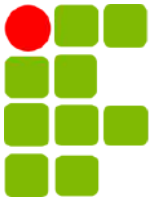


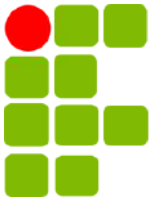
Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

Proposta de implementação de um Sistema de Monitoramento de Acesso Baseado em RFID no IFPB

João Vitor Nepomuceno Máximo

Orientador: Dr. Éwerton Rômulo Silva Castro

Campina Grande, Dezembro de 2025



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

Proposta de implementação de um Sistema de Monitoramento de Acesso Baseado em RFID no IFPB

João Vitor Nepomuceno Máximo

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Dr. Éwerton Rômulo Silva Castro

Campina Grande, Dezembro de 2025

Catalogação na fonte:
Ficha catalográfica

M564p Máximo, João Vitor Nepomuceno.
Proposta de implementação de um Sistema de Monitoramento de Acesso Baseado em RFID no IFPB / João Vitor Nepomuceno Máximo. - Campina Grande, 2025.
52f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2025.
Orientador: Prof. Dr .Éwerton Rômulo Silva Castro.

1. Telemática - Arquitetura de sistema. 2. RFID. 3. Gestão de espaços - Monitoramento de fluxo. 4. NFC. 5. ESP32. I. Castro, Éwerton Rômulo Silva (orient.). II Título.

CDU 621.396

Proposta de implementação de um Sistema de Monitoramento de Acesso Baseado em RFID no IFPB

João Vitor Nepomuceno Máximo

Dr. Éwerton Rômulo Silva Castro
Orientador

Msc. Iana Daya Cavalcante Facundo Passos
Membro da Banca

Dr. Anderson Fabiano Batista Ferreira da Costa
Membro da Banca

Campina Grande, Paraíba, Brasil
Dezembro/2025

Dedico esta conquista, antes de tudo, à minha mãe, Alba Rejane Nepomuceno, por seu incentivo incondicional e por acreditar em meu potencial desde o primeiro dia. Seu apoio foi a base para que eu chegasse até aqui.

"O que pode ser medido, pode ser gerenciado."
Peter Drucker

Agradecimentos

Gostaria de expressar minha profunda gratidão a todas as pessoas que, de alguma forma, contribuíram para a realização deste trabalho e para a minha jornada acadêmica.

Em primeiro lugar, agradeço imensamente à minha mãe, Alba Rejane Nepomuceno, por seu amor, incentivo incondicional e por sempre acreditar em meu potencial. Seu apoio foi a base fundamental para esta e todas as minhas conquistas.

Aos meus mestres, expresso meu sincero reconhecimento. Ao professor Marcelo Portela Sousa, por me inspirar a estudar mais e a almejar ir o mais longe possível. Ao meu orientador, professor Dr. Éwerton Rômulo Silva Castro, a quem agradeço não apenas por ser um ótimo professor e profissional, mas também pela orientação paciente e fundamental que tornou este projeto possível.

Por fim, não poderia deixar de agradecer aos meus amigos e verdadeiros companheiros de jornada, Adonias Alves Cardoso Junior e Joseffer Maxwel Oliveira das Merces, que sempre estiveram comigo, oferecendo apoio e amizade ao longo de todos estes anos de curso.

A todos, o meu muito obrigado.

Resumo

A gestão de espaços em instituições de ensino demanda soluções que otimizem o uso da infraestrutura e forneçam dados para o planejamento estratégico. Sistemas de monitoramento de fluxo manuais ou obsoletos mostram-se ineficientes e incapazes de gerar as informações necessárias para uma administração baseada em evidências. Este trabalho tem como objetivo geral propor e analisar a viabilidade de um sistema de monitoramento de passagem baseado nas tecnologias RFID (*Radio-Frequency IDentification* - Identificação por Radiofrequência) e NFC (*Near Field Communication* - Comunicação por Campo de Proximidade), com foco primário de aplicação na entrada do IFPB - Campus Campina Grande. A metodologia adotada foi a de uma pesquisa aplicada, de natureza exploratória e descritiva, fundamentada na revisão da literatura e na análise de componentes de *hardware* e *software*. O resultado principal é a proposta de duas arquiteturas técnicas distintas: um Protótipo A, de baixo custo, focado na viabilidade imediata com ESP32 e etiquetas MIFARE Classic para validar a estabilidade da coleta de dados; e um Protótipo B, de alta segurança, que utiliza etiquetas com criptografia AES para mitigar as vulnerabilidades conhecidas da primeira proposta. Ambas as arquiteturas são baseadas em *software* de código aberto e preveem uma aplicação *web* para gerenciamento. O trabalho conclui analisando comparativamente a viabilidade técnica, os custos e os desafios de segurança de cada proposta, demonstrando que a implementação é uma solução promissora para automatizar a coleta de dados de fluxo na instituição.

