UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

ENGENHARIA DE CONTROLE E AUTOMAÇÃO

BEATRIZ ALMEIDA LINS LOPES

# PLATAFORMA LOCAL DE CONTROLE DE ACESSO PARA AMBIENTES ACADÊMICOS

RECIFE

2020

UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

ENGENHARIA DE CONTROLE E AUTOMAÇÃO

BEATRIZ ALMEIDA LINS LOPES

# PLATAFORMA LOCAL DE CONTROLE DE ACESSO PARA AMBIENTES ACADÊMICOS

Trabalho de Conclusão de Curso submetido à Universidade Federal de Pernambuco como parte dos requisitos necessários para a obtenção do título de Bacharel em Engenharia de Controle e Automação.

Orientador: Prof. Dr. Marcio Evaristo da Cruz Brito

RECIFE

2020

UNIVERSIDADE FEDERAL DE PERNAMBUCO

FOLHA DE APROVAÇÃO

# PLATAFORMA LOCAL DE CONTROLE DE ACESSO PARA O DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA UNIVERSIDADE FEDERAL DE PERNAMBUCO

BEATRIZ ALMEIDA LINS LOPES

Trabalho apresentado à Universidade Federal de Pernambuco (UFPE), como requisito parcial para obtenção do título de Bacharel em Engenharia de Controle e Automação.

Data da aprovação: Recife/ PE ___ / ___ / _____

**BANCA EXAMINADORA:**

Prof. Dr. Marcio Evaristo da Cruz Brito
Orientador/ UFPE

Prof. Dr.

Prof. Dr.

RECIFE

2020

*Dedico este trabalho à toda minha família, amigos e professores, que foram fundamentais na minha jornada.*

# AGRADECIMENTOS

*Gostaria de agradecer a todos que fizeram parte de forma positiva dessa jornada:*

*Aos meus pais, por sempre estarem presente em todos os momentos e sempre proverem todas as ferramentas, conforto e incentivo necessários para eu seguir em frente,*

*A minha irmã, por ser uma companhia tão boa e deixar meus dias mais leves,*

*A minha avó, por sempre ter incentivado o hábito da leitura e me ensinado o poder de transformação da educação na vida das pessoas,*

*Aos meus familiares: avós, tias e primos, por serem minha rocha,*

*Aos meus sócios e ex-sócios da ConnectON, por confiarem em mim e embarcarem nesta jornada tão desafiadora que é empreender e desenvolver tecnologia,*

*Aos meus amigos e colegas da escola, faculdade e da vida, por sempre me acolherem tão bem,*

*Ao meu orientador Prof. Dr. Marcio Evaristo da Cruz Brito, por todo o apoio e confiança no desenvolvimento deste trabalho e por todo conhecimento transmitido em diversas cadeiras na faculdade,*

*A todos os professores que me ensinaram a importância de compartilhar conhecimento e do incentivo à ciência, cultura e tecnologia.*

*"Se sentir que chegou ao seu limite, lembre-se do motivo pelo qual você cerra os punhos, lembre-se porque resolveu trilhar este caminho e permita que essa memória o carregue além de seus limites."*

*Nana Shimura*

# RESUMO

Este trabalho consiste no desenvolvimento e implementação de uma plataforma que permita o controle e gerenciamento do acesso aos principais ambientes do Departamento de Engenharia Elétrica da Universidade Federal de Pernambuco. O seu principal objetivo é garantir a segurança e integridade dos equipamentos de alto valor monetário e acadêmico dentro das salas de aula e laboratórios, impedindo a entrada de pessoas não autorizadas e registrando os horários de entrada e saída de todos os usuários permitidos no ambiente.

A plataforma permitirá a criação de três tipos de usuário: Aluno (que poderá acessar os ambientes nos dias e horários permitidos), Professor (além do acesso às salas, poderá ser responsável por disciplinas e ambientes, onde pode gerenciar o acesso e acessar o histórico) e Administrador (capaz de criar e editar ambientes, disciplinas e usuários e gerenciar todas salas).

O software desenvolvido estará hospedado em um servidor local *Apache HTTP Server*, instalado em uma *Raspberry Pi 3* Modelo B, assim como o banco de dados, que utiliza o sistema de gerenciamento de banco de dados MariaDB.

A comunicação com o hardware ocorre através do protocolo *Message Queue Telemetry Transport* (MQTT), publicando mensagens em um broker local, no qual o microcontrolador ESP8266-12F também está conectado. A ESP8266, por sua vez, interpreta as mensagens recebidas e se comunica através da sua porta serial com o microcontrolador PIC16F887, informando-o que a porta do ambiente deverá ser aberta. Ou seja, o sistema utilizará a rede local para transmitir dados entre os dispositivos clientes (aparelhos celulares dos usuários que estão acessando a plataforma), o servidor (instalado na Raspberry) e o hardware, seguindo o conceito de Internet das Coisas.

Para a criação das páginas web utilizadas na aplicação serão utilizadas as linguagens HTML (Hypertext Markup Language), CSS (Cascading Style Sheets) e JavaScript, além de PHP (Hypertext Preprocessor) para comunicação com o banco de dados, envio de requisições HTTP e mensagens para o broker MQTT com criptografia TLS.

**Palavras-chaves:** Controle de Acesso, Segurança, Servidor Local, Apache, Banco de dados MariaDB, PHP, HTML, CSS, HTTP, MQTT, Raspberry Pi, Internet das Coisas, TLS

# ABSTRACT

This work consists on the development and implementation of a platform that allows control and management of the access into the most important environments in the Federal University of Pernambuco's Department of Electrical Engineering. It’s main goal is to guarantee the safety and integrity of the equipment of high monetary and academic value inside classrooms and laboratories, preventing the entrance of unauthorized people and registering the horary of ingress and exit of all users that are allowed in the environment.

The application will allow the creation of three types of users: Student (who can access the environments on the days and times allowed), Teacher (beyond accessing the rooms, they can also be responsible for disciplines and environments, where they can manage access and visualize history) and Manager (able to create and edit environments, disciplines and users and manage all environments).

The software will be hosted in a local server Apache HTTP Server, installed in a Raspberry Pi 3 Model B, as well as the database, that uses the database management system MariaDB.

The communication with the hardware uses the Message Queue Telemetry Transport (MQTT), publishing messages in a local broker, in which the microcontroller ESP8266-12F is also connected. The ESP8266, interprets the received messages and communicates through its serial interface with the microcontroller PIC, informing that the room’s door must be open. That is, the system will use the local network to transmit data between client devices (cell phones of users who are accessing the platform), the server (installed on the Raspberry) and the hardware, following the concept of Internet of Things

In order to create the pages of the application the following languages will be used: HTML (Hypertext Markup Language), CSS (Cascading Style Sheets) e JavaScript, as well as PHP (Hypertext Preprocessor) to communicate with the database, send the HTTP requests and messages to the MQTT broker with TLS criptography.



**Keywords**: Access Control, Safety, Local Server, Apache, MariaDB Database, PHP, HTML, MQTT, Raspberry Pi, Internet of Things,TLS.

# LISTA DE ILUSTRAÇÕES

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ASF | - *Apache Software Foundation* |
| CA | - *Autoridade Certificadora* |
| CSS | - *Cascading Style Sheets* |
| CSV | - *Comma Separated Values* |
| DEE | - *Departamento de Engenharia Elétrica* |
| HTML | - *Hypertext Markup Language* |
| HTTP | - *Hypertext Transfer Protocol* |
| IP | - *Internet Protocol* |
| JS | - *JavaScript* |
| MD5 | - *Message Digest 5* |
| MQTT | - *Message Queue Telemetry Transport* |
| PHP | - *Hypertext Preprocessor* |
| RFID | - *Radio Frequency Identification* |
| SSL | - *Secure Sockets Layer* |
| TLS | - *Transport Security Layer* |
| UFPE | - *Universidade Federal de Pernambuco* |

# SUMÁRIO

# 1. INTRODUÇÃO

## 1.1 Conceito de Controle de Acesso

Segundo Halasz (2005), o controle de acesso é um sistema de dispositivos que gerencia e monitora de forma inteligente os eventos de acesso, com o objetivo de aumentar o nível de segurança em um local.

De acordo com Souza (2010), o controle de acesso agrega tecnologias de captação de dados e barreiras físicas, de forma a gerir o fluxo de pessoas dentro de uma organização. Ainda segundo Souza (2010), a forma como o controle desse fluxo será feito dependerá de diversos dispositivos que foram desenvolvidos através dos tempos, como por exemplo sistemas complexos com fechaduras magnéticas, portas giratórias etc.

## 1.2 Formulação do problema

Conforme Souza (2010) afirma, um sistema de controle de acesso surge a partir de duas necessidades: segurança e organização, obtidas através do controle de fluxo de pessoas e materiais.

Dessa forma, o controle de acesso em ambientes que possuem equipamentos de alto valor é uma grande preocupação para muitos gestores, tanto em espaços privados como espaços públicos.

À vista disso, um relevante exemplo de local que necessita desse tipo de sistema são os estabelecimentos de ensino. Nesses lugares, existem diversos ambientes, como por exemplo laboratórios de pesquisa e informática, que guardam equipamentos caros e por onde circulam muitas pessoas ao longo do dia. Assim, torna-se imprescindível ter o controle deste fluxo de pessoas, tanto para impedir a entrada de pessoas não autorizadas, como para registrar todos os acessos a esses ambientes.

O furto e os danos causados aos equipamentos instalados nesses locais podem gerar um grande prejuízo financeiro e comprometem projetos de pesquisas e atividades que estão sendo desenvolvidas nos laboratórios e salas

de aula, pois estes necessitam de uma estrutura adequada e equipamentos em bom estado.

De acordo com Norman (2011), antes de desenvolver um sistema de controle de acesso de uma instituição, existem diversos aspectos que devem ser analisados, entre eles estão: os tipos de ativos que irão ser protegidos pelo sistema, os tipos de usuários que irão utilizar o sistema e a criticidade do mesmo.

No caso a ser trabalhado, onde o sistema será instalado em um departamento de engenharia de uma universidade pública, os tipos de ativos a serem protegidos são equipamentos utilizados no desenvolvimento de projetos e pesquisas em laboratórios, assim como itens de mobília como cadeiras, mesas, projetores e aparelhos de ar-condicionado.

Além disso, os usuários que utilizarão o sistema serão alunos, professores e funcionários da área administrativa e a criticidade do sistema é alta, pois existem equipamentos de alto valor envolvidos.

Observa-se então que é necessário que o sistema desenvolvido seja:

- Robusto e confiável, pois a criticidade é alta, tendo em vista que se trata de patrimônio público e de alto valor monetário e científico;

- Que possua uma interface amigável e intuitiva, de modo que pessoas de diferentes formações acadêmicas e idades possam utilizar;

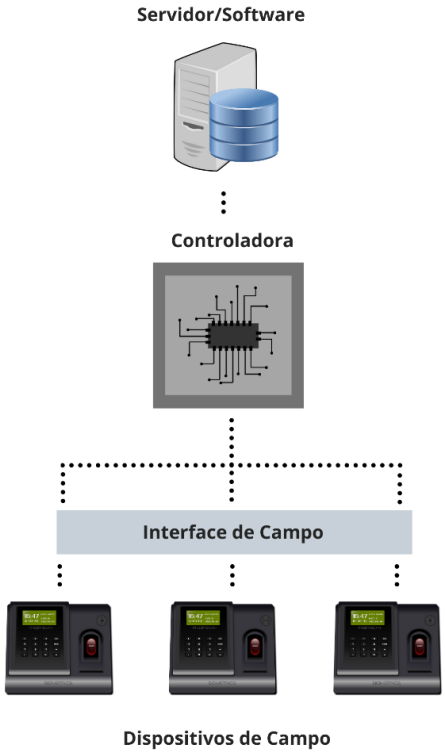
- Pouco invasivo, de modo a não alterar de forma significativa a estrutura do local e que possa ser instalado com facilidade em diversos ambientes;

## 1.3 Estrutura de um sistema de Controle de Acesso

De acordo com Halasz (2005), a maioria dos sistemas de controle de acesso disponíveis no mercado possui a seguinte arquitetura, dividida em 4 grupos: dispositivos de campo, interfaces de dispositivos de campo, controladoras/concentradoras e software/estação de trabalho/servidor.

A Figura 1 representa um esquemático da arquitetura básica com os elementos que serão apresentados.

*Figura 1: Arquitetura básica de um sistema de Controle de Acesso*




*Fonte: Próprio autor*

Os dispositivos de campo mais comuns são cartões de acesso (e seus respectivos leitores), leitores de biometria e controladores de fluxo (fechaduras, catracas, cancelas etc.).

As interfaces de campo são equipamentos responsáveis pela interface entre o sistema e os dispositivos de campo, monitorando seu funcionamento, sua condição (aberto/fechado) e que realiza sua interface de operação, através de comandos de abrir e fechar. Ou seja, recebe as informações dos dispositivos de campo e transmite para o sistema, de maneira que ele possa realizar a tomada de decisão (abrir/fechar), enviar a resposta para a interface, que irá transmitir para os dispositivos de campo controladores de fluxo.

As Controladoras/Concentradoras gerenciam o sistema. Elas possuem autonomia para operar o sistema, mesmo em caso de falha no servidor. Nem todos os sistemas possuem essa estrutura de “inteligência distribuída” e em

alguns sistemas a controladora e a interface de dispositivos se integram em um só equipamento.

O Software/Estação de trabalho é a interface gráfica principal entre os usuários e os dispositivos de campo. As principais estações de trabalho são a de cadastro e a de operação. O servidor é responsável pelo aplicativo e gerenciamento do acesso ao banco de dados.

## 1.4 Principais formas de Controle de Acesso existentes

Nesta seção serão apresentadas as principais formas de controle de acesso, assim como as vantagens e desvantagens relacionadas de cada uma delas. Em seguida, analisando as características de cada tipo de controle de acesso e as particularidades dos ambientes onde o sistema desenvolvido será instalado, será exposta a justificativa da escolha realizada do tipo de sistema.

