Controle de Acesso por Proximidade com ESP32 e BLE: Validação Local e Interface Web de Gerenciamento

Luiz Felipe Lazarotto Pires[1], Fernando de Cristo[2]

[1]Instituto Federal de Educação – Ciência e Tecnologia Farroupilha (iFFar)
Campus Frederico Westphalen – RS – Brasil

luiz.2022007899@aluno.iffar.edu.br,
fernando.cristo@iffarroupilha.edu.br

Abstract. *This article presents and evaluates a proximity-based access control system that uses a BLE scanner to identify beacons transmitted by smartphones and unlock an electronic door through local validation. The objective of the study was to develop and demonstrate the feasibility of an autonomous, low-cost, and locally operated solution capable of managing authorized tokens and recording events through an integrated web interface. Tests were conducted involving BLE signal detection, identifier validation, and relay activation, along with the analysis of complementary metrics such as signal strength (RSSI), response latency, and hit rate. The results demonstrate operational stability and suitability of the system for residential and small business scenarios, reinforcing its potential as a simple, secure, and service-independent alternative.*

Resumo. *Este artigo apresenta e avalia um sistema de controle de acesso por proximidade que utiliza um scanner BLE para identificar beacons emitidos por smartphones e liberar uma fechadura eletrônica mediante validação local. O objetivo do estudo foi desenvolver e demonstrar a viabilidade de uma solução autônoma, de baixo custo e operante em rede local, capaz de gerenciar tokens autorizados e registrar eventos por meio de uma interface web integrada. Foram realizados testes envolvendo detecção dos sinais BLE, validação de identificadores, acionamento do relé, além da análise de métricas complementares, como intensidade do sinal (RSSI), latência de resposta e taxa de acertos. Os resultados obtidos evidenciam estabilidade operacional e adequação do sistema para aplicações residenciais e de pequenas empresas, reforçando seu potencial como alternativa simples, segura e independente de serviços externos.*

Palavras-chave: Bluetooth Low Energy; autenticação por proximidade; beacons; controle de acesso; IoT.
Keywords: Bluetooth Low Energy; proximity authentication; beacons; access control; IoT.

1. Introdução

O controle de acesso físico é um tema cada vez mais relevante no contexto atual, impulsionado pela disseminação de tecnologias da Internet das Coisas (IoT) e pela necessidade de soluções práticas e seguras em residências, empresas e instituições. Métodos tradicionais como chaves, senhas ou cartões ainda são amplamente utilizados, porém apresentam limitações relacionadas à praticidade, e custos de manutenção. Nesse

cenário, a autenticação por proximidade, baseada em sinais digitais emitidos por dispositivos móveis, surge como alternativa viável e moderna para o gerenciamento de entradas e saídas em ambientes físicos.

A proposta deste trabalho consiste no desenvolvimento de um sistema de controle de acesso por proximidade utilizando o microcontrolador ESP32 como scanner Bluetooth Low Energy (BLE). O sistema identifica sinais emitidos por smartphones configurados como beacons, por meio de aplicativos de terceiros, e mediante validação em uma base de dados local, libera ou bloqueia uma fechadura eletrônica. Além do mecanismo de autenticação, foi implementada uma interface web local para o cadastro e gerenciamento de tokens, permitindo também a visualização de estatísticas de acesso. Essa integração entre hardware embarcado e sistema web busca garantir maior autonomia, simplicidade de uso e segurança na validação, sem depender de serviços externos.

O objetivo central é oferecer uma solução de baixo custo, robusta e acessível para diferentes contextos de aplicação, desde ambientes residenciais até pequenos empreendimentos. A arquitetura proposta demonstra como tecnologias embarcadas, aliadas a recursos de conectividade, podem ser aplicadas de forma eficiente no controle de acesso físico. Os testes realizados comprovam a viabilidade técnica da solução e apontam possibilidades de aprimoramento, como integração com sistemas em nuvem, uso de criptografia avançada e expansão das funcionalidades da interface web.

2. Referencial Teórico

Entre as diversas aplicações da Internet das Coisas (IoT), o controle de acesso por proximidade destaca-se com avanços recentes da área. Tecnologias sem fio como RFID e Bluetooth Low Energy (BLE) possibilitam autenticação rápida e segura sem a necessidade de contato físico, substituindo métodos tradicionais baseados em chaves, cartões ou senhas. Entre essas tecnologias, o BLE se destaca por seu baixo consumo de energia, disponibilidade em smartphones modernos e simplicidade de implementação.

O Bluetooth Low Energy é uma variante do padrão Bluetooth voltada para comunicação de curto alcance e baixo consumo (Bluetooth SIG, 2023). Amplamente utilizada em dispositivos móveis e sensores. Embora não seja uma prática consolidada, a utilização de beacons em controle de acesso, pode ser considerada uma alternativa viável, permitindo que identificadores digitais, compostos por um UUID e valores complementares denominados *major* e *minor*, sejam tratados como chaves de autenticação, possibilitando a validação de usuários autorizados de forma prática e confiável.

O microcontrolador *ESP32 DevKit* combina conectividade Wi-Fi e BLE, (ESPRESSIF SYSTEMS, 2023), em um único chip, além de recursos de processamento adequados à aplicação proposta. Seu suporte nativo a BLE permite atuar como scanner, capturando e processando sinais de dispositivos móveis em tempo real. Dispõe ainda de pinos de entrada e saída para acionamento de mecanismos físicos, como relés ou solenoides, o que o torna apropriado para sistemas de controle de acesso. Outro recurso relevante é o *SPIFFS*, sistema de arquivos interno que armazena dados na memória flash, garantindo funcionamento mesmo sem rede. A sincronização de data e hora é feita pelo

protocolo NTP *MILLS, D. L. Network Time Protocol (NTP). RFC 5905, IETF, 2010.* Assegurando precisão nos registros de acesso.

Para que o microcontrolador se comunique com o ambiente de gerenciamento, foi implementada uma *API* desenvolvida em FastAPI (RAMIREZ, 2018), que disponibiliza endpoints para cadastro, consulta e exclusão de tokens, além de recepção de registros de acesso. No processo de autenticação, considera-se também a intensidade do sinal recebido, *RSSI* ***(****Received Signal Strength Indicator****),*** utilizada como parâmetro de proximidade, a fim de evitar a validação de dispositivos localizados além do limite estabelecido.