Palavras-chave: rfid; monitoramento de fluxo; nfc; arquitetura de sistema; gestão de espaços; esp32;

Abstract

The management of spaces in educational institutions requires solutions that optimize infrastructure use and provide data for strategic planning. Manual or obsolete flow monitoring systems are inefficient and unable to generate the necessary information for evidence-based administration. This work aims to propose and analyze the feasibility of a passage monitoring system based on RFID and NFC technologies, focusing primarily on the entrance of the IFPB Campus Campina Grande as its application. The methodology adopted was an applied, exploratory, and descriptive research, grounded in a literature review and an analysis of hardware and software components. The main result is the proposal of two distinct technical architectures: a low-cost Prototype A, focused on immediate feasibility using ESP32 and MIFARE Classic tags to validate data collection stability; and a high-security Prototype B, which uses tags with AES encryption to mitigate the known vulnerabilities of the first proposal. Both architectures are based on open-source software and include a web application for management. The work concludes by comparatively analyzing the technical feasibility, costs, and security challenges of each proposal, demonstrating that the implementation is a promising solution to automate flow data collection at the institution.

Keywords: rfid; flow monitoring; nfc; system architecture; space management; esp32;

Sumário

Lista de Siglas

AES	*Advanced Encryption Standard* (Padrão Avançado de Criptografia)
API	*Application Programming Interface* (Interface de Programação de Aplicações)
HTTPS	*Hypertext Transfer Protocol Secure* (Protocolo de Transferência de Hipertexto Seguro)
IDE	*Integrated Development Environment* (Ambiente de Desenvolvimento Integrado)
IFF	*Identity Friend or Foe* (Identificação de Amigo ou Inimigo)
IoT	*Internet of Things* (Internet das Coisas)
LGPD	Lei Geral de Proteção de Dados
LTS	*Long-Term Support* (Suporte de Longo Prazo)
MITM	*Man-In-The-Middle* (Atacante no Meio)
NDEF	*NFC Data Exchange Format* (Formato de Troca de Dados NFC)
NFC	*Near Field Communication* (Comunicação por Campo de Proximidade)
PII	*Personally Identifiable Information* (Informações Pessoalmente Identificáveis)
RFID	*Radio-Frequency IDentification* (Identificação por Radiofrequência)
SGBD	Sistema de Gerenciamento de Banco de Dados
SPI	*Serial Peripheral Interface* (Interface Periférica Serial)
SSL	*Secure Sockets Layer* (Camada de Soquetes Segura)
SUAP	Sistema Unificado de Administração Pública
TLS	*Transport Layer Security* (Segurança da Camada de Transporte)
UID	*Unique Identifier* (Identificador Único)

Lista de Figuras

Lista de Quadros e Tabelas

Capítulo 1

Introdução

A tecnologia de RFID (*Radio-Frequency IDentification* - Identificação por Radiofrequência), que serve de alicerce para o sistema proposto neste trabalho, possui um histórico de desenvolvimento que remonta a meados do século XX. Seus primórdios datam da década de 1940, quando, durante a Segunda Guerra Mundial, foi desenvolvida a tecnologia IFF (*Identity Friend or Foe* - Identificação de Amigo ou Inimigo) para distinguir aeronaves aliadas das inimigas por meio de um *transponder* (transpondedor) [Sartori 2020]. Após anos de evolução, a tecnologia transcendeu seu uso militar e passou a ser amplamente empregada em diversas áreas civis, como controle de acesso, sistemas de pagamento e rastreamento de itens [Sartori 2020].