### 1.4.1 Controladores de Fluxo: Fechaduras Elétricas e Eletromagnéticas

Como o sistema de controle desenvolvido neste trabalho é projetado para a instalação em ambientes internos de uma universidade, os dispositivos de campo utilizados para controlar o fluxo de pessoas não poderão ser catracas ou torniquetes (mais apropriados para instalação em ambientes externos).

Segundo Halasz (2005, p.14):

“As fechaduras são os dispositivos controladores mais utilizados, devido ao fato de ser necessário o controle de um grande número de salas em qualquer empresa, além do fato de que a maioria das salas já possui portas, o que reduz o investimento a ser feito”.

Dessa forma, a escolha será feita entre os dois tipos de fechadura mais comuns: fechaduras eletromagnéticas e fechaduras elétricas.

- Fechaduras Eletromagnéticas:

Segundo Halasz (2005) as fechaduras eletromagnéticas funcionam com eletroímãs que realizam o destravamento quando o fornecimento de energia é interrompido. Elas são mais silenciosas e menos invasivas que as fechaduras

elétricas, porém consomem mais energia, pois precisam estar sempre energizadas. Além disso, caso ocorra uma queda no fornecimento de energia e não tenha um sistema *nobreak* instalado, as portas serão destravadas e os ambientes ficarão vulneráveis. A Figura 2 apresenta uma Fechadura Eletromagnética, da marca IPEC.

*Figura 2: Fechadura Eletromagnética da marca IPEC*

*Fonte: Site UpperSeg (2020)*

- Fechaduras Elétricas: com relação ao consumo de energia, as fechaduras elétricas funcionam de maneira diferente das fechaduras eletromagnéticas. Nelas a lógica é inversa: quando elas são energizadas ocorre o destravamento da porta. Dessa forma, consomem menos energia e não necessitam da instalação de um sistema de *nobreak*, trazendo, dessa forma, um menor custo na instalação e manutenção. Porém, possuem menor durabilidade se comparadas às eletromagnéticas, devido à sua estrutura mecânica. A Figura 3 mostra um exemplo de Fechadura Elétrica, da marca IntelBras.

*Figura 3: Fechadura Elétrica da marca Intelbras*


*Fonte: Site Havan (2020)*

### 1.4.2 Cartões de Acesso

O tipo mais comum de controle de acesso é através da utilização de cartões de acesso, especialmente em grandes organizações. Nesse tipo de sistema, cada cartão é único e possui a identificação de cada usuário. Dessa forma, além de permitir somente a entrada de pessoas autorizadas, ele também possibilita aos gestores monitorar os horários de entrada e saída de funcionários.

- Códigos de Barras: é o tipo mais antigo de cartão de acesso. Nele, um certo padrão de barras (impressos ou colados sobre o cartão), correspondente à um código binário, é utilizado para identificar o cartão (e consequentemente o usuário), afirma Halasz (2005). Porém, esse padrão, por estar visível na superfície do cartão, como mostra a Figura 4, é muito vulnerável a cópias. De acordo com Souza (2010), esse tipo de controle de acesso é mais utilizado em processos que não são muito críticos ou para processos puramente administrativos.

*Figura 4: Cartão com código de Barras, da GlobalCards*

*Fonte: Site Global Cards (2020)*

- Cartões Magnéticos: possuem em sua superfície uma tarja magnética na parte de trás do cartão, ilustrada na Figura 5, onde ficam armazenadas as informações necessárias para a identificação do usuário.

A leitura desse tipo de cartão é feita através de um leitor que detecta as mudanças no campo magnético causadas pela tarja magnética. A maioria dos leitores usam dos seguintes métodos: inserção (usuário deve inserir o cartão no leitor), *swipe* (o cartão é deslizado por uma fenda) e proximidade (o usuário encosta o cartão na superfície do leitor).

Esse tipo de cartão, apesar de possuir um custo baixo de produção, pode ser facilmente danificado, especialmente se for exposto à campos magnéticos fortes. Além disso, assim como os cartões de códigos de barras, possui a desvantagem de serem facilmente copiados.

*Figura 5: Cartão Magnético, da empresa DuBrasil Soluções*


*Fonte: Site DuBrasil Soluções (2020)*

- Cartões de Proximidade: de acordo com Norman (2011), são os cartões que utilizam a tecnologia RFID (*Radio Frequency Identification* - Identificação por Radio Frequência) e são lidos quando colocados próximos à leitora de proximidade (sem a necessidade de tocar sua superfície, diferente dos cartões magnéticos de proximidade), como mostra a Figura 6. Os cartões de proximidade possuem três componentes: uma antena (bobina), um capacitor e um circuito integrado (que armazena o código único de cada cartão). A leitora de proximidade possui um campo magnético que excita a bobina e carrega o capacitor, energizando o circuito integrado, que descarrega seu código para a leitora através da antena. Segundo Halasz (2005), tipicamente cada fabricante utiliza frequências de operação diferentes, de modo que cartões de um fabricante não funcionem com leitores de outro.

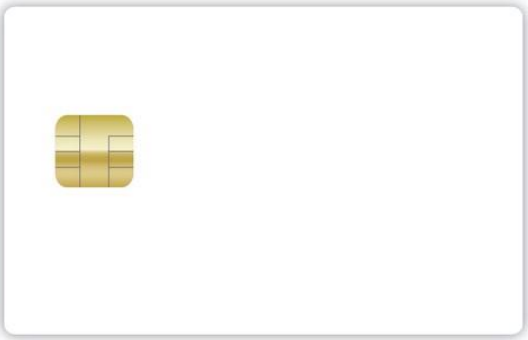
Suas principais vantagens são: maior confiabilidade (capazes de funcionar em ambientes hostis), maior durabilidade e alta velocidade. Porém possui custo elevado (comparado à outras tecnologias) e interferência de campos magnéticos gerados por materiais metálicos, como afirma Loureiro, Souza e Lopes (2015).

*Figura 6: Exemplo de uso do Cartão Magnético de Proximidade*

*Fonte: Site OnixSecurity (2017)*

- *Smartcards*: a tecnologia dos *smartcards,* ilustrada na Figura 7, tem operação muito semelhante à operação do cartão de proximidade, exceto pelo fato de que o microchip pode armazenar dados e não apenas transmitir os dados previamente gravados, segundo Halasz (2005). Devido a essa possibilidade de armazenamento, o nível de segurança pode ser maior, pois algoritmos mais complexos podem ser gravados nos cartões. De acordo com Souza (2010) a grande vantagem destes cartões é a facilidade de desenvolver aplicações muito interessantes já que eles possuem memória para gravação de informações e processamento.

*Figura 7: Smartcard, da marca GIESECKE + DEVRIENT*



*Fonte: Site Esp Tecnologia (2020)*

### 1.4.3 Teclado

O uso de teclados no controle de acesso é baseado na utilização de senhas, conhecidas apenas por pessoas autorizadas. Este tipo de sistema é bastante utilizado em condomínios e prédios, onde apenas moradores e funcionários sabem a senha. O teclado pode ser combinado com outras formas de controle como biometria e cartões, aumentando o nível de segurança. Além disso, pode ser usado em locais externos ou internos, como mostra a Figura 8.

Uma das vantagens dos teclados é a simplicidade no uso, sendo facilmente utilizados por pessoas de diferentes idades e com pouca familiaridade com tecnologias mais avançadas. Porém possui a desvantagem: a necessidade do toque nas teclas, podendo ser um meio de transmissão de vírus e bactérias.

*Figura 8: Teclados de uso interno e externo*


*Fonte: SOUZA (2010)*

### 1.4.4 Biometria

É uma tecnologia de custo mais elevado que utiliza uma característica física do usuário para identificá-lo e permitir o seu acesso. Essa característica pode ser a digital, a palma da mão, a face, a íris e até a voz. Em algumas aplicações, como as que utilizam a digital, há a necessidade do contato físico, como a representada na Figura 9.

*Figura 9: Leitor de Biometria da marca Futronic*

*Fonte: Site FX Biometria (2020)*

### 1.4.5 Justificativa

A partir do que foi exposto, é possível realizar a seguinte análise dos diferentes tipos de controle de acesso, como mostra a Tabela 1:

*Tabela 1: Tipos de fechadura*

| Tipo de Fechadura | Vantagens | Desvantagens |
|---|---|---|
| Fechadura Elétrica | Sem necessidade de sistema *nobreak* (menor custo) e menor consumo de energia | Menor durabilidade e mais ruidoso |
| Fechadura Eletromagnética | Silenciosas e menos invasivas | Necessidade de sistema *nobreak* (maior custo) e maior consumo de energia |

*Fonte: Próprio Autor*

Analisando a Tabela 1, observa-se que a fechadura eletromagnética, apesar de ser mais silenciosa (importante em ambientes como salas de aula e laboratórios) e menos invasiva, necessita da instalação de um sistema de *nobreak*, aumentando bastante o custo do sistema. Dessa forma, foi escolhida a

fechadura elétrica, pois atende suficientemente bem o sistema, possuindo menor custo de instalação e menor consumo de energia.

Observa-se na Tabela 2, que cada tipo de dispositivo possui suas vantagens e desvantagens.

*Tabela 2: Vantagens e Desvantagens dos dispositivos*

| Dispositivos | Vantagens | Desvantagens |
|---|---|---|
| Cartão com Código de Barras | Baixa complexidade | Vulnerável a cópias |
| Cartão Magnéticos | Custo Baixo | Facilmente danificados e vulnerável a cópias |
| Cartão de Proximidade | Maior confiabilidade, durabilidade e alta velocidade | Custo elevado e interferência de campos magnéticos |
| Smartcard | Capacidade de armazenamento no cartão, maior nível de segurança | Possibilidade de perda do cartão |
| Teclado | Facilidade no uso | Necessidade de contato físico |
| Biometria | Maior segurança | Custo elevado e algumas vezes necessidade de contato físico |

*Fonte: Próprio Autor*

É possível utilizar um dispositivo, diferente dos apresentados, mas que reúna todas as vantagens deles e não apresente as mesmas desvantagens?

A resposta está na utilização de uma plataforma acessível através dos aparelhos de celular. Dessa forma, o sistema utiliza dispositivos que os próprios usuários já dispõem e possuem familiaridade. Além disso, a solução elimina custos com produção de cartões e não há a possibilidade de perda ou danos de cartões.

Outra vantagem é que não haverá necessidade de contato físico em um objeto ou superfície compartilhado por várias pessoas, pois os celulares são objetos pessoais.

Ou seja, os cartões, teclados e leitoras são substituídos por um usuário e senha, acessível de qualquer dispositivo móvel conectado na rede do sistema.

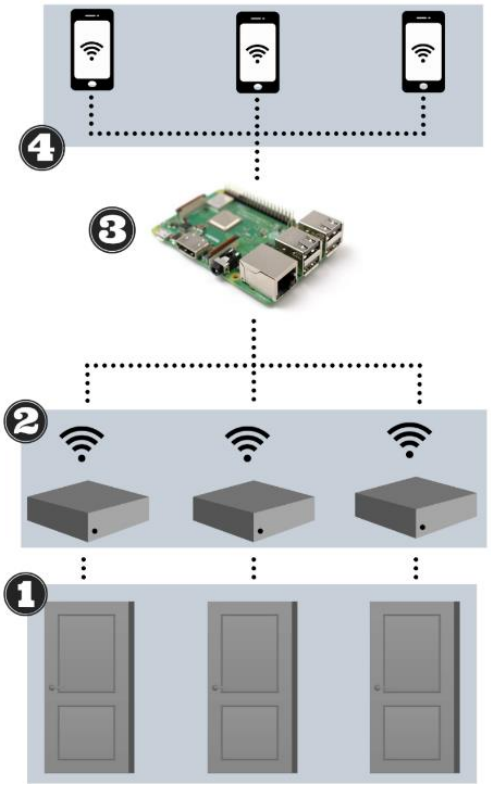
## 1.5 Arquitetura do sistema desenvolvido

No sistema de controle de acesso desenvolvido neste trabalho, é possível identificar os elementos que compõem a estrutura de um sistema de controle de acesso.

Na Figura 10, tem-se os seguintes componentes:

1) Dispositivos de campo: no sistema desenvolvido, os dispositivos de campo serão fechaduras eletrônicas que se comunicarão com as interfaces de campo através do canal serial.
2) Interfaces de campo: serão dispositivos elaborados e construídos de forma a se comunicar com os dispositivos de campo através do canal serial e com o servidor através da rede WiFi na qual ambos estão conectados. Esses dispositivos, irão receber comandos do servidor, interpretar e enviar o sinal para a fechadura eletrônica.
3) Controladora/Concentradora + Software/Servidor: na aplicação desenvolvida, o servidor, juntamente com o banco de dados e as páginas web da plataforma estão hospedados em uma Raspberry Pi 3. A plataforma possui a estação de cadastro, acessível aos usuários do tipo Administrador, e a estação de operação, acessível à todos os usuários cadastrados (com diferentes níveis de acesso).
4) Usuários: os usuários acessam a interface gráfica da plataforma através de seus smartphones e computadores.

*Figura 10: Arquitetura do sistema*




*Fonte: Próprio Autor*

## 1.6 Solução Proposta

### 1.6.1 Objetivo Geral

A partir dos conceitos e necessidades apresentados com relação à segurança de equipamentos e monitoramento do acesso de ambientes dentro de instituições de ensino, torna-se objetivo principal do presente trabalho desenvolver uma plataforma completa e de fácil implementação que realize o controle de travas eletrônicas instaladas nas portas de um ambiente acadêmico e sirva como obstáculo perante tentativas de furto ou depredação de equipamentos e móveis.