Diversos trabalhos acadêmicos exploram soluções de autenticação por proximidade. Morais (2015) apresentou um sistema de controle de acesso baseado em RFID e Arduino, demonstrando a viabilidade do uso de identificação sem contato em ambientes acadêmicos. Roriz e Rodrigues (2018) implementaram controle veicular em vagas especiais com RFID, reforçando o potencial da automação para inclusão e acessibilidade. Mais recentemente, Alves e Corrêa (2022) utilizaram ESP32 em um protótipo de automação de laboratórios, validando o uso do microcontrolador em cenários reais de controle de acesso. Essas iniciativas demonstram a consolidação da autenticação sem fio como alternativa aos métodos tradicionais e fundamentam a proposta deste trabalho.

Com base nesses conceitos, este estudo explora a integração entre BLE, ESP32 e interface web local, propondo um sistema capaz de validar beacons emitidos por smartphones, liberar acessos físicos e registrar eventos em banco de dados. Essa abordagem alia baixo custo, com simplicidade de uso e robustez, demonstrando-se como uma solução viável para residências e pequenas empresas.

3. Metodologia

A metodologia adotada neste trabalho é de natureza aplicada e experimental, tendo como foco o desenvolvimento e vali**d**ação de um protótipo funcional de controle de acesso por proximidade. O sistema foi estruturado de forma modular, integrando hardware embarcado, comunicação sem fio por Bluetooth Low Energy (BLE), um servidor local em FastAPI com banco de dados e uma interface web para cadastro e gerenciamento de tokens.

3.1. Arquitetura Geral do Sistema

A arquitetura do sistema é formada por quatro elementos principais que operam de maneira integrada. O *smartphone* atua como chave de acesso, emitindo sinais de beacon via BLE por meio de aplicativos de terceiros. O *microcontrolador ESP32* realiza a varredura contínua desses sinais, verifica os tokens recebidos e aciona o relé conectado à fechadura eletrônica. O *servidor FastAPI*, integrado a um banco de dados SQLite (HIPP, 2023), mantém a lista de identificadores válidos e registra todos os eventos de acesso. Por fim, a *interface web* possibilita ao administrador cadastrar, editar e remover dispositivos autorizados, além de consultar os registros, centralizando a gestão e o monitoramento do sistema.

3.2. Fluxo de Funcionamento

O funcionamento do sistema inicia com a emissão de beacons pelos dispositivos móveis autorizados, que são detectados continuamente pelo ESP32. A cada detecção, o identificador extraído é comparado com a lista de tokens previamente carregada, validando se o dispositivo possui permissão de acesso. Quando a validação é positiva e a intensidade do sinal atende ao valor configurado, o microcontrolador aciona o relé, liberando a fechadura eletrônica de forma imediata. Em paralelo, cada evento de acesso é registrado e posteriormente exibido na interface web, permitindo ao administrador acompanhar os acessos de maneira centralizada. A Figura 1 apresenta o fluxograma desse processo, descrevendo as etapas executadas pelo ESP32 desde sua inicialização até a validação dos tokens e o registro dos acessos.

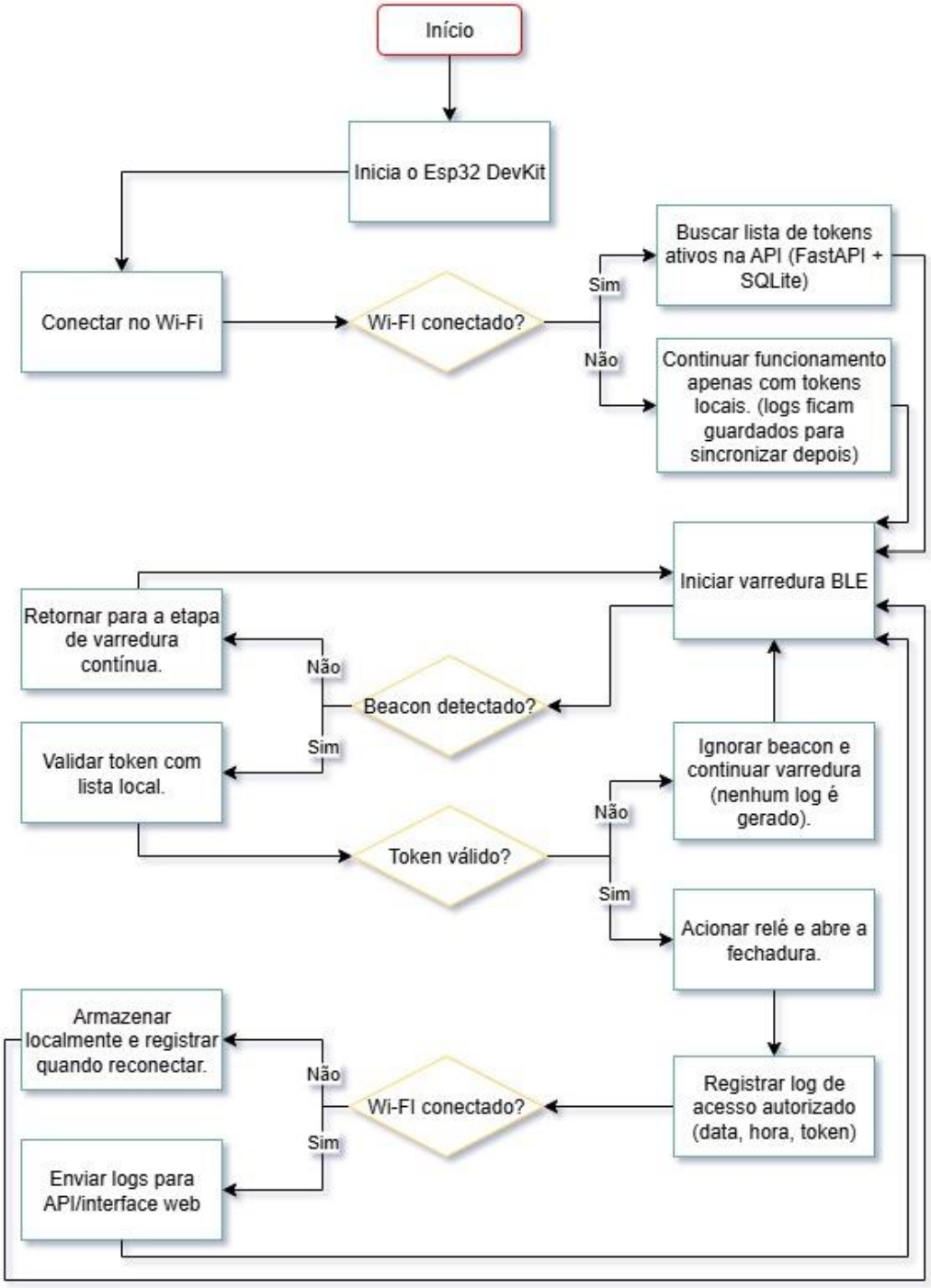


Figura 1. Diagrama do sistema.