Atualmente, instituições de ensino, como a que é objeto deste estudo, enfrentam desafios contínuos com sistemas de acesso manuais ou obsoletos, que frequentemente resultam em filas, atrasos e, mais criticamente, expõem alunos, servidores e o patrimônio institucional a riscos de segurança [Sartori 2020]. Diante deste cenário, a implementação de um sistema moderno para automatizar e agilizar o monitoramento do fluxo de pessoas surge como uma necessidade estratégica. Para isso, propõe-se o uso da tecnologia RFID e de sua evolução direta, a NFC (*Near Field Communication* - Comunicação por Campo de Proximidade). A tecnologia NFC, uma extensão da RFID que opera na frequência de 13,56 MHz, permite a troca de dados a curtas distâncias, facilitando interações naturais e intuitivas entre o mundo físico e os sistemas digitais [Thammarat 2020; Thanapal, Prabhu e Jakhar 2017; Firlej, Musial e Kubiak 2024; Lukito e Utami 2021].

1.1 Justificativa e Relevância do Trabalho

A gestão de espaços físicos em instituições de ensino de grande porte é um desafio complexo e contínuo. No IFPB-CG não é diferente e otimização da infraestrutura é fundamental para garantir a qualidade dos serviços e a segurança da comunidade acadêmica. Atualmente, a ausência de um sistema automatizado para monitorar o fluxo de pessoas e o acesso a ambientes críticos impõe barreiras para a tomada de decisões estratégicas baseadas em dados

concretos. Neste cenário, tecnologias de identificação automática, como a RFID e a NFC, surgem como soluções inovadoras [Thammarat 2020; Thanapal, Prabhu e Jakhar 2017; Firlej, Musial e Kubiak 2024; Lukito e Utami 2021].

A relevância deste trabalho se manifesta em dois pilares centrais para a instituição:

1. **Otimização da Gestão de Ambientes de Uso Coletivo:** A compreensão dos padrões de uso de áreas de grande circulação, como a entrada do campus, biblioteca, o refeitório, controle de chaves de salas e laboratórios é crucial para o planejamento de recursos. A implementação de um sistema de validação *Check-In/Check-Out* (Registo de entrada/Registro de saída) permite à gestão coletar dados precisos sobre horários de pico e tempo de permanência [Brumercikova e Bukova 2020]. Os dados de trajetória coletados podem, ainda, servir de base para um sistema de navegação interna que calcula e recalcula rotas ótimas para os usuários, ajudando a identificar e a mitigar pontos de congestionamento no campus [Ozdenizci, Coskun e Ok 2015], por exemplo no IFPB-CG.

2. **Fundamentação para Expansões e Investimentos Futuros:** Uma das maiores contribuições deste projeto é a capacidade de fornecer dados quantitativos para justificar futuras expansões. A análise do fluxo de pessoas permite criar "mapas de calor"que revelam áreas sobrecarregadas e subutilizadas, fornecendo uma base de evidências sólida para o planejamento estratégico e a aplicação eficiente de recursos. Contudo, a publicação de dados de trajetória, mesmo que anonimizada, apresenta riscos de privacidade. É crucial reconhecer que adversários com conhecimento parcial sobre a rotina de um indivíduo podem conseguir reidentificar sua trajetória completa [Terrovitis *et al.* 2017]. Portanto, a implementação de tal sistema deve ser acompanhada de uma rigorosa política de governança de dados, utilizando técnicas de supressão ou divisão de trajetórias para proteger a identidade dos usuários [Terrovitis *et al.* 2017].

Portanto, a proposta de implementação de um sistema de monitoramento baseado em RFID/NFC transcende a mera modernização tecnológica. Trata-se de uma iniciativa estratégica que oferece vantagens significativas sobre sistemas legados, como a redução de custos de mão de obra e de erros humanos [Thanapal, Prabhu e Jakhar 2017]. No entanto, seu sucesso depende de uma implementação cuidadosa que enderece os desafios de segurança, como ataques de interceptação (*eavesdropping*) e a necessidade de autenticação mútua para prevenir ataques MITM (*Man-In-The-Middle* - Atacante no Meio) [Thammarat 2020]. Além disso, é preciso mitigar o risco de vazamento de informações por meio de emissões eletromagnéticas não intencionais, que podem ser capturadas a distâncias de 2 a 3 metros dos leitores e da fiação do sistema [Firlej, Musial e Kubiak 2024]. Ao equilibrar os benefícios da coleta de dados com a proteção da privacidade e segurança, o projeto pode auxiliar a gestão do campus, promovendo um ambiente mais seguro, organizado e alinhado às práticas de gestão baseada em dados.

1.2 Objetivos

Nesta seção, serão definidos os objetivos que direcionam o desenvolvimento deste trabalho. Primeiramente, será apresentado o objetivo geral, que encapsula a finalidade principal e o impacto esperado do projeto. Em seguida, serão detalhados os objetivos específicos, que representam as metas concretas a serem alcançadas para que o objetivo geral seja atingido de forma estruturada e completa.