### 1.6.2 Objetivos Específicos

A aplicação desenvolvida deverá possuir as seguintes funcionalidades:

- Três tipos de usuários: Aluno, Professor e Administrador;

- O usuário Aluno será capaz de: abrir portas nos ambientes onde possui permissão, caso contrário também pode solicitar permissão de acesso aos responsáveis pelos ambientes;

- O usuário Professor poderá: além de todas as ações que um aluno é capaz de realizar, ele poderá também ser responsável por ambientes e disciplinas. Ao ser responsável pelo ambiente ele irá definir quais usuários terão acesso a ele, assim como visualizar, pesquisar e realizar o download de todos os dados do histórico (usuário, data e hora de todas as entradas e saídas realizadas no ambiente) do mesmo. Quando é responsável por uma disciplina, ele poderá editar ou remover essa disciplina;

- O usuário Administrador possui as seguintes possibilidades de ações: terá permissão para todas as ações que um professor é capaz de realizar e será capaz de criar e editar ambientes e disciplinas, além de cadastrar usuários. Ademais, possui acesso ao histórico e tem permissão de gerenciamento de todas as salas cadastradas no sistema;

- Além disso, ao abrir uma porta através da plataforma o usuário se torna “Ocupante” daquele ambiente até o momento que registra sua saída, de maneira a trazer um senso de responsabilidade e compromisso com a utilização dos ambientes, pois todo o seu histórico estará registrado no sistema. Enquanto há um “Ocupante” na sala, outros usuários, mesmo com permissão, não poderão abrir a porta pelo software;

- A plataforma será desenvolvida para uso em celulares, de modo a trazer praticidade sem a necessidade de conexão à Internet. Para acessar a plataforma, basta que o celular do usuário esteja conectado à mesma rede utilizada pelo sistema de controle de acesso.

# 2. REFERENCIAL TEÓRICO

Nesta seção serão comentadas as principais ferramentas utilizadas para a construção do sistema: o tipo de servidor, o gerenciador e a linguagem de banco de dados escolhida, as linguagens utilizadas para criação dos códigos e os protocolos de comunicação utilizados.

## 2.1 O protocolo de comunicação HTTP

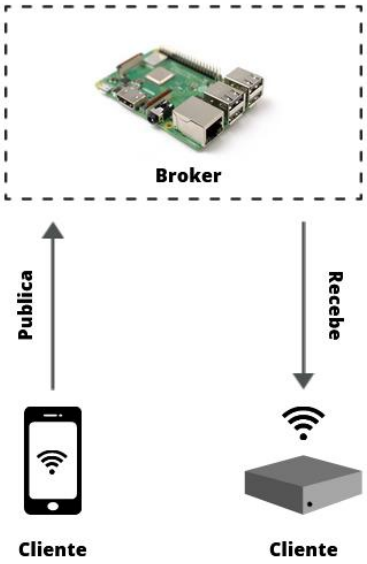
Um protocolo é um acordo entre partes, que estabelece as regras da comunicação, afirma Tanenbaum (2003). O protocolo escolhido para a comunicação dos usuários do sistema com o servidor foi o protocolo *HyperText Transfer Protocol* (HTTP).

Segundo Tanenbaum (2003), o HTTP é o protocolo de transferência utilizado em toda a *World Wide Web* e especifica as mensagens trocadas entre os clientes e servidores. Nesse protocolo, quando um navegador deseja ter acesso a uma página, ele envia a requisição ao servidor, que então transmite a página de volta.

## 2.2 O protocolo de comunicação MQTT

O protocolo de comunicação escolhido para a comunicação entre a aplicação e o hardware é o *Message Queuing Telemetry Transport* (MQTT). Esse protocolo segue o modelo publicação e assinatura. Neste modelo, existem dois tipos de entidades de rede: um broker, que é um servidor, e inúmeros clientes (que podem ser sensores, aplicações etc.), como afirma Yuan (2017). O cliente se conecta ao broker, se inscrevendo ou publicando em um tópico (o mesmo cliente pode se inscrever ou publicar em diversos tópicos). Todos os clientes que estão inscritos em um tópico ficam “ouvindo” o tópico e assim que chegar uma mensagem neste tópico, ele irá receber. Essa estrutura de broker e clientes, no contexto da aplicação desenvolvida neste trabalho, está representada na Figura 11.

*Figura 11: Estrutura de assinatura e publicação do MQTT*




*Fonte: Próprio Autor*

O broker MQTT possui usuário e senha, de forma a autenticar o cliente que está se conectando ao broker.

## 2.3 Segurança no broker: O protocolo TLS

Como a aplicação a ser desenvolvida se trata de um sistema de controle de acesso, a segurança é um aspecto que deve ser tratado com bastante seriedade.

Dessa forma, é necessário a utilização de protocolos que garantam segurança no tráfego de dados do sistema, protegendo-o de ataques externos.

O protocolo *Transport Layer Security* (TLS) foi uma evolução do antigo protocolo SSL (*Secure Sockets Layer*), de maneira que são referidos muitas vezes como o mesmo protocolo.

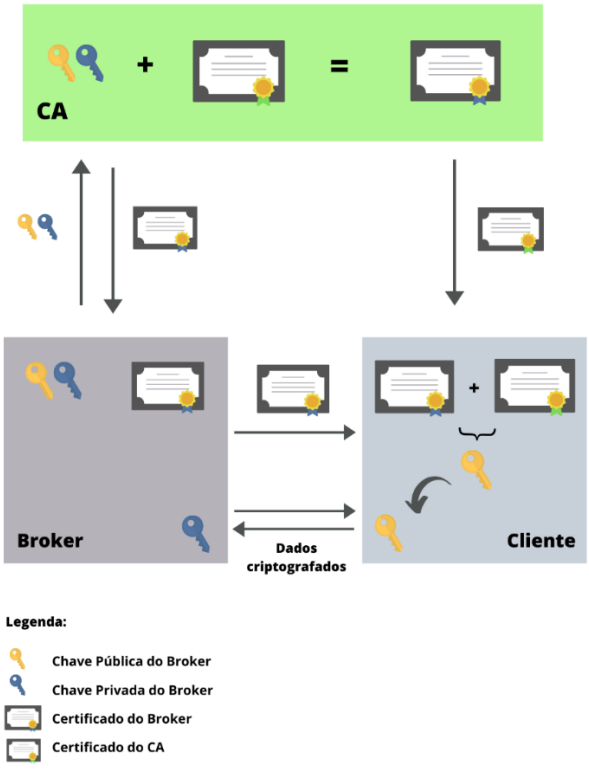
De acordo com Cope (2020), ao utilizar SSL/TLS é possível garantir que nenhum cliente não autorizado leu ou alterou sua mensagem e que você está se comunicando com o servidor correto, através da encriptação dos dados e da assinatura de quem enviou a mensagem, utilizando chaves. As chaves são números que, combinados com a mensagem através de um algoritmo, podem encriptar ou assinar a mensagem. São utilizadas duas chaves, uma pública e

uma privada (que são diferentes, mas possuem relação matemática entre si). Uma mensagem encriptada com uma chave pública não pode ser descriptada com a mesma chave pública, somente com a chave privada.

Ainda segundo Cope (2020), as chaves públicas são disponibilizadas para todo mundo e são verificadas através de certificados digitais, fornecidos por uma Certificadora (CA). Para obter um certificado digital é necessário preencher um formulário com as informações necessárias, adicionando o par de chaves e enviando para uma CA, que checa as informações e envia de volta as chaves em um certificado digital assinado do servidor.

Assim, quando algum cliente deseja acessar as chaves públicas de uma entidade, o certificado do servidor (que encapsula as chaves) é enviado, verificado (utilizando o certificado da CA) e, caso o resultado dessa verificação seja positivo, as chaves são consideradas confiáveis e utilizadas pelo cliente para trafegar dados criptografados, como mostra a Figura 12, onde o servidor é o broker do MQTT utilizado na aplicação.

*Figura 12: Estrutura de certificados e chaves do TLS aplicado à um broker*




*Fonte: Próprio autor*

## 2.4 Servidor local: Apache HTTP Server

Com o protocolo de comunicação definido, é necessário escolher qual servidor irá ser utilizado para hospedar a aplicação.

De acordo com a *Apache Software Foundation* (ASF), o *Apache HTTP Server* (Servidor HTTP da Apache) é um servidor web poderoso, flexível e atualizado com os protocolos mais recentes. Além disso, disponibiliza licença sem restrições e código aberto, sendo assim, constantemente atualizado.

Segundo Clemente (2019), o Apache HTTP Server é extremamente estável e utilizado por 43% de todos os sites do mundo, incluindo grandes nomes como Netflix, Airbnb, eBay e Microsoft.

Ou seja, é um servidor confiável, gratuito e compatível com diversos tipos de hardware, tornando-o bastante apropriado a aplicação desenvolvida neste trabalho.

Esse servidor será local e instalado em uma *Raspberry Pi* 3, computador portátil de baixo custo. Dessa forma, a aplicação não dependerá de conexão à internet, pois o servidor e os clientes poderão se comunicar através da rede local, como mostra a Figura 13.

*Figura 13: Comunicação via HTTP*


*Fonte: Próprio Autor*

## 2.5 Banco de Dados MariaDB

Guardar e relacionar informações é essencial para diversos tipos de aplicações, especialmente em sistemas de controle de acesso. É necessário armazenar informações sobre os ambientes cadastrados, os usuários, as permissões e o histórico de acesso de cada um deles.

De acordo com Alexandruk (2018), os sistemas gerenciadores de banco de dados são sistemas que armazenam e organizam os dados de forma que possam ser acessados de diferentes maneiras, gerando informações úteis para os sistemas.

O MariaDB é um dos bancos de dados relacionais de código aberto mais utilizados no mundo. Surgiu do MySQL (da Oracle), com o qual é compatível até hoje. O MariaDB libera atualizações com maior frequência que o MySQL, possui melhor desempenho e é totalmente gratuito. Por essas razões se tornou o gerenciador de banco de dados escolhido para a aplicação desenvolvida neste trabalho.

## 2.6 Construção de páginas web: HTML, CSS e JavaScript

A interface de interação com o usuário do sistema desenvolvido neste trabalho será construída utilizando as seguintes linguagens:

- Linguagem de Marcação de Hipertexto (HTML): é a linguagem padrão de construção de sites. Com ela é possível criar vários tipos de telas, exibir imagens, vídeos e criar diversos elementos como botões, formulários, menus, sliders etc.

- *Cascading Style Sheets* (CSS): é a linguagem utilizada para definir o estilo da página HTML. Os arquivos que contêm as propriedades (cor, tamanho, bordas, margens etc.) dos elementos HTML, escritos em CSS, são chamados de “folhas de estilo”.

- *JavaScript* (JS): de acordo com Flanagan (2013), é a linguagem que estabelece o comportamento da página web, utilizada pela maioria dos sites modernos, sendo assim a linguagem de programação mais onipresente da história. O *JavaScript* define a dinâmica da página e como ela vai interagir com os usuários.

## 2.7 PHP: Comunicação com o banco de dados e requisições HTTP

Nas seções anteriores foram definidos: o servidor que vai hospedar as páginas web (*Apache HTTP Server*), o sistema de gerenciador de banco de dados que irá guardar as informações necessárias (MariaDB) e as linguagens utilizadas na construção das páginas (HTML, CSS e JavaScript). Mas como as páginas irão consultar e alterar as informações que estão no banco de dados? É necessária a utilização de uma linguagem que realize essa comunicação, a linguagem PHP (*Hypertext Preprocessor*). Diferente do JavaScript, que é executado pelo cliente, geralmente um navegador web, o PHP é executado pelo servidor, que no caso desta aplicação será o Apache.

Além de realizar a comunicação com o banco de dados, a linguagem PHP também será utilizada para transportar dados entre as páginas, garantindo que as informações sigam o fluxo de navegação do usuário, através de requisições HTTP.

## 2.8 Criptografando dados: Criptografia MD5

O algoritmo *Message-Digest* 5, MD5, é um algoritmo de *hash* de 128 bits unidirecional, ou seja, não pode ser reconvertido no texto que o gerou. Dessa forma, é muito utilizado para proteger senhas, pois se torna difícil de descobrir, através de tentativa e erro, duas mensagens que gerem a mesma *hash*. No sistema criado nesse trabalho, esse tipo de criptografia será usado para proteger as senhas dos usuários, guardadas no banco de dados.

## 2.9 Gerando arquivos: o formato CSV

Uma das principais ferramentas que garantem a segurança de um ambiente que possui um sistema de controle de acesso é o Histórico de Acesso.

O Histórico de Acesso é um log onde estão registrados todos os acessos ao ambiente, contendo informações dos usuários que acessaram o ambiente e os horários e datas de cada acesso. Dessa forma, é importante ter a opção de

gerar um arquivo contendo esses dados. Existem diversos tipos de formatos de arquivo que podem ser utilizados nessa aplicação, entre elas o formato CSV (*Comma Separated Values*).

No formato CSV os dados são armazenados separados por vírgulas. Este formato é aceito por diversas aplicações (entre elas, o Excel) e é facilmente gerado utilizando funções da linguagem PHP, sendo assim é uma escolha adequada para esse tipo de sistema.

# 3 DESENVOLVIMENTO

No capítulo a seguir será mostrado todo o processo de desenvolvimento da plataforma, desde a elaboração do fluxo entre as páginas da plataforma para cada tipo de usuário, o mapeamento da estrutura do banco de dados e as telas (já implementadas e completamente funcionais) do sistema.