3.3. Desenvolvimento do Protótipo

3.3.1. Hardware

O protótipo (Figura 2) foi desenvolvido utilizando o módulo ESP32-Wroom-32, escolhido por integrar conectividade Wi-Fi e BLE, além de oferecer recursos de processamento adequados. Para o acionamento físico da fechadura foi utilizado um

módulo relé, SRD-05VDC-SL-C, responsável por liberar ou bloquear a passagem de corrente elétrica para a fechadura eletrônica.

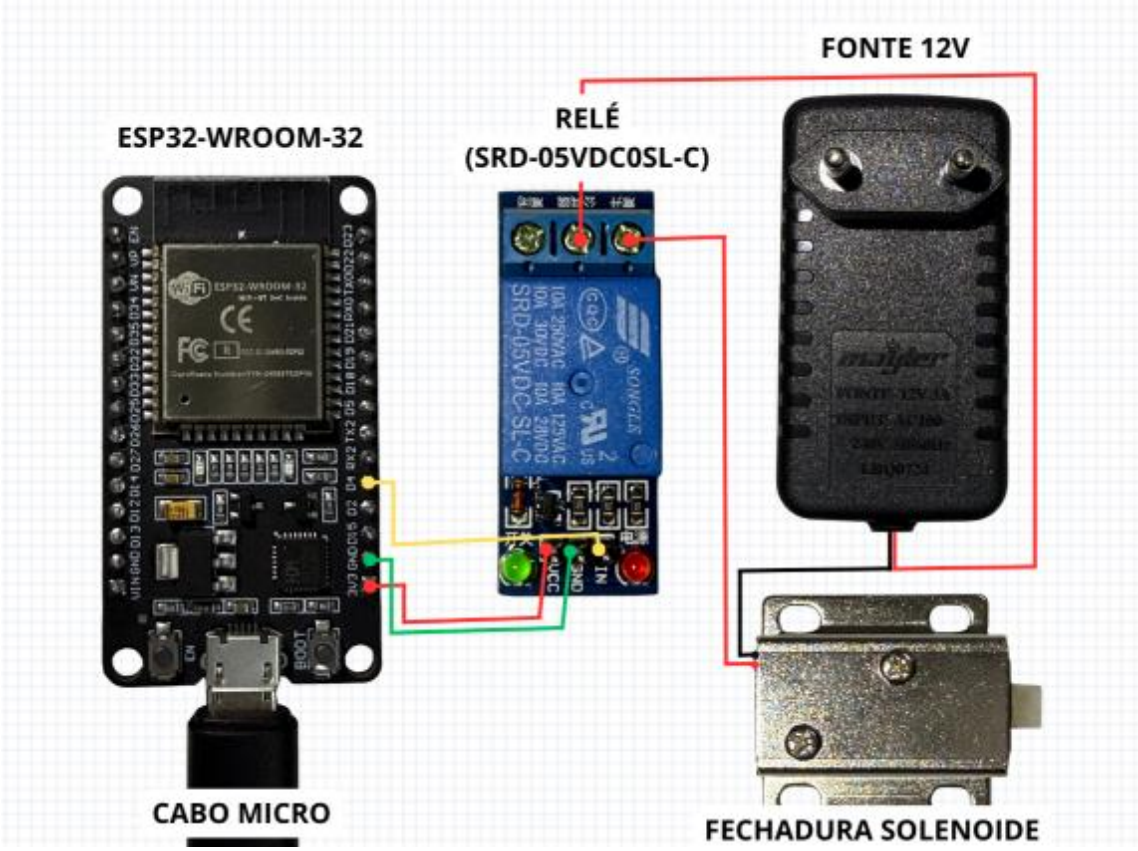


Figura 2. Esquema elétrico do protótipo.

A montagem inicial do protótipo foi feita em protoboard, utilizando jumpers e fontes de alimentação estáveis, configuração adequada para a fase de prototipagem. Na versão final, entretanto, as conexões passaram a ser realizadas de forma direta entre os componentes, eliminando o uso da protoboard. Essa adaptação proporcionou maior confiabilidade e menor risco de falhas por mau contato, com os elementos sendo acomodados em um gabinete, garantindo organização do circuito e segurança na utilização.

3.3.2. Software embarcado

O código embarcado (Figura 3) foi desenvolvido em C++ utilizando a plataforma Arduino IDE (ARDUINO, 2023). Sua lógica foi estruturada em etapas bem definidas: configuração inicial, seguida pelos módulos de varredura BLE, validação de tokens, acionamento do relé e persistência de dados e registros de acesso.

Na fase de inicialização, o ESP32 prepara o ambiente para execução do sistema configurando o pino responsável pelo acionamento do relé e garantindo que ele permaneça desligado no estado inicial, evitando ativações indesejadas. Em seguida, o

sistema de arquivos SPIFFS (PETERSON, 2015) é montado para permitir o armazenamento local de tokens e registros, enquanto o dispositivo se conecta à rede Wi-Fi utilizando as credenciais fornecidas, sincroniza data e hora via NTP e carrega tokens previamente salvos. Logo após, é realizada uma consulta à API para buscar a lista de tokens autorizados mais recente, que também é salva localmente, e o scanner BLE é configurado em modo contínuo com callbacks para análise de dispositivos próximos, além da definição dos marcadores de tempo que controlam as rotinas de reinício do scanner, atualização de tokens e envio de logs.

```
INÍCIO

Configurar pino do relé como saída
Garantir relé desligado no estado inicial
Iniciar SPIFFS (memória flash)
Conectar ao Wi-Fi (SSID, senha)
Sincronizar data/hora via NTP (UTC)
Carregar tokens salvos do SPIFFS
Consultar API → buscar tokens autorizados
Salvar tokens no SPIFFS
Configurar scanner BLE contínuo com callbacks
Marcar tempos de referência (scanner, tokens, logs)
```

Figura 3. Pseudocódigo – Módulo 1.