1.2.1 Objetivo Geral

Propor uma arquitetura de sistema de monitoramento de passagem funcional, responsiva e de baixo custo para o IFPB - Campus Campina Grande, baseada nas tecnologias de RFID/NFC, visando a geração de dados para análise de fluxo e otimização da gestão de espaços, possivelmente servindo também como um modelo de referência para outras instituições.

1.2.2 Objetivos Específicos

Para alcançar o objetivo geral, os seguintes objetivos específicos serão desenvolvidos:

1. **Apresentar** um levantamento técnico de *hardware* e *software* para sistemas de monitoramento RFID, com base na literatura, detalhando as especificações, custos e casos de uso de seus componentes [Sartori 2020; Melo 2021].

2. **Propor** uma arquitetura de **Protótipo A (Menor Custo)** para o ponto de entrada principal do IFPB - CG, detalhando os componentes (ESP32, RFID-RC522, MIFARE Classic 1K) e a arquitetura de *software*, visando validar a estabilidade e a confiabilidade da coleta de dados [Chairunnas e Abdurrasyid 2018; Sartori 2020].

3. **Propor** uma arquitetura de **Protótipo B (Alta Segurança)** como uma evolução do protótipo A, sugerindo a substituição de componentes para mitigar as vulnerabilidades de segurança conhecidas (como a clonagem de cartões), recomendando o uso de etiquetas com criptografia robusta (MIFARE DESFire Light) [Sartori 2020; Firlej, Musial e Kubiak 2024].

4. **Analisar** a viabilidade técnica e financeira comparativa de ambas as arquiteturas propostas (A e B), detalhando os desafios de implementação e os benefícios esperados para a gestão do campus [Melo 2021; Terrovitis *et al.* 2017].

5. **Demonstrar** a modularidade e a escalabilidade da arquitetura proposta, indicando como o sistema pode ser rapidamente adaptado para outros ambientes e aplicações (como o controle da Central de Chaves) com alterações mínimas.

1.3 Metodologia

Esta proposta caracteriza-se como uma pesquisa aplicada de natureza exploratória e descritiva, que culminará na elaboração de uma proposta tecnológica detalhada, incluindo a análise comparativa de duas arquiteturas de sistema. A metodologia será estruturada nas seguintes etapas:

1. **Revisão Bibliográfica:** A pesquisa se fundamenta em uma revisão da literatura, analisando artigos científicos e TCCs que abordam a aplicação de RFID/NFC para monitoramento de fluxo e controle de acesso em ambientes acadêmicos [Lukito e Utami 2021; Ozdenizci, Coskun e Ok 2015; Tabuenca, Kalz e Specht 2015]. Esta etapa é importante para identificar os principais desafios a serem endereçados, como a necessidade de autenticação mútua para prevenir ataques de interceptação [Thammarat 2020], o risco de vazamento de dados por emissões eletromagnéticas não intencionais dos componentes do sistema [Firlej, Musial e Kubiak 2024], e a importância de técnicas para anonimização de dados de trajetória a fim de evitar a reidentificação de usuários [Terrovitis *et al.* 2017].

2. **Análise Comparativa e Proposta de Arquiteturas:** Com base na literatura, será realizada uma análise qualitativa e descritiva dos componentes de *hardware* e *software*. Serão propostas duas arquiteturas técnicas distintas: (A) uma de menor custo, focada na viabilidade econômica imediata (utilizando ESP32 Uno e MIFARE Classic), e (B) uma de alta segurança, que mitiga as vulnerabilidades conhecidas da primeira (sugerindo o uso da etiqueta MIFARE DESFire Light).

3. **Análise de Viabilidade e Recomendações:** A análise dos resultados será qualitativa, focada na avaliação da viabilidade das propostas. Os modelos propostos (A e B) serão confrontados com os desafios levantados na literatura e com os objetivos do projeto, realizando uma estimativa de custos comparativa. Serão elaboradas recomendações para uma futura implementação em larga escala, considerando a infraestrutura de rede, o banco de dados e as políticas de governança de dados necessárias para proteger a privacidade da comunidade acadêmica.