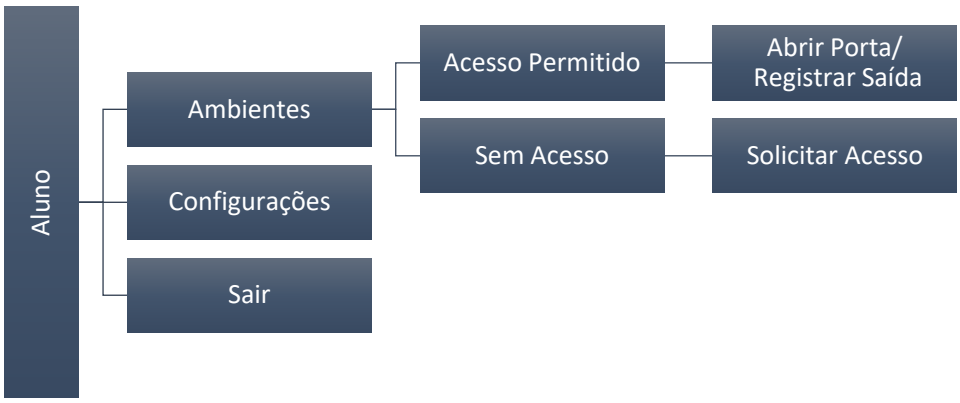
## 3.1 Estrutura da Plataforma

A plataforma de controle de acesso foi desenvolvida de forma que existam três estruturas diferentes, uma para cada tipo de usuário.

### 3.1.1 Estrutura do tipo Aluno

A Estrutura do tipo Aluno é composta das seguintes páginas, como mostra a Figura 14:

*Figura 14: Estrutura do tipo Aluno*




*Fonte: Próprio Autor*

O menu principal do usuário do tipo Aluno terá três opções:

- Ambientes: Ao selecionar essa opção, o usuário será redirecionado a uma página que mostrará todos os ambientes existentes na plataforma, onde ele poderá escolher a visualização dos ambientes que ele

possui permissão de acesso e os ambientes que ainda não possui permissão de acesso.

Nos ambientes que possui permissão de acesso, ao selecionar um ambiente são exibidas informações sobre ele (tipo de ambiente, capacidade e quantidade de aparelhos de ar-condicionado) e as opções de “Abrir Porta” (caso a sala não esteja com um Ocupante) ou “Registrar Saída” (caso o próprio usuário seja o Ocupante). Caso nenhuma das duas opções apareça, uma mensagem indicando que a sala já está ocupada é exibida na tela.

Nos ambientes que o usuário não possui permissão de acesso, as mesmas informações sobre o ambiente são exibidas, porém a única opção que aparece é a de “Solicitar Acesso”, onde o usuário é redirecionado para uma página onde pode escrever uma mensagem solicitando o acesso, que será encaminhada para o responsável pelo ambiente, que poderá aprovar ou não o pedido.

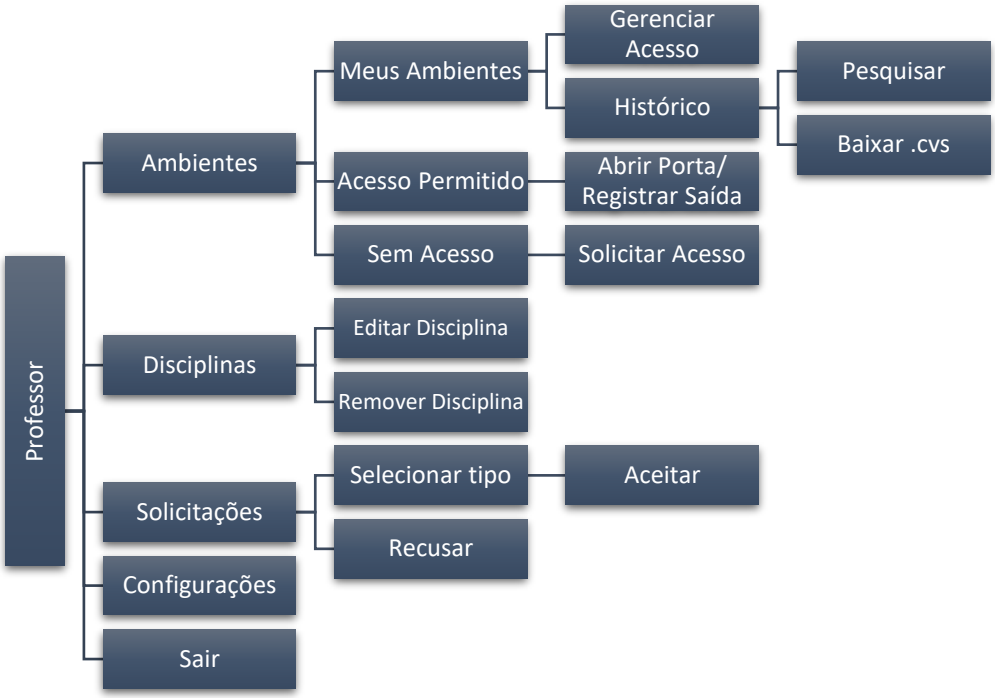
- Configurações: nesta seção, o usuário poderá editar o seu nome de usuário, CPF, e-mail e senha.

- Sair: redireciona o usuário para a tela de Login.

### 3.1.2 Estrutura do tipo Professor

A Estrutura do tipo Professor é composta das seguintes páginas, como mostra a Figura 15:

*Figura 15: Estrutura do tipo Professor*




*Fonte: Próprio Autor*

O usuário do tipo Professor terá cinco opções:

- Ambientes: Ao selecionar essa opção, o usuário será redirecionado a uma página que mostrará todos os ambientes existentes na plataforma, onde ele poderá escolher a visualização dos ambientes pelos quais é responsável, dos que ele possui permissão de acesso e os ambientes que não possui permissão de acesso.

Nos ambientes em que o usuário professor não é responsável, que possui permissão de acesso ou não, o funcionamento é similar ao da Estrutura do tipo Aluno.

Nos ambientes pelos quais é responsável, uma página denominada “Meus Ambientes”, aparecerá com uma lista de todos os ambientes cujo usuário professor está registrado como Responsável. Nesses ambientes ele acessa o “Histórico” e poderá “Gerenciar o Acesso” a esses ambientes.

Ao selecionar a opção “Histórico”, ele poderá ver todo o registro de entradas e saídas daquele ambiente em uma tabela que trará informações do CPF do usuário que entrou/saiu do ambiente, horário e data da ação e o tipo do registro (Entrada/Saída). Além disso, ele poderá pesquisar os registros de uma data específica e baixar todos os dados em formato CSV.

Na opção “Gerenciar Acesso”, o professor visualizará uma lista de todos os usuários que possuem permissão para acessar as salas sob sua responsabilidade, podendo a qualquer momento, remover a permissão de acesso de algum desses usuários.

- Disciplinas: nesta página estão disponíveis todas as disciplinas em que o usuário está cadastrado como professor. Ao selecionar a disciplina, ele terá acesso a todas as informações daquela disciplina (horário da disciplina, dias da semana e código) e poderá editá-las.

- Solicitações: lista com todas as solicitações de acesso para os ambientes pelos quais o usuário é responsável. Na lista, aparecem o nome e o CPF do solicitante e ao clicar sobre o pedido, o professor visualizará a mensagem relacionada ao pedido, tendo as opções de aceitar ou recusar a solicitação.

Para aceitar uma solicitação ele deverá escolher o tipo de acesso que o usuário solicitante irá receber: “Acesso Provisório”, “Acesso Permanente” ou “Acesso por Disciplina”.

Se o acesso for Provisório, o usuário terá acesso total (todos os dias da semana, 24 horas por dia) ao ambiente, até determinada data.

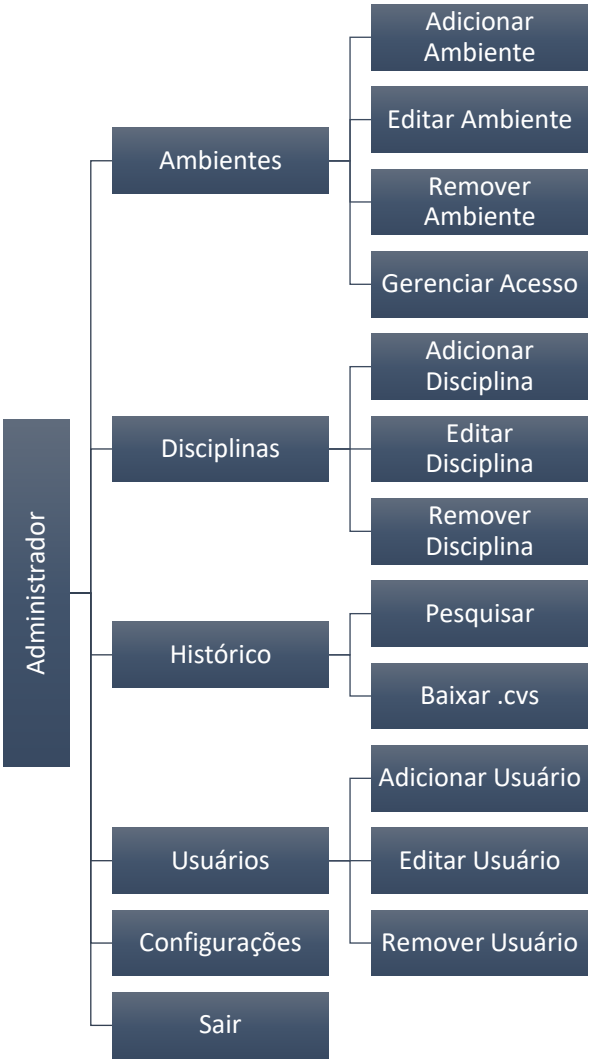
Se o acesso for Permanente, o usuário terá acesso total ao ambiente, até que o responsável pela sala remova o seu acesso.

Se o acesso for por Disciplina, o responsável pela sala irá escolher, entre as disciplinas cadastradas, qual delas é a que o solicitante pertence. Dessa forma, o usuário solicitante poderá abrir a sala apenas nos horários e dias da semana correspondentes ao da disciplina.

### 3.1.3 Estrutura do tipo Administrador

A Estrutura do tipo Administrador é composta das seguintes páginas, como mostra a Figura 16:

*Figura 16: Estrutura do tipo Administrador*




*Fonte: Próprio autor*

O menu principal do usuário do tipo Administrador terá seis opções:

- Ambientes: o administrador terá acesso a todos os ambientes cadastrados no sistema, em cada ambiente ele poderá editar a sala (alterar nome, CPF do responsável, capacidade, quantidade de aparelhos de ar-condicionado e endereço IP (*Internet Protocol Address*) do hardware na rede local), remover o ambiente do sistema, gerenciar acesso (da mesma forma que o responsável pela sala) e histórico (da mesma forma que o responsável pela sala). Além disso também poderá adicionar um novo ambiente ao sistema.

- Disciplinas: nesta página, ele poderá visualizar as disciplinas existentes, adicionar, editar ou remover uma disciplina.

- Usuários: o administrador terá acesso às informações sobre todos os usuários cadastrados, podendo adicionar ou remover um usuário do sistema.

## 3.2 Estrutura do Banco de Dados

O banco de dados utilizado para armazenar informações sobre os usuários e registros de acesso é formado por 4 tabelas padrão, além de uma tabela por usuário do tipo Professor. As tabelas padrão são Ambientes, Acesso, Histórico e Usuários.

### 3.2.1 Tabela Ambientes

A Tabela de Ambientes possui os dados cadastrados de todos os ambientes. Os campos da tabela Ambientes são:

*Tabela 3: Campos da tabela Ambiente*

| Campo | Descrição |
|---|---|
| id_Ambiente | Número de identificação do ambiente. Cada ambiente possui seu próprio ID, que é único. |
| nome_Ambiente | Número de identificação do ambiente. Cada ambiente possui seu próprio ID, que é único. |
| CPF_Responsavel | CPF do usuário responsável pela sala |
| Tipo | Define se o ambiente é uma Sala de Aula ou um Laboratório |
| Capacidade | Informa a capacidade máxima de alunos que o ambiente pode acomodar. |
| Quantidade_AC | Quantidade de aparelhos de ar-condicionado instalados no ambiente |
| Mac | Endereço MAC do microcontrolador Esp8266 incorporado ao hardware instalado na porta do ambiente. |
| Status | Informa se o ambiente está ocupado (ou seja, possui um ocupante ativo que entrou no ambiente e ainda não registrou a |

| | |
|---|---|
| | saída). Se o ambiente estiver ocupado seu valor é 0 (FALSE), caso contrário seu valor é 1 (TRUE). |
| Ocupante | CPF do ocupante atual do ambiente. |

*Fonte: Próprio autor*

.

### 3.2.2 Tabela Acesso

A tabela de Acesso guarda informações de permissão de acesso de todos os ambientes cadastrados. A Tabela 4 mostra os campos relacionados à Acesso.

*Tabela 4: Campos da tabela Acesso*

| Campo | Descrição |
|---|---|
| Id_Ambiente | Número de identificação do ambiente. É o mesmo da coluna Id_Ambiente da Tabela Ambientes. |
| CPF | CPF do usuário que possui permissão de acessar aquele ambiente. |
| Tipo | Indica o tipo do acesso (Permanente, Provisório ou Disciplina). |
| Disciplina | Caso o acesso seja do tipo Disciplina este campo é preenchido com o nome da disciplina, caso contrário, fica vazio. |

*Fonte: Próprio autor*

### 3.2.3 Tabela Histórico

A tabela de Histórico possui todos os registros de entradas e saídas dos ambientes cadastrados ao longo do tempo. A Tabela 5 mostra os campos relacionados à Histórico.

*Tabela 5: Campos da tabela Histórico*

| Campo | Descrição |
|---|---|
| Id_Ambiente | Número de identificação do ambiente onde houve o registro de acesso. É o mesmo da coluna Id_Ambiente da Tabela Ambientes e Acesso. |
| Nome_Ambiente | Nome do ambiente |
| CPF_Usuario | CPF do usuário que entrou/saiu do ambiente. |
| Hora | Horário em que ocorreu o acesso. |
| Data | Dia em que ocorreu o acesso. |
| Tipo | Informa se o registro é de Entrada ou Saída. |

*Fonte: Próprio autor*

### 3.2.4 Tabela Usuários

A tabela de Usuários guarda as informações referentes aos usuários que utilizam o sistema. A Tabela 6 mostra os campos relacionados à Usuários.