O segundo módulo (Figura 4) é responsável pela varredura contínua do ambiente em busca de anúncios Bluetooth Low Energy (BLE). O scanner do ESP32 foi configurado para identificar pacotes nos formatos iBeacon (Apple) e AltBeacon (Android), (APPLE, 2014; RADIUS NETWORKS, 2014). Extraindo automaticamente os parâmetros de identificação de cada anúncio, como UUID, major, minor e intensidade do sinal (RSSI). Esses dados são então encaminhados ao terceiro módulo, responsável pelo processo de validação dos tokens.

```
Iniciar scanner BLE em modo contínuo
Para cada anúncio recebido:
    Verificar se é iBeacon ou AltBeacon
    Extrair UUID, major, minor e RSSI
    Encaminhar dados para processo de validação
```

Figura 4. Pseudocódigo – Módulo 2.

No terceiro módulo (Figura 5), os dados extraídos dos anúncios BLE (UUID, major, minor) e RSSI são processados para formar uma chave única no formato uuid-major-minor. Essa chave é comparada com a lista de tokens autorizados previamente carregada no dispositivo. Caso exista correspondência e a intensidade do sinal recebido (RSSI) esteja acima do limiar definido (−55 dBm), o token é considerado válido e o fluxo é direcionado para o módulo seguinte, responsável pelo acionamento do relé. Se não houver correspondência ou o sinal estiver abaixo do limite, o anúncio é descartado.

```
Montar chave = UUID-MAJOR-MINOR
SE chave está na lista de tokens autorizados E RSSI ≥ -55 dBm:
    Considerar token válido
    Encaminhar para módulo do relé
SENÃO:
    Descartar anúncio
```

Figura 5. Pseudocódigo – Módulo 3.

O quarto módulo (Figura 6) controla o relé, que atua como interruptor eletrônico da fechadura. Quando um token válido é identificado, o ESP32 aciona o pino digital configurado, liberando a passagem de corrente para destravar a fechadura. Esse acionamento ocorre de forma imediata e permanece ativo apenas enquanto houver um dispositivo autorizado dentro do alcance configurado. Caso nenhum token válido seja detectado após o tempo limite estabelecido, o relé é desativado automaticamente, garantindo que a fechadura retorne ao estado de segurança.

```
SE token válido detectado:
    Acionar relé (abrir fechadura)
    Manter estado ativo enquanto houver detecção
SE tempo limite sem token válido:
    Desativar relé (fechar fechadura)
```

Figura 6. Pseudocódigo – Módulo 4.

O quinto módulo (Figura 7) registra e armazena os eventos de acesso, garantindo rastreabilidade mesmo em situações de instabilidade de rede. A cada detecção validada, o ESP32 gera um log em formato JSON contendo o identificador do dispositivo, intensidade do sinal e timestamp obtido via NTP. Esses registros são gravados no sistema de arquivos SPIFFS e, periodicamente, o dispositivo tenta enviá-los à API. Quando a conexão com a rede está disponível, os logs são transmitidos e removidos da memória local. Caso contrário, permanecem armazenados até que a conectividade seja restabelecida, evitando perda de informações e assegurando a integridade do histórico de acessos.

```
SE token válido detectado:
    Criar log JSON (UUID, RSSI, timestamp)
    Salvar log no SPIFFS

A cada intervalo definido:
    SE Wi-Fi conectado:
        Carregar logs do SPIFFS
        Enviar logs para API
        SE envio bem-sucedido:
            Remover logs enviados da memória local
    SENÃO:
        Manter logs armazenados no SPIFFS

FIM
```

Figura 7. Pseudocódigo – Módulo 5.

A organização do software embarcado em módulos, aliada à representação em pseudocódigo, evidencia que o sistema não se limita a um simples acionamento de relé. O ESP32 integra diferentes camadas funcionais: comunicação com a API, varredura BLE, validação de tokens, controle físico e persistência de dados. Que operam de maneira coordenada para assegurar segurança, confiabilidade e resiliência. Essa representação modular favorece a compreensão do fluxo de execução e evidencia a complexidade da solução desenvolvida, reforçando tanto seu caráter acadêmico quanto sua viabilidade prática em aplicações de controle de acesso.

3.3.3. Interface Web

A interface web foi desenvolvida com o propósito de fornecer ao administrador uma ferramenta simples e intuitiva para gerenciar os acessos ao sistema. Essa camada complementa diretamente o software embarcado, permitindo que as credenciais de usuários sejam cadastradas, editadas ou removidas sem a necessidade de reprogramação do ESP32, tornando a operação mais prática e acessível mesmo para usuários sem conhecimento técnico avançado.

Além disso, visando a utilização da solução em um contexto comercial, implementou-se um modelo de multiusuários estruturalmente baseado no isolamento lógico de dados. Essa abordagem garante que cada cliente autenticado tenha acesso exclusivo aos seus próprios tokens, registros de acesso e estatísticas, impedindo que informações de diferentes instalações sejam misturadas. Com isso, o sistema se torna seguro, escalável e adequado para cenários em que diversas unidades ou contratantes compartilham a mesma infraestrutura de servidor, mantendo a privacidade e a integridade das informações de forma rigorosa.

O backend foi implementado em *Python*, utilizando o framework *FastAPI* para expor os endpoints de cadastro, consulta e exclusão de tokens, além de registrar os acessos recebidos. A aplicação é executada por meio do servidor *Uvicorn (ENCODE, 2018)*, que possibilita processamento assíncrono e eficiente. Já o frontend foi construído em *HTML*, *CSS* e *JavaScript*, oferecendo uma interface clara e de fácil utilização. Esse servidor está integrado a um banco de dados *SQLite*, responsável por armazenar de forma segura tanto os identificadores autorizados quanto os registros de uso do sistema.

A primeira tela (Figura 8) apresentada ao usuário é a página de login, responsável por autenticar o cliente no sistema e garantir que apenas instalações autorizadas tenham acesso ao painel de gerenciamento. Nessa etapa, cada cliente utiliza suas próprias credenciais, o que permite isolar completamente os dados de diferentes usuários mesmo quando compartilham a mesma infraestrutura de servidor. A interface foi projetada de forma simples e funcional, exibindo apenas os campos essenciais para autenticação. Após o login, o cliente é redirecionado automaticamente ao painel correspondente à sua instalação, assegurando uma experiência intuitiva e segura.