Capítulo 2

Referencial Teórico

A tecnologia de Identificação por Radiofrequência (RFID), que fundamenta o sistema proposto neste trabalho, possui um histórico de desenvolvimento que remonta a meados do século XX. Seus conceitos iniciais tomaram forma entre as décadas de 1940 e 1950 com tecnologias como o sistema IFF, que auxiliava na identificação de aeronaves durante a Segunda Guerra Mundial por meio de um *transponder* de longo alcance [Sartori 2020].

Contudo, foi em 1973 que a primeira patente para RFID foi registrada. Mario W. Cardullo requisitou a patente para um sistema RFID ativo com memória regravável. No mesmo ano, de forma notavelmente relevante para o escopo deste trabalho, foi registrada na Califórnia outra patente para um sistema passivo destinado ao destravamento de portas sem o uso de chaves, uma das primeiras aplicações concebidas para o controle de acesso [Melo 2021]. A utilização da tecnologia foi mais evidenciada na década de 1980, impulsionada pela popularização dos computadores pessoais, que trouxeram maior flexibilidade e permitiram o gerenciamento dos dados coletados.

Apesar de sua longa trajetória, a tecnologia RFID está longe de ser ultrapassada. Na verdade, muitos projetos inovadores, principalmente no que se refere à automatização e integração de processos, continuam a ser guiados por esta solução [Melo 2021]. Para o melhor entendimento do cerne do trabalho que será apresentado, as seções seguintes abordarão discussões sobre como a tecnologia funciona, seus conceitos básicos, as partes integrantes do sistema proposto, suas principais aplicações e exemplos desenvolvidos.

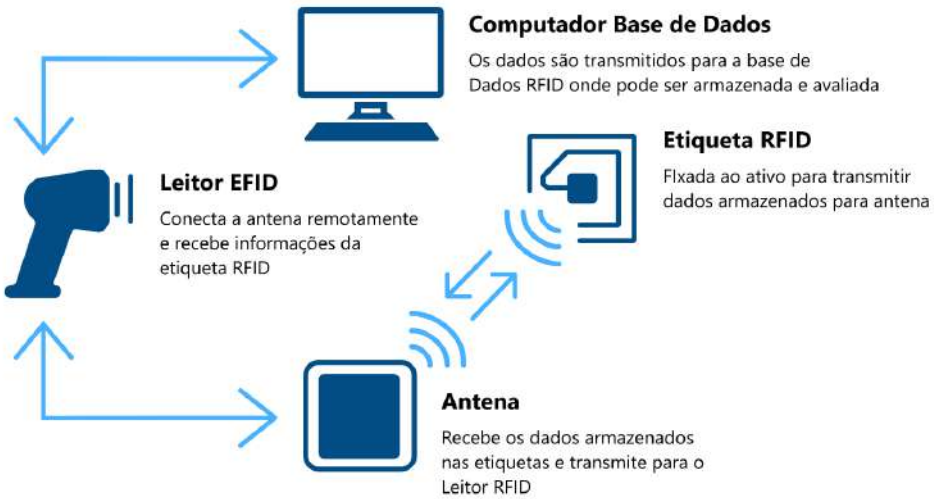
2.1 Identificação por Radiofrequência (RFID)

A RFID é um termo genérico para tecnologias que utilizam ondas de rádio para identificar objetos ou pessoas de forma automática e sem fio [Thanapal, Prabhu e Jakhar 2017; Lukito e Utami 2021]. Um sistema RFID básico é composto por três componentes principais: a etiqueta (ou *tag*), o leitor (ou interrogador) e uma antena. A etiqueta, também conhecida como *transponder*, consiste em um *microchip* de silício para armazenamento e processamento de informações e uma antena para receber e transmitir sinais. As etiquetas podem ser pas-

sivas, ativas ou semi-passivas. As etiquetas passivas, mais comuns em aplicações de controle de acesso, não possuem fonte de energia; elas são energizadas pelo campo eletromagnético gerado pelo leitor quando se aproximam o suficiente [Thanapal, Prabhu e Jakhar 2017; Firlej, Musial e Kubiak 2024]. O leitor, por sua vez, é um dispositivo transceptor que gera o campo de radiofrequência, envia comandos para a etiqueta e recebe os dados armazenados nela, atuando como a ponte entre a etiqueta e o sistema de controle central [Firlej, Musial e Kubiak 2024; Lukito e Utami 2021].