*Tabela 6: Campos da tabela Usuários*

| Campos | Descrição |
|---|---|
| Nome | Nome do usuário. |
| CPF | CPF do usuário |
| Senha | Senha utilizada pelo usuário para acessar o sistema. |
| E-mail | E-mail do usuário. |
| Tipo | Aluno, Professor ou Administrador |

*Fonte: Próprio autor*

### 3.2.5 Tabela Solicitações

Na tabela de Solicitações encontram-se todas as solicitações de acesso que ainda não foram respondidas. A Tabela 7 mostra os campos relacionados à Solicitações.

*Tabela 7: Campos da tabela Solicitações*

| Campo | Descrição |
|---|---|
| Nome_Solicitante | Nome do usuário que fez a solicitação |
| CPF_Solicitante | CPF do usuário que fez a solicitação |
| id_Amb | Id do ambiente que o usuário solicitou acesso. |
| Mensagem | Mensagem da solicitação. |
| CPF_Responsável | CPF do usuário responsável pelo ambiente. |

*Fonte: Próprio autor*

## 3.3 Implementação do sistema

### 3.3.1. Tela de Login

Na Tela de login do sistema, como mostra a Figura 17, o usuário deverá informar o seu CPF e a sua senha (previamente cadastrados no sistema). Dessa forma o sistema irá identificar se o usuário e senha existem no sistema, através de uma consulta ao banco de dados. Essa consulta, além de verificar se o usuário está cadastrado e a senha está correta, também informa qual o tipo de acesso que esse usuário possui (Aluno, Professor ou Administrador), de forma que o sistema possa direcionar esse usuário para as páginas correspondentes ao seu nível de acesso. O sistema também codifica a senha informada (utilizando MD5), de forma a analisar se a senha é a mesma que está guardada no banco e autorizar o login do usuário.

Além disso, o sistema envia o CPF do usuário para a tela inicial do usuário, em forma de *cookie* (informação que será enviada junto aos cabeçalhos HTTP). Essa informação é enviada neste formato sempre que o usuário sai de uma página e vai para outra, de forma que o sistema sempre tenha essa informação disponível.

Caso o usuário ou senha estejam incorretos, o sistema exibirá a mensagem “Usuário e/ou Senha incorretos” e o sistema será redirecionado para a Tela de login.

.

*Figura 17: Tela de login do sistema*


*Fonte: Próprio autor*

### 3.3.2. Aluno: Tela Inicial

Ao ser redirecionado para a tela inicial do tipo Aluno, o sistema (que possui a informação do CPF do usuário) realiza uma consulta na tabela **Acesso** do banco de dados. Nesta consulta ele compara o CPF do usuário com o valor da coluna “CPF” em todas as linhas da tabela.

Caso o valor seja igual, é necessário verificar qual o tipo de acesso e analisar a sua validade.

Se o acesso for do tipo “Permanente”, o sistema automaticamente já considera que o usuário tem acesso a esse ambiente.

Se for do tipo “Provisório”, o sistema irá verificar na coluna “Prazo_Limite” qual a data limite de acesso e comparar com a data atual, verificando se o usuário ainda possui acesso válido.

Para o acesso do tipo “Disciplina”, o sistema irá seguir o seguinte passo a passo:

1. Obter o nome da disciplina, na coluna Disciplina da tabela Acesso;

2. Verificar, na tabela Disciplinas, quais os dias da semana e horários desta disciplina;
3. Descobrir o dia da semana e horário atuais;
4. Conferir se o dia da semana e horário atuais estão dentro dos horários da disciplina.

Caso o passo 4 tenha um resultado positivo, o aluno terá acesso ao ambiente.

Dessa forma, a tela inicial do usuário do tipo Aluno exibirá uma lista de todos os ambientes que ele possui acesso naquele momento.

Cada item da lista, além de conter o nome do ambiente, possui um indicador de ocupação em seu canto superior direito. Caso o ambiente esteja com um ocupante registrado (ou seja, um usuário registrou a entrada no ambiente, mas ainda não registrou a saída), o indicador fica azul, caso contrário, cinza, como mostra a Figura 18.

*Figura 18: Aluno – Tela inicial*

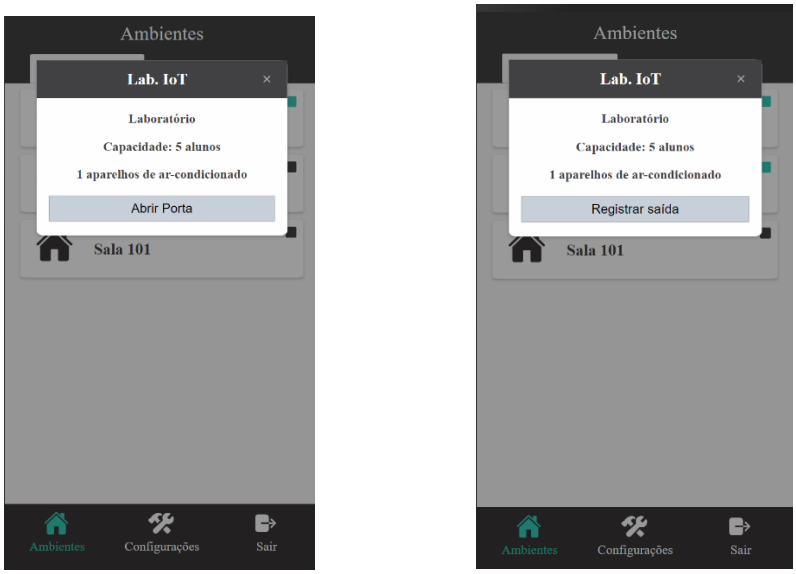

*Fonte: Próprio autor*

Quando o usuário clica em um dos ambientes, um modal referente ao ambiente selecionado aparece na tela. Se o ambiente não possuir um ocupante ativo, além das principais informações sobre a sala (nome, tipo, capacidade e quantidade de aparelhos de ar-condicionado), um botão de “Abrir Porta” é exibido, como mostra a Figura 19 (a). Se o aluno apertar esse botão, o sistema

envia um comando de “Abrir” para o dispositivo instalado na porta daquele ambiente. Além disso, registra a data e horário de entrada do usuário no histórico do ambiente.

Ao sair do ambiente, o usuário deve registrar a saída, seguindo o mesmo caminho mostrado anteriormente, desta vez apertando o botão “Registrar Saída”, a Figura 19 (b) mostra.

*Figura 19: Aluno – Ambiente com acesso permitido*

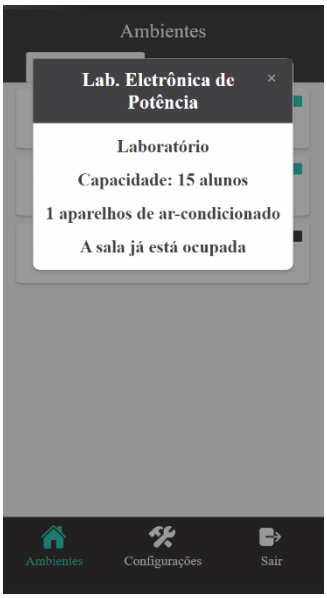



*(a) Opção de Abrir Porta* *(b) Registro de saída do Ambiente*

*Fonte: Próprio autor*

Caso o ambiente já esteja ocupado, uma mensagem “O ambiente está ocupado” é exibida na tela (Figura 20).

*Figura 20: Ambiente ocupado por outro usuário*

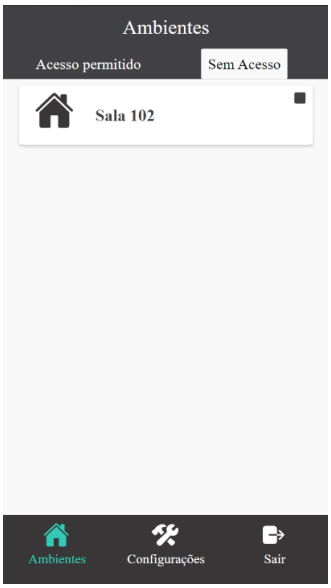



*Fonte: Próprio autor*

Além disso a tela também possui outros elementos, como o menu na área inferior da tela, que dá acesso a todas as páginas do sistema.

Na região superior da tela, observa-se a aba “Sem Acesso”, que ao ser selecionada redireciona o usuário para uma lista dos ambientes cadastrados no sistema que ele não possui acesso, como mostra a Figura 21.

*Figura 21: Aluno - Ambientes sem acesso*

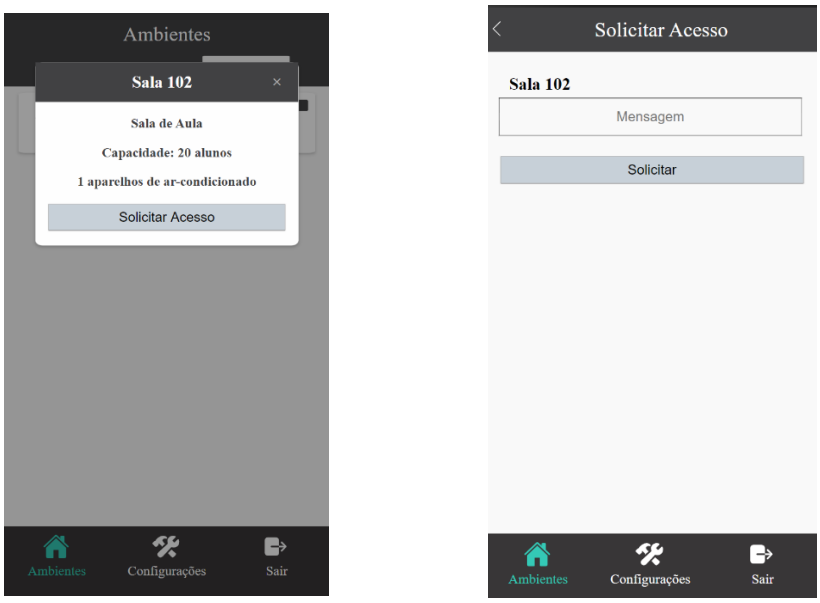



*Fonte: Próprio autor*

Para exibir a tela de Ambientes sem acesso, o sistema realiza duas consultas ao banco de dados: na primeira, consulta os id's de todos os ambientes que o usuário possui acesso na tabela Acesso, armazenando-os em um vetor e na segunda, percorre a tabela Ambientes comparando o id de cada ambiente com os id's armazenados no vetor. Caso o id do ambiente não esteja dentre os guardados no vetor, o sistema reconhece que o usuário não possui acesso a ele e o exibe na tela.

Para solicitar acesso ao ambiente, o usuário deverá clicar no ambiente desejado e em seguida apertar no botão "Solicitar Acesso", como mostra a Figura 22 (a).

*Figura 22: Solicitando acesso a um ambiente*




*(a) Opção de Solicitar Acesso* *(b) Aluno - Tela de solicitação de acesso*

*Fonte: Próprio autor*

Ao clicar nesse botão, o usuário é redirecionado à página de solicitação de acesso, como mostra a Figura 22 (b)

Na página de solicitação de acesso, o aluno poderá inserir uma mensagem, que será enviada ao responsável pelo ambiente, junto com a solicitação.

Quando o aluno envia uma solicitação, o sistema insere na tabela Solicitações a nova solicitação, com o nome e CPF do usuário solicitante, mensagem, id do ambiente e CPF do responsável pelo ambiente. Após o envio, o sistema é redirecionado para a página de Ambientes sem acesso.

### 3.3.3. Aluno: Configurações

Na tela de configurações, conforme a Figura 23, são exibidos os dados do usuário, que podem ser alterados e salvos, ao apertar o botão “Salvar Alterações”. Quando o usuário salva as alterações, o sistema compara todas as informações enviadas com as informações antigas e identifica se houve alguma alteração de valor em algum dos campos. Se houver alteração, ele salva os novos valores, caso contrário, salva os valores antigos.

Se o usuário selecionar a opção “Sair”, será direcionado para a página de login.

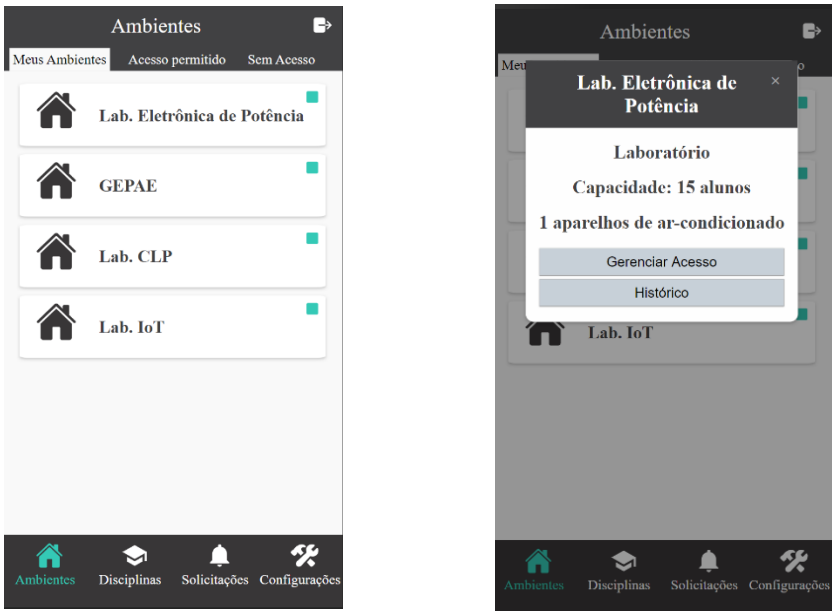
*Figura 23: Aluno - Tela de configurações*


*Fonte: Próprio autor*

### 3.3.4. Professor: Tela Inicial

A tela inicial do usuário do tipo professor é a tela de “Meus Ambientes”. Nesta tela, o sistema realiza uma busca na tabela Ambientes do banco de dados e exibe todos os ambientes cujo CPF do responsável é igual ao CPF do usuário. Possui um layout similar ao da tela principal do usuário do tipo Aluno, inclusive com o mesmo indicativo de ocupação do ambiente, conforme mostra a Figura 24 (a).

