREIRA, N. A. **Eletroímã**. 2021. Https://mundoeducacao.uol.com.br/fisica/eletroima.htm/. Acessado em: 20 set. 2022.

JIA, X. et al. Rfid technology and its applications in internet of things (iot). In: IEEE. **2012 2nd international conference on consumer electronics, communications and networks (CECNet)**. [S.l.], 2012. p. 1282–1285.

Khan Academy. **Equação i-v do indutor em ação**. 2016. All Khan Academy content is available for free at, www.khanacademy.org Acessado em Agosto de 2022.

MARCONDES, J. S. **Controle de Acesso Físico: O que é? Definição, Objetivos, Características**. 2021. Https://gestaodesegurancaprivada.com.br/controle-de-acesso-fisico/#Dados-citação-trabalhos. Acessado em: 17 ago. 2022.

MOURA, M. L. S. de; FERREIRA, M. C.; PAINE, P. A. **Manual de elaboração de projetos de pesquisa**. [S.l.]: EdUERJ, 1998.

SACCO, F. **Comunicação SPI – Parte 1**. 2014. Https://embarcados.com.br/spi-parte-1/. Acessado em: 31 ago. 2022.

SANTANA, L. et al. Estudo comparativo entre petg e pla para impressão 3d através de caracterização térmica, química e mecânica. **Matéria (Rio de Janeiro)**, SciELO Brasil, v. 23, 2018.

SYSTEMS, E. **ESPRESSIF SYSTEMS. ESP32 Datasheet,**. 2015. Https://html.alldatasheet.com/html-pdf/1148023/ESPRESSIF/ESP32/6845/12/ESP32.html. Acessado em: 30 jul. 2022.

TEIXEIRA, G.; CAMPOS, G. Sistema automatizado para redução de perdas associadas ao processo de refrigeração do leite em pequenas propriedades. **ForScience**, v. 7, 04 2019.

THAKUR, M. R. **ESP32 DevKit ESP32-WROOM GPIO Pinout**. 2018. Https://circuits4you.com/2018/12/31/esp32-devkit-esp32-wroom-gpio-pinout/. Acessado em: 31 ago. 2022.