A Figura 2.1 ilustra a arquitetura fundamental e o fluxo de comunicação de um sistema de RFID. O processo é composto por quatro elementos principais que interagem para realizar a captura e o processamento de dados. A **Etiqueta RFID** (*tag*), que é fixada ao item a ser monitorado, armazena um identificador único em seu *chip* interno [Sartori 2020; Melo 2021]. A **Antena** é o componente responsável por emitir o sinal de radiofrequência que ativa a etiqueta (no caso de etiquetas passivas) e por receber os dados transmitidos de volta por ela [Sartori 2020]. O **Leitor RFID**, conectado à antena, gerencia a operação de leitura, decodifica o sinal da etiqueta e atua como uma interface entre o *hardware* de captura e o sistema de *software* [Melo 2021]. Finalmente, o **Computador Base de Dados** recebe as informações enviadas pelo leitor, onde os dados são armazenados, processados e avaliados, permitindo o gerenciamento das informações coletadas [Sartori 2020]. O fluxo operacional, indicado pelas setas, demonstra como o leitor interroga a etiqueta através da antena, e a etiqueta responde com seus dados, que são captados e enviados ao sistema central para processamento e tomada de decisão.

Figura 2.1: *Diagrama de funcionamento de um sistema RFID.*



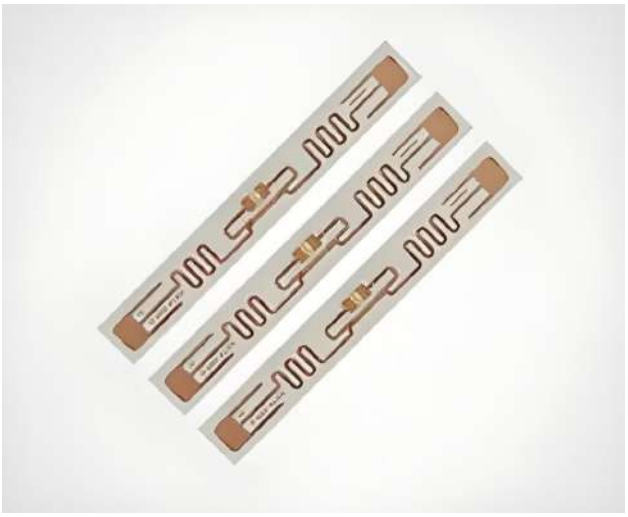
Fonte: [CPCON Sistemas 2022]

2.1.1 Etiquetas *(Tags)* RFID

A etiqueta é o elemento responsável por armazenar um número de série exclusivo e/ou outras informações sobre o objeto ao qual está anexada [Sartori 2020]. Sua estrutura básica contém um *microchip*, que armazena e controla a comunicação, e uma antena, que transmite e responde aos comandos do leitor [Melo 2021]. As etiquetas são classificadas principalmente com base em sua fonte de energia, dividindo-se em passivas e ativas.

- **Etiquetas Passivas**: As etiquetas passivas são caracterizadas por não possuírem uma fonte de energia interna, como uma bateria [Sartori 2020; Melo 2021]. A energia necessária para o seu funcionamento é extraída do campo eletromagnético gerado pelo leitor no momento da comunicação [Melo 2021]. Por essa razão, possuem um alcance de leitura relativamente curto, que pode variar de centímetros a poucos metros [Sartori 2020]. Devido à sua simplicidade, têm um custo de fabricação consideravelmente menor em comparação com as etiquetas ativas, além de um tempo de vida útil praticamente ilimitado, já que não dependem de uma bateria [Sartori 2020]. Sua capacidade de armazenamento é geralmente menor, variando de 64 bits a 8 kilobits [Melo 2021]. São a escolha predominante para aplicações de grande volume e baixo custo, como o controle de acesso proposto neste trabalho. A Figura 2.2 ilustra o design de uma etiqueta RFID passiva, comumente utilizada em aplicações de monitoramento. É possível observar claramente sua estrutura interna, composta pela antena, cujo padrão sinuoso é projetado para a comunicação por radiofrequência, e o *microchip* central, responsável pelo armazenamento do identificador único [RFIDHY; Sartori 2020]. Por não possuírem fonte de energia, estas etiquetas são energizadas pelo campo eletromagnético do leitor, o que lhes confere baixo custo [Sartori 2020; Melo 2021].