*Figura 24: Professor – Tela "Meus Ambientes"*




*(a) Professor - Meus Ambientes'* *(b) Professor - Tela de Ambiente*

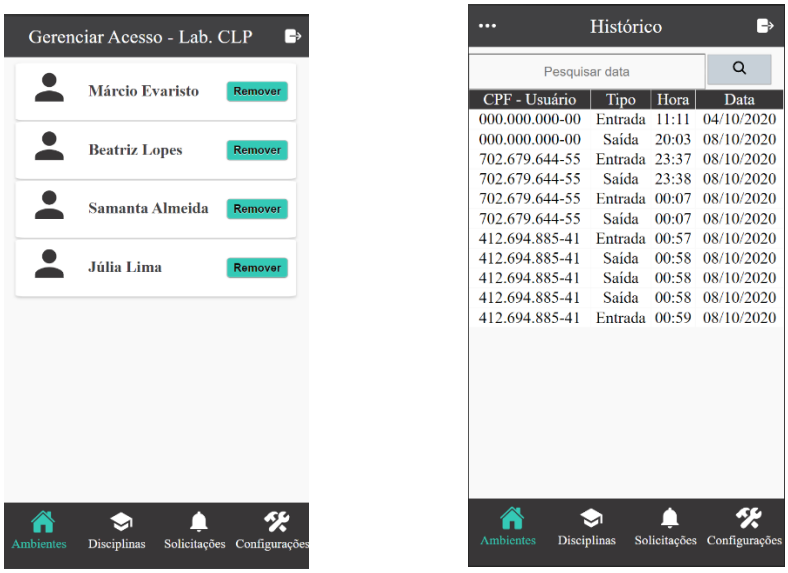
*Fonte: Próprio autor*

As abas "Acesso Permitido" e "Sem Acesso" funcionam da mesma forma que no usuário do tipo Aluno.

Ao clicar em um dos ambientes, uma tela será exibida, com as informações do ambiente e as opções de "Gerenciar Acesso" e "Histórico", como mostra a Figura 24 (b).

Em "Gerenciar Acesso", o professor tem acesso a uma lista com todos os usuários que possuem acesso ao ambiente, como mostra a Figura 25 (a).

*Figura 25: Professor – Ferramentas de gestão de ambientes*




*(a) Professor – Gerenciamento de Acesso* *(b) Professor – Histórico de Ambiente*

*Fonte: Próprio autor*

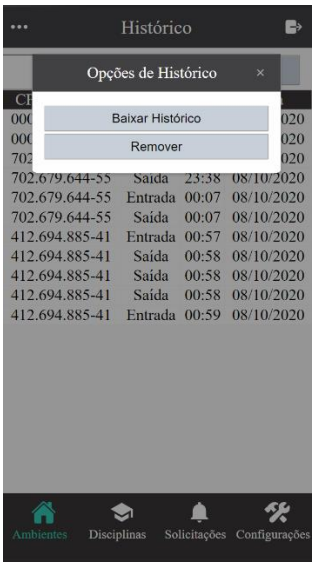
Nesta página, o sistema pesquisa na tabela Acesso todos os usuários que possuem acesso ao ambiente, comparando os valores do campo “Id_Ambiente” com o id do ambiente selecionado.

Além disso, o professor também pode remover o acesso dos usuários, clicando no botão remover, ao lado do nome do usuário. Dessa forma, o acesso é removido do banco de dados.

Analisando a Figura 25 (b), é possível observar a página de Histórico do ambiente. Nela, o usuário visualiza todo o histórico de acessos do ambiente, podendo filtrar as informações inserindo a data desejada na barra de pesquisa.

Além disso, também possui a opção de baixar um arquivo no formato CSV contendo todo o histórico (ou apenas da data desejada) e remover o histórico daquele ambiente, como é possível visualizar na Figura 26.

*Figura 26: Professor – Histórico do Ambiente*



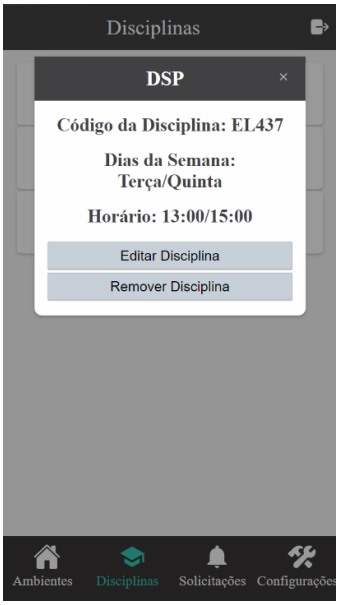

*Fonte: Próprio autor*

### 3.3.5. Professor: Disciplinas

Ao selecionar a opção “Disciplinas” no menu inferior, o usuário acessa a lista de disciplinas em que ele está cadastrado como professor, conforme a Figura 27 (a).

*Figura 27: Professor – Disciplinas*


*(a) Professor – Tela de Disciplinas*

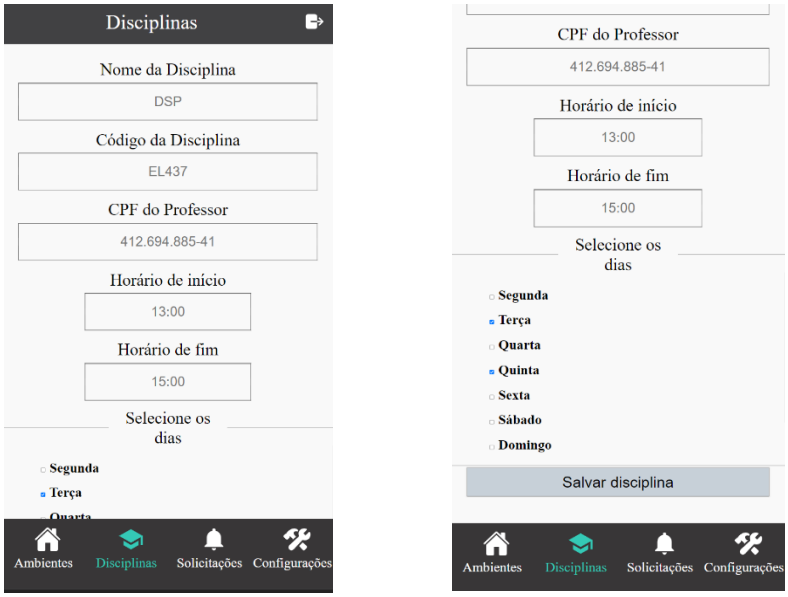



*(b) Professor – Tela de Disciplina*

*Fonte: Próprio autor*

Ao clicar na disciplina, é possível ver as suas informações e acessar a área de edição da disciplina, como mostra a Figura 27 (b).

*Figura 28: Professor – Edição de Disciplina*




*(a) Professor – Edição de Disciplina* *(b) Professor – Edição de Disciplina*

*Fonte: Próprio autor*

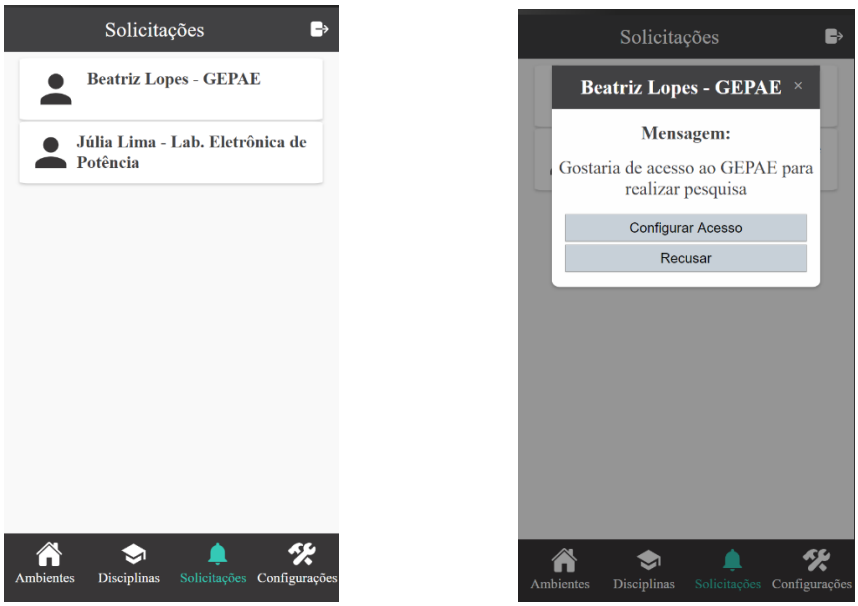
Na tela de Edição de Disciplina, é possível alterar as informações cadastradas da disciplina, conforme exibido nas Figuras 28 (a) e 28 (b).

### 3.3.6. Professor: Solicitações

Na barra inferior de navegação, caso exista alguma solicitação pendente endereçada ao usuário, um número aparece junto ao ícone de Solicitações, indicando a quantidade de solicitações pendentes.

Na tela de solicitações, o usuário visualiza todos os pedidos de permissão de acesso direcionados aos ambientes pelos quais ele é responsável, ou seja, todas as linhas da tabela Solicitações onde o campo “CPF_Responsavel” é igual ao CPF do usuário logado, conforme a Figura 29 (a).

*Figura 29: Professor - Solicitações*




*(a) Professor – Tela de Solicitações* *(b) Professor – Tela de Solicitação*

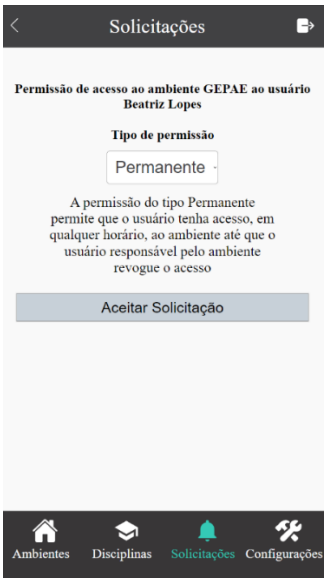
*Fonte: Próprio autor*

Como mostra a figura 29 (b), ao selecionar uma solicitação o professor poderá configurar o acesso, ou seja, escolher o tipo de permissão que ele irá conceder ao usuário, ou recusar o pedido.

Ao escolher a opção de configurar o acesso, o primeiro tipo de solicitação é o Permanente. Para alterar o tipo, basta selecionar as outras opções utilizando o dropdown.

Se for Permanente, nenhuma entrada é solicitada e o professor pode simplesmente aceitar a solicitação, como mostra a Figura 30. Dessa forma, uma nova linha é adicionada à tabela Acesso, com o id do ambiente, o CPF do usuário ao qual o acesso foi concedido, e o tipo “Permanente”. Nesse caso, os campos “Disciplina” e “Prazo_Limite” ficam nulos, pois não são utilizados.

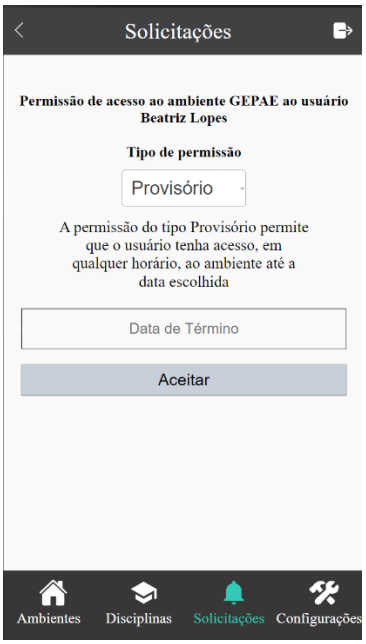
*Figura 30: Professor – Solicitação Permanente*




*Fonte: Próprio autor*

Caso o professor queira conceder um acesso com data limite, ou seja do tipo “Provisório”, ele terá que preencher a entrada “Data de Término”, que será o valor do campo “Prazo_Limite”, determinando a data em que o acesso perderá a validade, conforme a Figura 31.

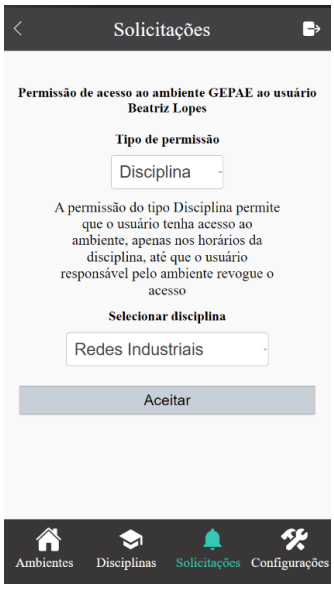
*Figura 31: Professor – Solicitação Provisória*




*Fonte: Próprio autor*

Na terceira opção o acesso do Tipo Disciplina, exibida na Figura 32, o sistema exibirá um dropdown com todas as disciplinas que o professor ensina (ou seja, as mesmas exibidas na tela Disciplinas). O nome da disciplina selecionada será o valor do campo “Disciplina” na nova linha da tabela Acesso.

*Figura 32: Professor – Solicitação do tipo Disciplina*




*Fonte: Próprio autor*

### 3.3.7. Professor: Configurações

A página de Configurações do usuário Professor tem o funcionamento similar ao do tipo Aluno, como mostra a Figura 33.