Figura 8. Página de login do sistema.

A tela principal (Figura 9) foi projetada para simplificar o processo de administração dos dispositivos autorizados, oferecendo ao administrador um painel intuitivo para cadastro e gerenciamento de tokens. Nela é possível registrar novos identificadores, ativar ou desativar dispositivos já cadastrados e excluir registros quando necessário, garantindo flexibilidade na gestão. A Figura 3 apresenta a tela inicial da interface, na qual essas funcionalidades são disponibilizadas de forma clara e organizada.

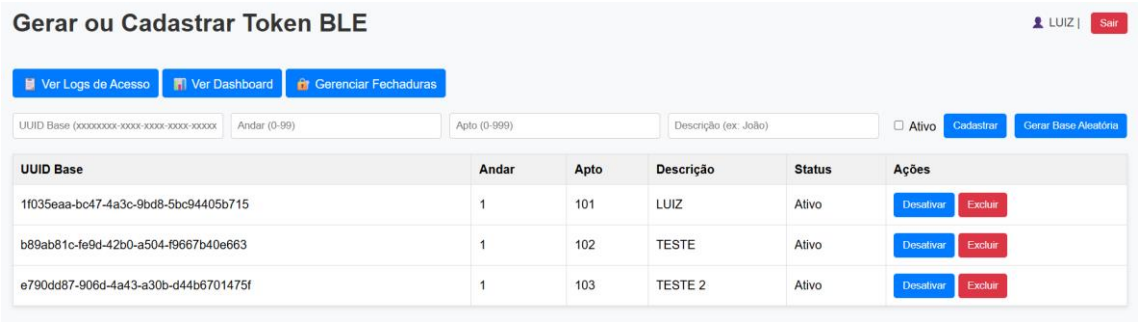
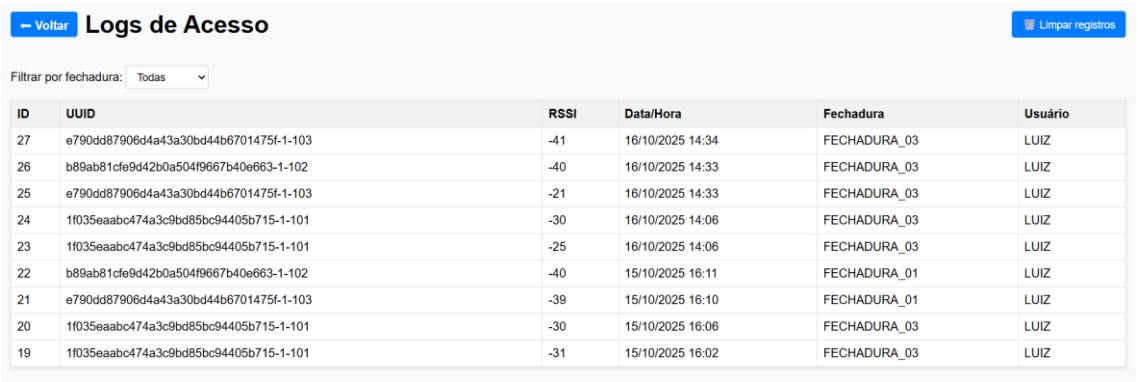


Figura 9. Página inicial do sistema.

Além do gerenciamento de credenciais, a interface web conta com uma seção dedicada à visualização dos logs de acesso, (Figura 10). Nessa área são listados em formato de tabela os dispositivos detectados, juntamente com o identificador utilizado, a intensidade do sinal recebido (RSSI) e a data e hora do evento. Essa funcionalidade proporciona rastreabilidade e permite ao administrador acompanhar o funcionamento do sistema, analisando o histórico de entradas e a intensidade do sinal captado durante cada tentativa de acesso. Como recurso adicional, foi implementado um botão que possibilita limpar os

registros armazenados, permitindo reiniciar o monitoramento de forma prática sempre que necessário.



ID	UUID	RSSI	Data/Hora	Fechadura	Usuário
27	e790dd87906d4a43a30bd44b6701475f-1-103	-41	16/10/2025 14:34	FECHADURA_03	LUIZ
26	b89ab81cfe9d42b0a504f9667b40e663-1-102	-40	16/10/2025 14:33	FECHADURA_03	LUIZ
25	e790dd87906d4a43a30bd44b6701475f-1-103	-21	16/10/2025 14:33	FECHADURA_03	LUIZ
24	1f035eaabc474a3c9bd85bc94405b715-1-101	-30	16/10/2025 14:06	FECHADURA_03	LUIZ
23	1f035eaabc474a3c9bd85bc94405b715-1-101	-25	16/10/2025 14:06	FECHADURA_03	LUIZ
22	b89ab81cfe9d42b0a504f9667b40e663-1-102	-40	15/10/2025 16:11	FECHADURA_01	LUIZ
21	e790dd87906d4a43a30bd44b6701475f-1-103	-39	15/10/2025 16:10	FECHADURA_01	LUIZ
20	1f035eaabc474a3c9bd85bc94405b715-1-101	-30	15/10/2025 16:06	FECHADURA_03	LUIZ
19	1f035eaabc474a3c9bd85bc94405b715-1-101	-31	15/10/2025 16:02	FECHADURA_03	LUIZ

Figura 10. Página de logs de acesso do sistema.

Para clientes que administram mais de um ponto de acesso, a interface web inclui uma página dedicada à visualização e seleção dos dispositivos vinculados à sua conta, (Figura 11). Cada dispositivo representa uma fechadura ou unidade independente, e somente os dispositivos pertencentes ao cliente autenticado são exibidos, preservando o isolamento das informações. Nessa tela, o administrador pode selecionar qual dispositivo deseja gerenciar e, a partir dessa escolha, acessar as listas de tokens permitidos, os logs de acesso e as estatísticas correspondentes àquela instalação específica.

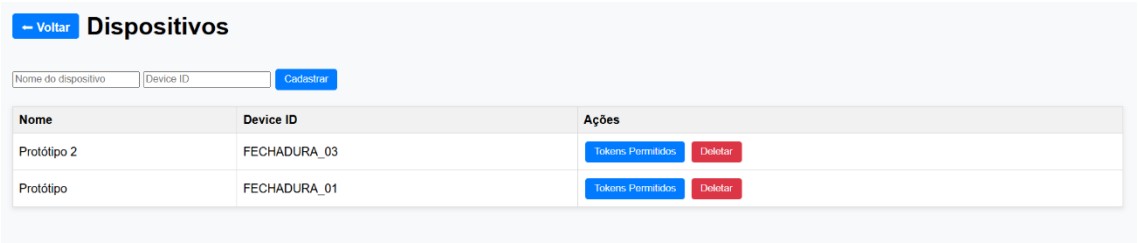


Figura 11. Página de dispositivos do sistema.