Figura 2.2: *Etiqueta Passiva.*



Fonte: [RFIDHY]

- **Etiquetas Ativas**: Diferentemente das passivas, as etiquetas ativas possuem uma fonte de energia, como uma bateria interna [Sartori 2020; Melo 2021]. Essa característica lhes permite transmitir seu sinal ativamente, resultando em um alcance de comunicação muito superior, que pode chegar a dezenas de metros [Sartori 2020]. Por serem mais robustas e complexas, possuem um custo maior e sua vida útil é limitada pela duração da bateria [Sartori 2020]. Essas etiquetas geralmente oferecem maior capacidade de armazenamento e podem integrar funcionalidades adicionais, como sensores para monitoramento de condições ambientais [Melo 2021]. São utilizadas em projetos que demandam maior precisão e alcance de leitura, como no rastreamento de contêineres ou ativos de alto valor [Melo 2021]. A Figura 2.3 apresenta o design de uma etiqueta RFID ativa, caracterizada por possuir uma fonte de energia interna, como uma bateria [Visioshop; Sartori 2020]. Essa autonomia energética permite que ela transmita seu sinal a distâncias maiores, sendo mais robusta para aplicações que exigem maior alcance e poder de comunicação, embora seu custo e vida útil sejam mais elevados em comparação com as etiquetas passivas [Sartori 2020; Melo 2021].

Figura 2.3: *Etiqueta Ativa.*

Fonte: [Visioshop]

2.1.2 Antenas

As antenas são componentes fundamentais em qualquer sistema de comunicação sem fio, sendo essenciais para o funcionamento do RFID [Melo 2021]. Elas atuam como o elemento condutor que converte a energia elétrica em ondas de rádio para transmissão e, inversamente, as ondas de rádio recebidas em energia elétrica para leitura [Sartori 2020]. No leitor, a antena é responsável por emitir o sinal de radiofrequência que cria o campo eletromagnético para

ativar e comunicar-se com as etiquetas, além de receber o sinal de resposta delas [Sartori 2020]. Na etiqueta, a antena capta a energia do campo do leitor (no caso das passivas) e reflete ou transmite o sinal contendo os dados do chip de volta para o leitor [Sartori 2020]. O alinhamento entre a antena da etiqueta e a do leitor é um fator crucial para a eficiência da comunicação [Melo 2021]. A Figura 2.4 exibe um modelo de antena RFID fixa, componente essencial para a comunicação entre o leitor e as etiquetas [Zebra Technologies]. Sua função é converter a energia elétrica do leitor em ondas de radiofrequência para interrogar as etiquetas e, no sentido inverso, captar as ondas de resposta e enviá-las de volta ao leitor para decodificação [Sartori 2020; Melo 2021]. Antenas como esta são frequentemente instaladas em portais e pontos de passagem para criar zonas de leitura definidas.

Figura 2.4: *Antena RFID.*

Fonte: [Zebra Technologies]

2.1.3 Leitor RFID

O leitor, também chamado de transceptor, é o dispositivo que gerencia a comunicação com as etiquetas. Suas principais funções são ativar o *transponder* por meio de um sinal de radiofrequência, estabelecer a comunicação, decodificar os dados recebidos e repassá-los a um sistema computacional (como um microcontrolador ou um servidor) para processamento [Melo 2021; Sartori 2020]. Fatores como a posição do leitor, o meio (materiais como metal e líquidos podem causar interferência) e a compatibilidade entre os equipamentos são essenciais para uma comunicação eficaz [Melo 2021]. Os leitores podem ser classificados como fixos, como os modelos em formato de portal instalados em entradas e saídas, ou portáteis (de mão), que oferecem mobilidade para atividades como a realização de inventários [Melo 2021].

A Figura 2.5 demonstra um leitor RFID fixo instalado em uma estrutura, servindo como a unidade central de processamento em um ponto de monitoramento [Duts Tecnologia]. Este dispositivo, também conhecido como transceptor, gerencia a comunicação com as antenas, envia os sinais de radiofrequência para interrogar as etiquetas e recebe os dados de resposta [Sartori 2020; Melo 2021]. Após decodificar as informações, o leitor as encaminha para o sistema de banco de dados para registro e análise, completando o processo de captura de dados.