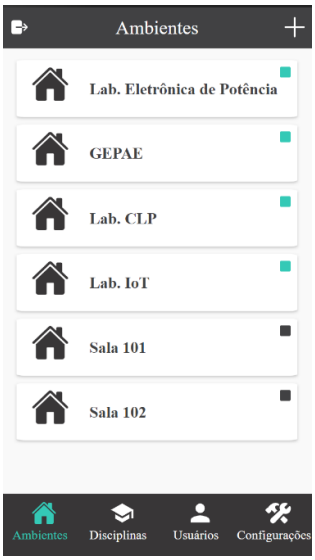
*Figura 33: Professor – Telas de Configurações*


*Fonte: Próprio autor*

### 3.3.8. Administrador: Tela inicial

Para o usuário do tipo Administrador, a tela inicial mostra todos os ambientes cadastrados no sistema, em um layout similar ao dos outros tipos de usuários, porém sem restrições, conforme a Figura 34.

*Figura 34: Administrador – Tela Inicial*




*Fonte: Próprio autor*

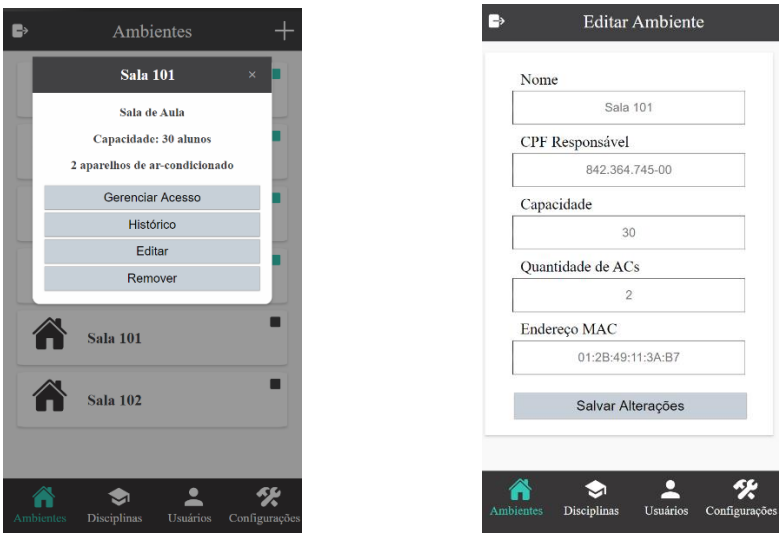
Na região superior da tela existem dois botões: o botão de sair, no canto superior esquerdo, que leva o usuário de volta à tela de login e o botão de adicionar ambiente. Nesta última opção, é exibida uma tela onde são preenchidos os dados no novo ambiente a ser cadastrado no sistema, como mostra a Figura 35, adicionando uma nova linha na tabela Ambientes. Quando um novo ambiente é adicionado, é concedido automaticamente o acesso permanente ao responsável pelo ambiente.

*Figura 35: Administrador – Tela de criação de ambiente*


*Fonte: Próprio autor*

Na tela de ambientes, ao selecionar um ambiente, o usuário possui 4 opções: Gerenciar Acesso e Histórico (que possuem as opções semelhantes a um usuário Professor, quando responsável por um ambiente), Editar e Remover, como mostra a Figura 36 (a).

*Figura 36: Administrador – Telas de Ambiente e Edição de Ambiente*




*(a) Administrador – Tela de Ambiente* *(b) Professor – Tela de Edição de Ambiente*

*Fonte: Próprio autor*

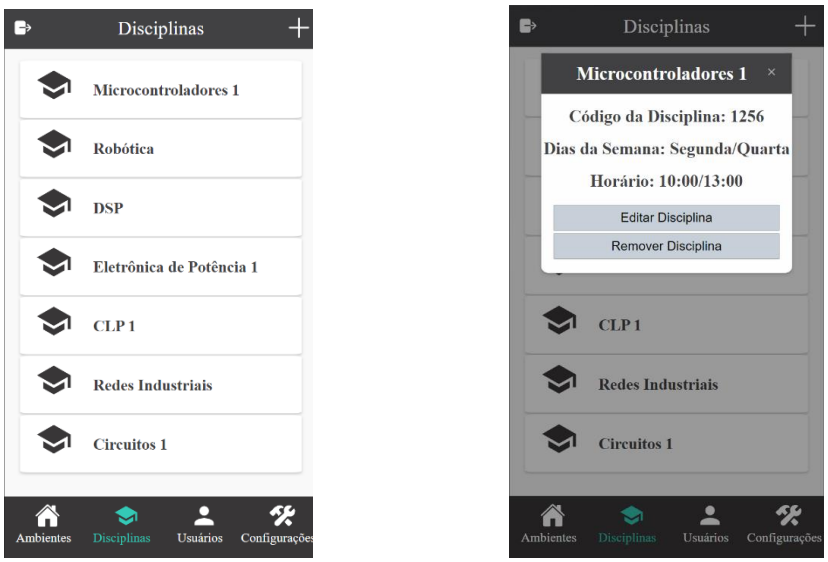
Selecionando a opção Editar, uma tela similar à de Configurações dos usuários Aluno e Professor é exibida, desta vez com as informações do ambiente, conforme a Figura 36 (b).

Ao clicar na opção “Remover”, o ambiente selecionado é removido da tabela ambientes.

### 3.3.9. Administrador: Disciplinas

Em “Disciplinas” o sistema exibe todas as disciplinas cadastradas no sistema, como mostra a Figura 37 (a). Na barra horizontal superior da tela, existem as opções de sair e de adicionar disciplina, da mesma forma que a tela “Ambientes”.

*Figura 37: Administrador – Telas de Disciplinas*



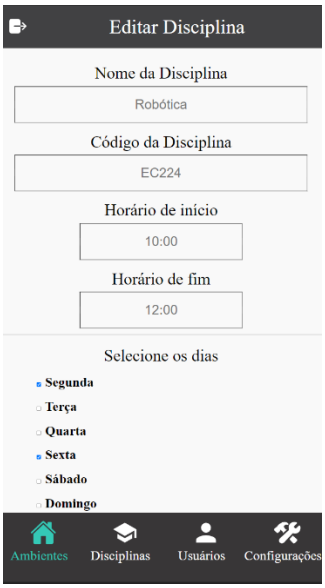

*(a) Administrador – Tela de Ambiente* *(b) Administrador – Tela de Edição de Ambiente*

*Fonte: Próprio autor*

Quando o usuário seleciona uma das disciplinas, um modal com dados da disciplina e botões de ação é exibido, de forma semelhante à tela de “Disciplinas” do usuário professor, com duas opções: “Editar Disciplina” e “Remover Disciplina”, conforme mostra a Figura 37 (b).

Na tela de edição de Disciplina, ilustrada na Figura 38, é possível editar os dados da disciplina, semelhante ao usuário Professor, porém com a possibilidade de editar todas as disciplinas cadastradas no sistema.

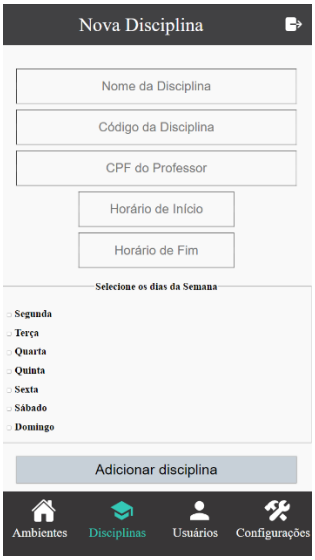
*Figura 38: Administrador – Tela de Edição de Disciplina*



*Fonte: Próprio autor*

Ao selecionar a opção de adicionar nova disciplina, o usuário é redirecionado para a tela “Nova Disciplina” (Figura 39), informações sobre a disciplina a ser cadastrada são preenchidas. Na opção de dias da semana (ou seja, os dias que a disciplina é lecionada), o usuário pode escolher mais de uma opção. Nesse caso, o sistema irá identificar os valores de todas as opções selecionadas e concatenar em uma única string, com os valores separados por “/”, inserindo, com este formato, no campo “dias_Semana” da nova linha da tabela Disciplina.

*Figura 39: Administrador – Tela de criação de Disciplina*

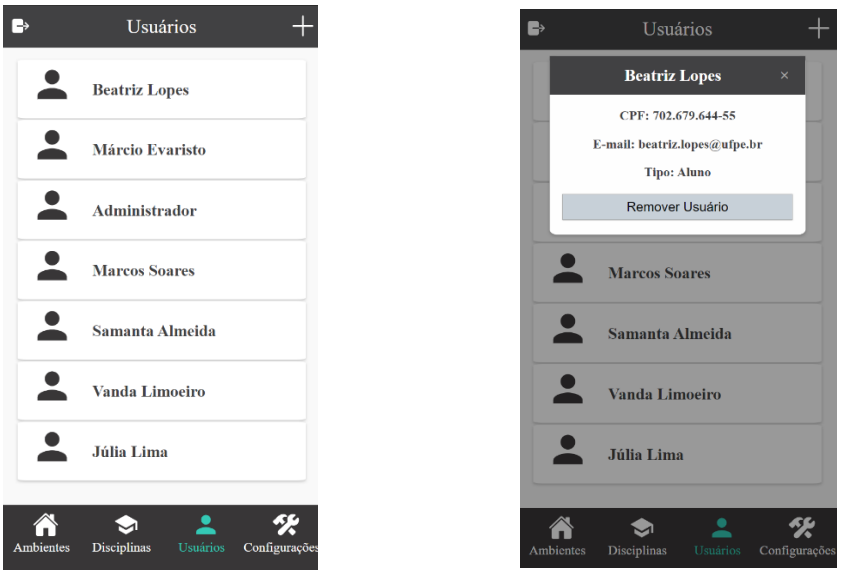



*Fonte: Próprio autor*

### 3.3.10. Administrador: Usuários

Em “Usuários”, o administrador tem acesso à lista com todos os usuários do sistema, conforme a Figura 40 (a).

*Figura 40: Administrador – Telas de Usuários*




*(a) Administrador – Tela de Usuários* *(b) Administrador – Tela de Usuário*

*Fonte: Próprio autor*

Como mostra a Figura 40 (b), ao selecionar o usuário, ele tem acesso à suas informações (exceto senha) e a opção de remover o usuário do sistema.

Além disso, também é capaz de adicionar um novo usuário ao sistema, seguindo o mesmo padrão das telas “Ambientes” e “Disciplinas”, como mostra a Figura 41.

*Figura 41: Administrador – Tela de criação de usuário*


*Fonte: Próprio autor*

## 3.3.11. Administrador: Configurações

A página de Configurações tem o funcionamento semelhante aos outros tipos de usuário, conforme a Figura 42.

*Figura 42: Administrador – Tela de Configurações*


*Fonte: Próprio autor*

# 4 Resultados

Nesta seção serão apresentadas situações reais de utilização da plataforma, assim como a resposta da plataforma à essas situações. Os casos a serem retratados são:

- Usuário com permissão no momento da solicitação
- Usuário com permissão do tipo Disciplina, fora do horário da disciplina
- Usuário com permissão do tipo Provisório, fora da data limite

Para cada situação, serão apresentadas as telas de interface do usuário, assim como imagens do banco de dados e do broker, de forma a visualizar como os dados estão estruturados e monitorar os tópicos do broker.

## 4.1 Acesso Permitido

Neste tipo de situação, o usuário possui permissão de acesso no momento que entra na página do Ambiente. Esta situação pode ocorrer de 3 formas:

- O usuário possui permissão do tipo Permanente com esse Ambiente;
- O usuário possui permissão do tipo Provisória e a data atual é anterior ao prazo limite;
- O usuário possui permissão do tipo Disciplina e o horário atual está dentro dos horários permitidos da Disciplina.

A Figura 43 mostra a tabela de Acesso no banco de dados, onde é possível observar que o usuário cujo CPF é “000.000.000-00” (meramente ilustrativo e escolhido apenas para testes) possui acesso do tipo permanente ao ambiente cujo id é 3, que corresponde ao ambiente “GEPAE”, como mostra a imagem da tabela de Ambientes na Figura 44.

*Figura 43: Tabela Acesso*

| Id_Ambiente | CPF | Disciplina | Tipo | Prazo_Limite |
|---|---|---|---|---|
| 2 | 000.000.000-00 | NULL | Provisorio | 10/08/2020 |
| 3 | 000.000.000-00 | NULL | Permanente | NULL |
| 4 | 000.000.000-00 | NULL | Permanente | NULL |
| 6 | 000.000.000-00 | Robótica | Disciplina | NULL |

*Fonte: Próprio Autor*

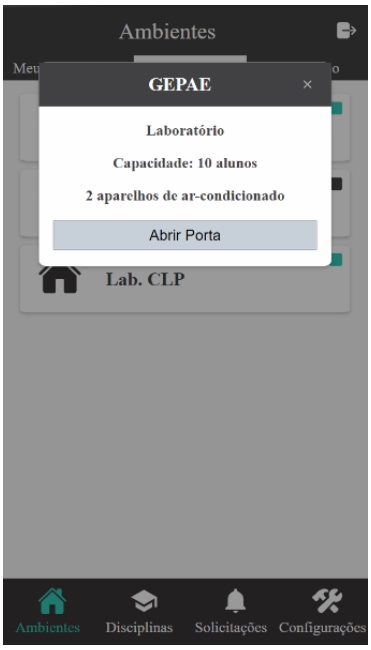
*Figura 44: Tabela de Ambientes*

| id_Ambiente | nome_Ambiente | CPF_Responsavel | Tipo |
|---|---|---|---|
| 2 | Lab. Eletrônica de Potência | 412.694.885-41 | Laboratório |
| 3 | GEPAE | 412.694.885-41 | Laboratório |
| 4 | Lab. CLP | 412.694.885-41 | Laboratório |
| 6 | Lab. IoT | 412.694.885-41 | Laboratório |

*Fonte: Próprio Autor*

Na plataforma, ao acessar esse ambiente, o usuário se depara com a tela do ambiente, apresentada anteriormente. Caso o ambiente não esteja com um Ocupante cadastrado, o botão “Abrir Porta” ficará disponível para o usuário, como mostra a Figura 45.