Após selecionar um dispositivo, o administrador é encaminhado para a tela de gerenciamento de tokens específicos daquela unidade, (Figura 12). Essa seção permite visualizar todos os identificadores autorizados a realizar acesso, além de cadastrar novos tokens, editar permissões existentes ou remover credenciais que não devem mais ser aceitas. Essa divisão por dispositivo garante precisão na gestão, principalmente em cenários onde um mesmo cliente possui múltiplas fechaduras ou pontos de entrada. Ao manter listas independentes para cada instalação, o sistema assegura que permissões não sejam compartilhadas de forma indevida entre diferentes dispositivos. A Figura 12 apresenta a página de gerenciamento de tokens autorizados.

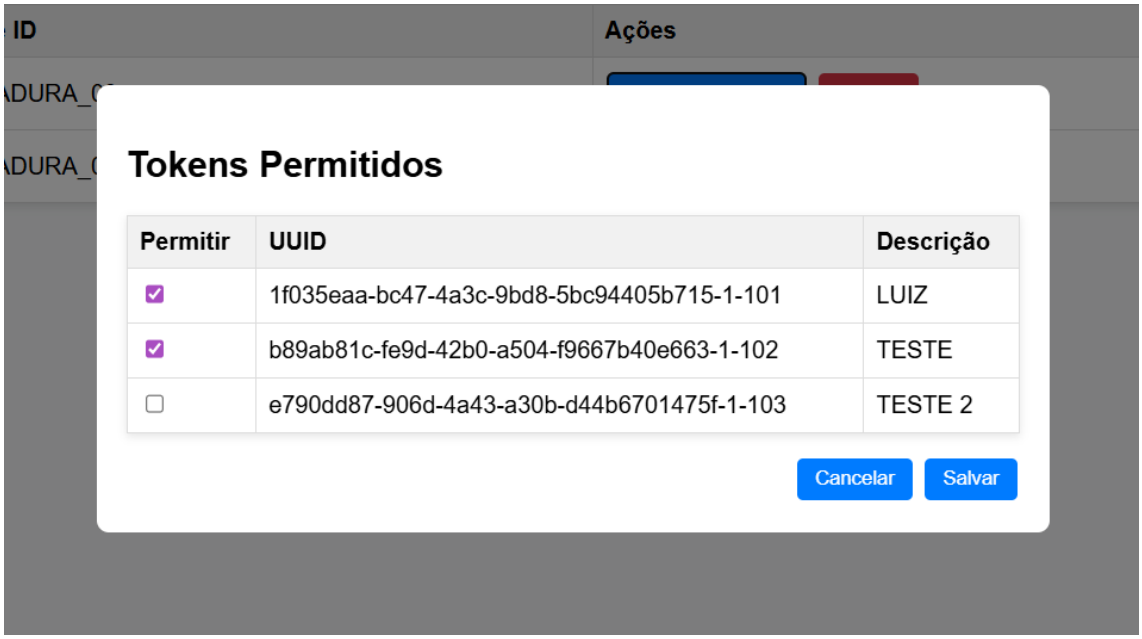


Figura 12. Página de dispositivos do sistema.

Além do gerenciamento de credenciais e da visualização dos registros de acesso, a interface web disponibiliza uma seção dedicada às estatísticas do sistema. Nessa área, o administrador pode verificar o total de acessos, o último registro realizado, a média diária e o andar mais utilizado. Os gráficos complementam essas informações ao apresentar a distribuição de acessos por dia, hora, andar e por token. Esses recursos oferecem uma visão mais ampla do funcionamento do sistema e auxiliam na identificação de padrões de uso, contribuindo para análises mais detalhadas do comportamento dos usuários. A Figura 13 apresenta a página de estatísticas da interface, na qual essas informações são exibidas de forma clara e acessível.

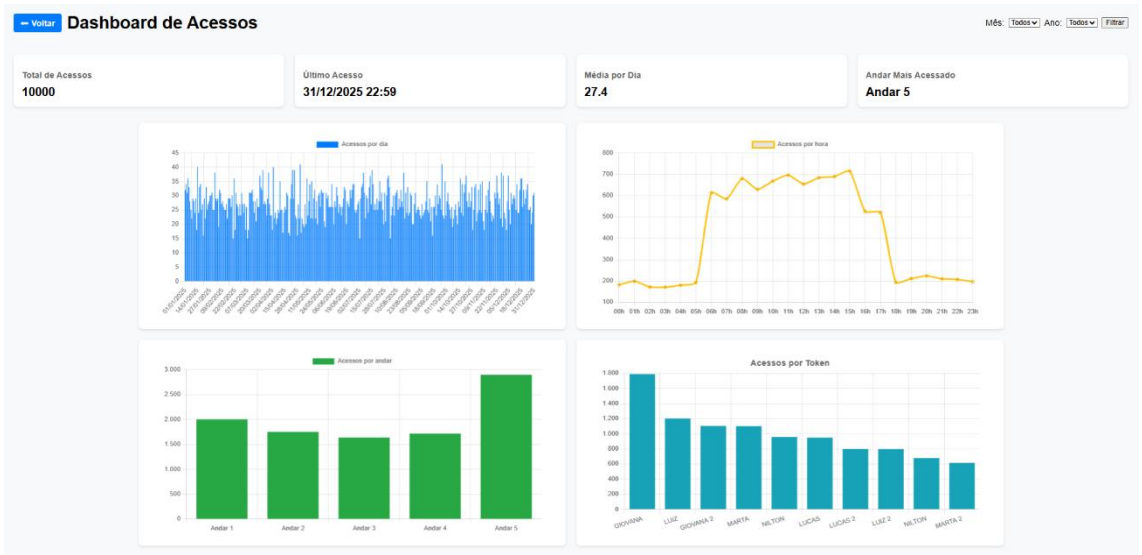


Figura 13. Página de logs de acesso do sistema.