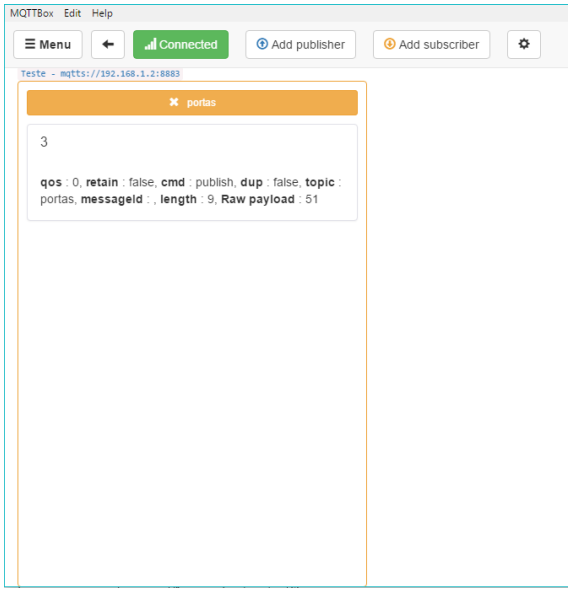
*Figura 45: Acesso permitido*




*Fonte: Próprio Autor*

Quando o usuário aperta o botão “Abrir Porta”, uma mensagem é enviada ao tópico “Portas” no broker, com o id do ambiente no qual a porta deverá ser aberta. Utilizando o software MQTTBox, disponibilizado pelo Google Chrome, é possível monitorar as mensagens que chegam nesse tópico (Figura 46).

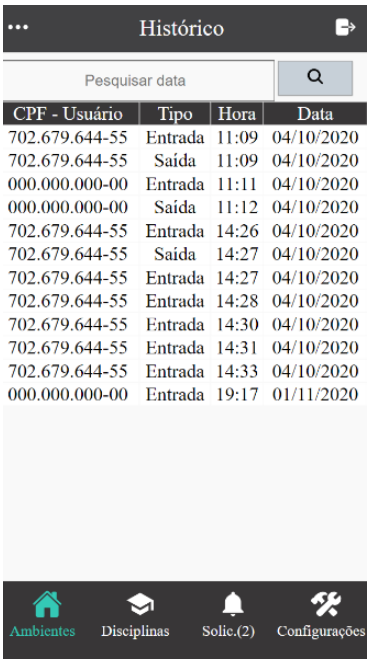
*Figura 46: Mensagem enviada ao broker*




*Fonte: Próprio Autor*

Além disso, também é registrada a entrada no histórico do Ambiente, conforme ilustrado na Figura 47.

*Figura 47: Registro do acesso no histórico*




*Fonte: Próprio Autor*

## 4.2 Permissão do tipo Disciplina, fora do horário permitido

A Figura 43 mostra que o usuário possui a permissão do tipo Disciplina para o ambiente com id = 6, ou seja, “Lab. IoT”, cuja Disciplina cadastrada é “Robótica”. É possível observar na tabela Disciplinas, que o horário que o usuário tem acesso ao ambiente são de 10h às 12h nos dias de segunda-feira e sexta-feira, como mostra a Figura 48.

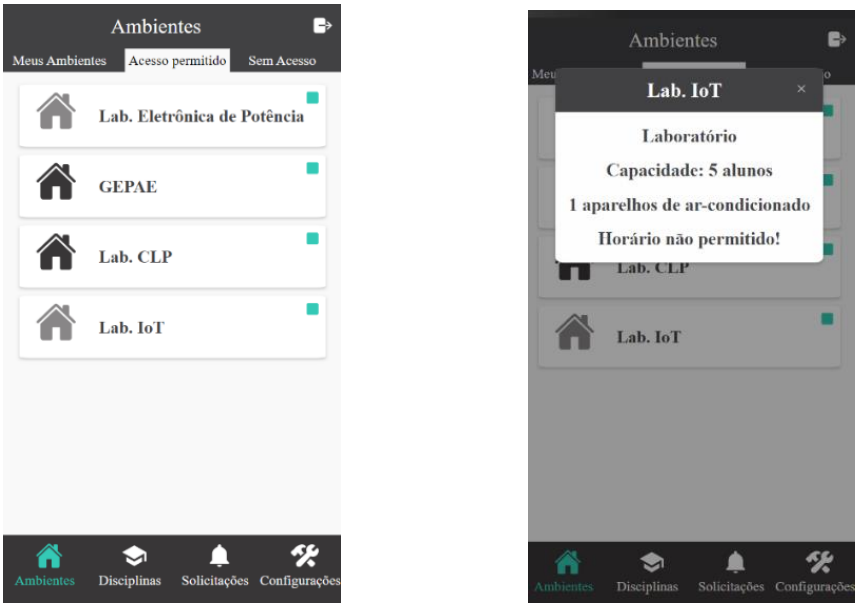
*Figura 48: Tabela Disciplinas*

| nome_Disciplina | cod_Disciplina | CPF_Professor | dias_Semana | horario |
|---|---|---|---|---|
| Microcontroladores 1 | 1256 | 000.000.000-00 | Segunda/Quarta | 10:00/13:00 |
| Robótica | EC224 | 000.000.000-00 | Segunda/Sexta | 10:00/12:00 |
| DSP | EL437 | 412.694.885-41 | Terça/Quinta | 13:00/15:00 |
| Eletrônica de Potência 1 | EL396 | 412.694.885-41 | Segunda/Quarta | 15:00/17:00 |
| CLP 1 | EL407 | 842.364.745-00 | Terça/Sexta | 10:00/12:00 |
| Redes Industriais | EL408 | 412.694.885-41 | Quinta | 13:00/15:00 |
| Circuitos 1 | EE102 | 842.364.885-12 | Terça/Quinta | 08:00/10:00 |

*Fonte: Próprio Autor*

Dessa forma, caso o usuário tente acessar o ambiente em um horário fora desses intervalos permitidos, ele não conseguirá abrir o ambiente, como mostram as telas mostradas nas Figuras 49 (a) e 49 (b).

*Figura 49: Ambiente bloqueado em horários não permitidos*



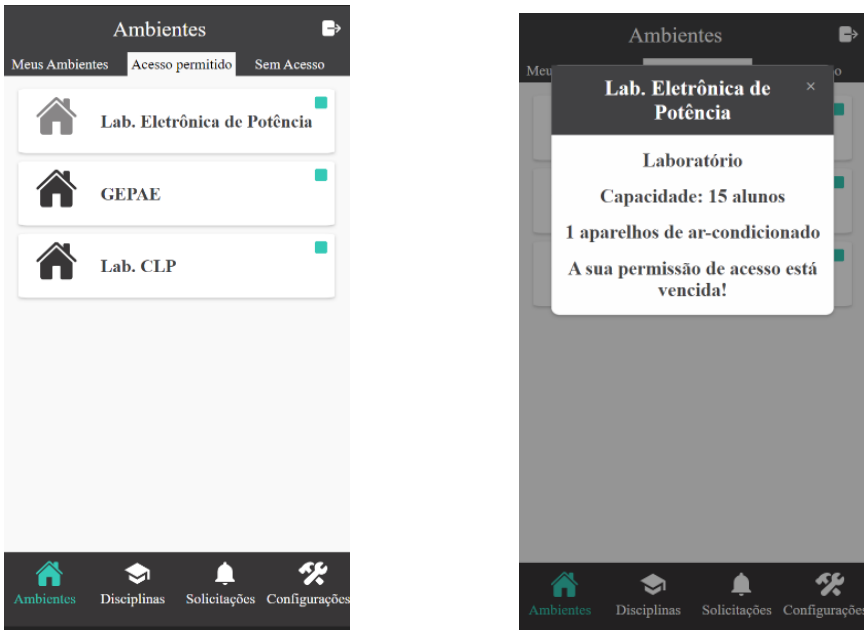

*(a) Tela com ambientes bloqueados* *(b) Aviso de horário não permitido*

*Fonte: Próprio autor*

## 4.3 Permissão do tipo Provisório, depois da data limite

Na Figura 44 apresentada anteriormente, também é possível observar que o usuário possui a permissão do tipo provisório para o ambiente com id = 2, ou seja, “Lab. de Eletrônica de Potência”, cujo prazo limite é o dia 10/08/2020. Ao acessar a página de Ambientes em uma data posterior ao prazo limite, o usuário se depara com as telas mostradas nas Figuras 50 (a) e 50 (b), que mostra que o usuário não pode acessar o ambiente.

*Figura 50: Ambiente bloqueado por vencimento de permissão*




*(a) Tela com ambientes bloqueados* *(b) Aviso de permissão vencida*

*Fonte: Próprio autor*

# 4. CONCLUSÃO

É possível observar que a plataforma desenvolvida atingiu os objetivos propostos para a construção de um sistema de controle de acesso para uso em ambientes acadêmicos, atendendo os seguintes aspectos:

- Segurança: plataforma acessível somente através de usuário e senha cadastrados, uso de protocolo TLS para garantir integridade e legitimidade dos dados e criptografia de senhas MD5 no banco de dados;

- Organização: diferentes níveis de acesso e permissões;

- Confiabilidade: não depende de conexão com a internet, evitando a instabilidade;

- Sem necessidade de contato físico em superfícies compartilhadas como telas ou teclados: o usuário utiliza o próprio celular para acessar o sistema e abrir a porta/registrar saída;

- Menor custo operacional: não há custos associados à compra de cartões ou manutenção de leitoras;

- Facilidade no uso: interface amigável e intuitiva, com mensagens explicativas;

Além disso, o sistema foi projetado para diversos tipos de situações, baseadas em fatos do dia a dia de um campus universitário e de acordo com demandas trazidas pelos próprios docentes e discentes, de forma a atender ao máximo as necessidades dos usuários finais.

Após a instalação dos primeiros protótipos, serão recolhidos feedbacks de alunos, professores e funcionários do departamento onde será instalado o projeto piloto. Essas informações serão utilizadas futuramente no desenvolvimento de uma nova versão do sistema, com as seguintes características:

- Ajustes relacionados aos feedbacks recebidos (adição, alteração ou remoção de funcionalidades, melhorias no fluxo de utilização da plataforma e na interface);

- Implementação de cadastro feito pelo próprio usuário, com opção de recuperar senha.

- Criação de log de utilização do sistema: registrar quando um usuário altera, adiciona ou remove um ambiente, disciplina ou permissão de um usuário.

- Mensagens de confirmação para ações críticas como remover ambientes, disciplinas e usuários;

# 5. REFERÊNCIAS BIBLIOGRÁFICAS


1. SOUZA, Marcelo Barbosa de; **Controle de acesso: conceitos, tecnologias e benefícios**. 1º edição, São Paulo: Sicurezza, 2010.
2. HALASZ, Rodolfo Simon; **Sistema Integrados de Segurança**. 1º edição, São Paulo: Sicurezza, 2005.
3. NORMAN, Thomas; **Eletronic Access Control**, 1º edição, Butterworth-Heinemann, 2011.
4. SEU CONDOMÍNIO. **Controle de Acesso com Cartão Magnético**. [*S. l.*], 21 set. 2018. Disponível em: https://www.seucondominio.com.br/noticias/controle-de-acesso-com-cartao-magnetico. Acesso em: 12 abr. 2020.
5. **CONTROLE de Acesso com Cartão Magnético**. [*S. l.*], 21 set. 2018. Disponível em: https://www.seucondominio.com.br/noticias/controle-de-acesso-com-cartao-magnetico. Acesso em: 12 abr. 2020.
6. **FAQ - HTTPD - Apache Software Foundation**. [*S. l.*], 2019. Disponível em: https://cwiki.apache.org/confluence/display/HTTPD/FAQ. Acesso em: 16 maio 2020.
7. **O QUE é e por que usar o servidor Apache**. [*S. l.*], 26 jun. 2019. Disponível em: https://rockcontent.com/blog/apache/. Acesso em: 16 maio 2020.
8. ALEXANDRUK, Marcos. **SQL – Structured Query Language: rápido e fácil**. São Paulo: Universidade Nove de Julho: UNINOVE, 2018. 232 p. ISBN 78-85-89852-66-1.
9. **9 vantagens de migrar do MySQL para o MariaDB**. [*S. l.*], 4 jul. 2018. Disponível em: 9 vantagens de migrar do MySQL para o MariaDB. Acesso em: 16 maio 2020.
10. FLANAGAN, David. **JavaScript: o guia definitivo**. 6. ed. Porto Alegre: Bookman, 2013. 1062 p. ISBN 978-85-65837-19-4.
11. TANEMBAUM, Andrew S. **Redes de computadores**. 4. ed. [*S. l.*]: Campus, 2003. 955 p. ISBN 9788535211856.

12. **RFID Identificação por Rádio Frequência: Vantagens e Desvantagens**. [*S. l.*], 2015. Disponível em: https://www.gta.ufrj.br/grad/15_1/rfid/vantadesvan.html. Acesso em: 17 maio 2020.
13. VALE, Cristiano. **Criptografia MD5**. [*S. l.*], 2007. Disponível em: https://www.devmedia.com.br/criptografia-md5/2944. Acesso em: 4 out. 2020.
14. YUAN, Michael. **Conhecendo o MQTT**: Por que o MQTT é um dos melhores protocolos de rede para a Internet das Coisas?. [*S. l.*], 4 out. 2017. Disponível em: https://developer.ibm.com/br/articles/iot-mqtt-why-good-for-iot/. Acesso em: 7 out. 2020.
15. COPE, Stephen. **SSL and SSL Certificates Explained For Beginners**. [*S. l.*], 17 mar. 2020. Disponível em: http://www.steves-internet-guide.com/ssl-certificates-explained/. Acesso em: 1 nov. 2020.