De maneira geral, a interface web atua como elo entre o administrador e o sistema embarcado, centralizando o gerenciamento de credenciais e a supervisão de acessos em um ambiente de fácil utilização. Essa integração contribui para a usabilidade e robustez da solução proposta, consolidando sua aplicabilidade em cenários reais de controle de acesso.

3.4. Procedimentos de Teste

A validação do protótipo foi conduzida em um ambiente real de utilização, instalado em uma porta residencial, com o objetivo de simular condições práticas de operação. Para a emissão dos sinais BLE, foram utilizados os aplicativos Beacon Simulator – Agile 4 (em dispositivos Android) e Locate Beacon (em dispositivos iOS), configurados para reproduzir pacotes nos padrões AltBeacon e iBeacon, respectivamente.

Os testes foram realizados utilizando diferentes marcas e modelos de smartphones, possibilitados pelo ambiente profissional do autor. Foram avaliados os seguintes dispositivos:

- **Samsung**: Galaxy A12, Galaxy A13, Galaxy A14, Galaxy A05, Galaxy S21 Fe, Galaxy S20 Plus
- **Motorola**: Moto E20, Moto E22, Moto G8, Moto G14
- **Apple (iOS)**: iPhone 11, iPhone 12, iPhone 13, iPhone 13 Pro Max, iPhone 14, iPhone 14 Pro Max, iPhone 15, iPhone 15 Pro Max, iPhone 16 Pro Max

A partir desses equipamentos, foram executados os seguintes procedimentos de teste:

- Detecção e identificação de dispositivos autorizados;
- Execução de testes nos padrões AltBeacon (Android) e iBeacon (iOS);
- Avaliação da distância máxima segura de leitura, com base nos valores de RSSI captados;
- Simulação de tentativas de acesso não autorizado, a fim de verificar a confiabilidade da validação;
- Medição do tempo médio de resposta entre a detecção do beacon e o acionamento do relé.

Durante os testes, também foram avaliadas as características operacionais dos protocolos BLE utilizados. O iBeacon, desenvolvido pela Apple, apresentou desempenho consistente nos modelos de iPhone, enquanto o AltBeacon, por ser um protocolo aberto, demonstrou ampla compatibilidade com dispositivos Android. A adoção simultânea de ambos os padrões garantiu que o sistema funcionasse de forma estável e previsível nas duas principais plataformas móveis disponíveis no mercado.

A diversidade de dispositivos empregados permitiu verificar o comportamento do sistema em cenários variados, analisando desempenho, responsividade e robustez frente a diferentes fabricantes e versões de hardware. Esses resultados fornecem evidências concretas da eficácia e da aplicabilidade do protótipo em situações reais de controle de acesso.

5. Resultados e Discussão

Os resultados obtidos com o protótipo demonstraram o pleno funcionamento da solução proposta, sem ocorrência de falhas durante os testes realizados. O ESP32 apresentou desempenho consistente na detecção de beacons, validando corretamente os dispositivos autorizados e negandoa acesso a não cadastrados. O acionamento do relé foi imediato, garantindo a liberação da fechadura em menos de um segundo após a validação.

A Tabela 1 apresenta os principais indicadores coletados durante os testes. Observa-se que a taxa de acerto foi de 100%, reforçando a confiabilidade do sistema.

Métrica	Resultado	Observação
Tempo médio de resposta Android	$\leq 3\,s$	Abertura muito rápida
Tempo médio de resposta iPhone	$\leq 4\,s$	Abertura rápida
Compatibilidade Android (AltBeacon)	Ótima	Detecção rápida e estável
Compatibilidade iPhone (iBeacon)	Boa	Detecção boa e estável
Taxa de acerto	100%	Nenhuma falha observada
Distância de leitura	Até 10 cm	RSSI permitido até este limite

Tabela 1. Indicadores de desempenho do sistema

Nos testes comparativos entre dispositivos, verificou-se que em smartphones Android, utilizando o aplicativo *Beacon Simulator – Agile 4*, a detecção ocorreu de forma estável e praticamente instantânea. A leitura mais demorada registrada foi de 3 segundos, mas, na maioria dos casos, a resposta foi imediata, sem falhas de autenticação.

Já em dispositivos iOS, o protocolo iBeacon apresentou funcionamento igualmente estável, sem registros de instabilidade, apenas com uma diferença ocasional no tempo de resposta em relação ao Android. Em média, os iPhones apresentaram um tempo até 1 segundo superior ao observado nos testes com Android, ainda dentro de limites aceitáveis para a aplicação.

A interface web implementada também se mostrou eficiente no gerenciamento do sistema. As funcionalidades de cadastro, exclusão e geração de tokens funcionaram sem inconsistências, e os logs de acesso foram registrados corretamente.

De forma geral, o protótipo atendeu às expectativas, demonstrando viabilidade técnica, baixo custo de implementação e aplicabilidade em ambientes residenciais e empresariais de pequeno porte. A operação em rede local, sem dependência de serviços externos, reforça a autonomia e a segurança do sistema, tornando-o competitivo frente a soluções tradicionais de controle de acesso.

5.1 Análise de Segurança e Limitações da Solução

Embora o sistema desenvolvido tenha apresentado funcionamento estável e confiável durante os testes realizados, é fundamental discutir seus limites de segurança e as implicações do uso da tecnologia Bluetooth Low Energy (BLE) como mecanismo de autenticação por proximidade. Essa análise é particularmente relevante para

contextualizar a solução proposta dentro de um modelo de ameaça compatível com seu escopo de aplicação.

A solução foi projetada para ambientes de baixo a médio risco, como residências e pequenos empreendimentos, operando inteiramente em rede local. Tanto o módulo embarcado quanto a interface web de gerenciamento são executados em infraestrutura local, sem exposição direta à internet, o que reduz significativamente a superfície de ataque e elimina riscos associados a serviços externos ou comunicação em nuvem.

No processo de autenticação, o sistema utiliza uma whitelist rígida de tokens previamente cadastrados, associada à validação local no ESP32. Apenas beacons emitidos em formatos específicos (iBeacon e AltBeacon) são processados, sendo automaticamente descartados anúncios que não atendam ao padrão esperado. Além disso, o uso do RSSI não é tratado como critério único de autenticação, mas como um filtro auxiliar de proximidade física. Mesmo que um token válido esteja presente na whitelist, o acesso somente é liberado se a intensidade do sinal recebido estiver acima do limiar configurado, garantindo que o dispositivo autorizado esteja dentro da distância considerada segura.

A confiabilidade do RSSI como métrica absoluta de proximidade pode ser limitada, uma vez que fatores como obstáculos físicos e interferências no sinal, podem influenciar sua variação. Nos testes realizados, não foram observadas variações significativas entre diferentes modelos de smartphones. Em cenários onde a leitura atravessou obstáculos, o ajuste conservador do limiar de RSSI mostrou-se suficiente para manter o comportamento esperado do sistema.

Em relação a falhas conhecidas associadas ao uso de BLE, como spoofing e replay attacks, é importante destacar que, embora teoricamente possíveis, tais ataques apresentam baixa viabilidade prática no contexto da aplicação proposta. O spoofing exigiria o conhecimento prévio dos identificadores autorizados, cuja disseminação depende diretamente do usuário legítimo. Já ataques de replay são dificultados pelo curto alcance do BLE, pela necessidade de proximidade física extrema e pela emissão contínua dos beacons. Adicionalmente, a validação local e em tempo real impede qualquer liberação que não corresponda exatamente a um token previamente autorizado.

Quanto à interferência eletromagnética, os testes foram conduzidos tanto em ambientes residenciais quanto em locais com múltiplos dispositivos BLE e Wi-Fi ativos. Nessas condições, não foram observados atrasos perceptíveis, perdas de leitura ou comportamentos instáveis, tampouco ocorrências de abertura indevida da fechadura. Em todos os cenários testados, o sistema apresentou comportamento consistente, validando apenas dispositivos presentes na whitelist.

Como exemplo de soluções comerciais disponíveis no mercado brasileiro, destacam-se módulos de controle de acesso por Bluetooth Low Energy, como o Controlador KeyPass BLE Relay 110 Khomp – Intelbras, que possibilita o acionamento de travas e portões por meio de BLE, utilizando relé para integração com fechaduras eletrônicas. Esses dispositivos são comercializados como hardware adicional e proprietário, projetados para integração com fechaduras e sistemas pertencentes ao mesmo ecossistema do fabricante. Essa abordagem implica custo adicional relacionado

não apenas à aquisição do módulo controlador, mas também à necessidade de utilização de fechaduras compatíveis e acessórios específicos, fazendo com que o custo total de implantação possa atingir facilmente a faixa de centenas de reais por ponto de acesso, sem considerar eventuais despesas com instalação e manutenção.

Embora a solução não tenha como objetivo substituir mecanismos de autenticação criptograficamente robustos ou sistemas corporativos de alta segurança, ela se apresenta como uma alternativa complementar, de baixo custo, simples de implementar e eficiente para o controle de acesso em cenários compatíveis com seu modelo de ameaça. Dessa forma, o sistema equilibra usabilidade, autonomia e segurança operacional, atendendo de maneira satisfatória às demandas do contexto para o qual foi projetado.

Como perspectiva de evolução da solução proposta, trabalhos futuros podem contemplar o desenvolvimento de um aplicativo móvel dedicado para a emissão e gerenciamento dos sinais BLE utilizados no processo de autenticação. A adoção de um aplicativo móvel dedicado permitiria maior controle sobre o ciclo de vida dos identificadores, além de possibilitar a implementação de funcionalidades adicionais, como gerenciamento de permissões, ativação temporária de acessos e integração direta com a interface web do sistema. Ressalta-se, contudo, que a ausência desse componente não compromete o funcionamento atual da solução, que se mostrou plenamente operacional utilizando aplicações de terceiros para emissão de beacons.

6. Considerações Finais

Os resultados obtidos neste trabalho evidenciam o potencial do sistema de controle de acesso por proximidade desenvolvido com base no microcontrolador ESP32 e na tecnologia Bluetooth Low Energy (BLE). A integração entre o módulo embarcado, responsável pela detecção de beacons e acionamento da fechadura eletrônica, e a interface web, destinada ao gerenciamento dos tokens e registros de acesso, demonstrou-se eficiente e funcional.

Durante os testes, o protótipo apresentou desempenho estável e confiável, sem registro de falhas na comunicação ou no acionamento do relé, validando corretamente os dispositivos autorizados. A arquitetura proposta destacou-se pela simplicidade, baixo custo e facilidade de implementação, características que a tornam adequada para aplicações residenciais e empresariais de pequeno porte.

De forma geral, os achados deste estudo confirmam a viabilidade e a eficiência da utilização do ESP32 e da tecnologia BLE no desenvolvimento de sistemas automatizados de controle de acesso, representando uma alternativa acessível, segura e de fácil adaptação a diferentes contextos.

7. Referências

ALVES, M. S.; CORRÊA, R. Desenvolvimento de um sistema de controle de acesso a salas por RFID com reservas via web. 2022. Trabalho de Conclusão de Curso (Engenharia de Controle e Automação) – Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, Campus Farroupilha, Farroupilha, 2022.
APPLE INC. Getting Started with iBeacon. Apple Developer Documentation, 2014.

ARDUINO. Arduino IDE Documentation. Arduino AG, 2023.
BLUETOOTH SIG. Bluetooth Core Specification Version 5.4. Bluetooth Special Interest Group, 2023.
ENCODE. Uvicorn: The lightning-fast ASGI server. 2018.
ESPRESSIF SYSTEMS. ESP32 Series Datasheet. Espressif Systems, 2023.
HIPP, D. R. SQLite Documentation. SQLite Consortium, 2023.
KONDO, M.; KAWAGUCHI, N. Bluetooth Low Energy Device Identification Technique Using Encrypted Beacons. IEEE Access, 2019.
MILLS, D. L. Network Time Protocol (NTP). RFC 5905, IETF, 2010.
MORAIS DE OLIVEIRA, R. Sistema de controle de acesso ao mestrado em tecnologia da energia utilizando RFID. 2015. Trabalho de Conclusão de Curso (Engenharia de Computação) – Universidade de Pernambuco, Escola Politécnica de Pernambuco, Recife, 2015.
NTP – Network Time Protocol.
PETERSON, J. SPIFFS: SPI Flash File System. 2015.
RAMIREZ, S. FastAPI Documentation. 2018.
RADIUS NETWORKS. AltBeacon Specification. Radius Networks, 2014.
RORIZ, L. D.; RODRIGUES, T. S. Sistema de controle de acesso veicular à vaga especial utilizando tecnologia RFID. 2018. Trabalho de Conclusão de Curso (Engenharia Elétrica) – Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Campus Jataí, Jataí, 2018.