Figura 2.5: *Leitor RFID Fixo.*

Fonte: [Duts Tecnologia]

2.2 Comunicação por Campo de Proximidade (NFC)

A NFC é uma tecnologia de comunicação sem fio, de curto alcance e baseada em padrões, que funciona como uma subcategoria da RFID, operando na frequência de 13,56 MHz [Ozdenizci, Coskun e Ok 2015; Firlej, Musial e Kubiak 2024]. Sua principal característica é a necessidade de uma proximidade física de poucos centímetros (tipicamente até 10 cm) para que a interação ocorra, o que confere uma camada intrínseca de segurança ao dificultar a interceptação acidental ou maliciosa de dados [Thammarat 2020; Firlej, Musial e Kubiak 2024]. A tecnologia NFC suporta três modos de operação:

- **Modo Leitor/Gravador (*Reader/Writer*):** Neste modo, um dispositivo habilitado para NFC, como um *smartphone*, atua como um leitor ativo, capaz de ler informações de uma etiqueta NFC passiva (como um cartão de acesso) ou gravar dados nela [Ozdenizci, Coskun e Ok 2015].

- **Modo Ponto a Ponto (*Peer-to-Peer*):** Permite que dois dispositivos com NFC estabeleçam uma conexão bidirecional para trocar informações, como contatos, fotos ou outros arquivos [Ozdenizci, Coskun e Ok 2015].

- **Modo de Emulação de Cartão (*Card Emulation*):** Um dispositivo NFC, como um *smartphone*, pode emular o comportamento de um cartão inteligente sem contato, permitindo que seja usado para pagamentos, bilhetagem de transporte público ou controle de acesso, bastando aproximá-lo de um leitor compatível [Brumercikova e Bukova 2020; Ozdenizci, Coskun e Ok 2015].

2.3 Análise Comparativa das Tecnologias de Identificação

Os Quadros 2.1 e 2.2 oferecem um comparativo detalhado entre as tecnologias de identificação automática, destacando as características e distinções entre *Barcode* (Código de Barras), RFID e NFC.

O Quadro 2.1 demonstra uma visão geral, evidenciando que, enquanto o código de barras depende de uma "Linha de Visada" para a leitura, tanto o RFID quanto o NFC operam através de campos eletromagnéticos, dispensando o contato visual direto [Thanapal, Prabhu e Jakhar 2017]. Uma diferença crucial apontada é o alcance: o RFID se destaca com a capacidade de leitura de até 1 metro, sendo ideal para o rastreamento de "Produtos Volumosos" ou agrupados, enquanto o NFC e o código de barras possuem um alcance de apenas alguns centímetros, adequando-se melhor à identificação de um "Produto Único"por vez [Thanapal, Prabhu e Jakhar 2017]. As frequências de operação também variam significativamente, com o RFID operando na faixa de 850-970 MHz (UHF) e o NFC na frequência padrão de 13,60 MHz (HF) [Thanapal, Prabhu e Jakhar 2017].

O Quadro 2.2 aprofunda a comparação entre NFC e RFID, detalhando suas diferenças fundamentais. O RFID é um sistema mais abrangente, composto por "Antena, Transceptor e Transponder", enquanto o NFC é mais simplificado, consistindo em "Etiquetas NFC e leitor" [Thanapal, Prabhu e Jakhar 2017]. A distinção mais importante para a aplicação reside na comunicação e nas limitações: o RFID permite uma "Comunicação unidirecional" e a "Leitura de múltiplas etiquetas por vez", o que o torna altamente eficiente para tarefas como inventários de armazéns. Em contrapartida, o NFC utiliza uma "comunicação bidirecional" (ponto a ponto), mas está limitado à "Leitura de uma única etiqueta por vez", o que o torna mais adequado para interações seguras e intencionais, como em "Pagamentos sem contato" através de *smartphones* [Thanapal, Prabhu e Jakhar 2017].

Quadro 2.1: *Quadro Comparativo de Tecnologias.*

Tecnologia	Alcance	Técnica	Agrupamento	Frequência	Retenção de Dados
Barcode	3-5cm	Linha de Visada	Produto Único	-	Boa
RFID	1 metro	Radio-frequência	Produtos Volumosos	850-970 MHz	Boa
NFC	2-3cm	Campo Eletromagnético	Produto Único	13,60 MHz	Boa

Fonte: [Thanapal, Prabhu e Jakhar 2017]

Quadro 2.2: *Quadro Comparativo entre NFC e RFID.*

Característica	**NFC**	**RFID**
Princípio de Funcionamento	Campo Eletromagnético	Radiofrequência
Componentes	Etiquetas NFC e leitor	Antena, Transceptor, Transponder
Alcance	Curto alcance	Longo alcance
Comunicação	Ponto a ponto, comunicação bidirecional	Comunicação unidirecional
Limitações	Leitura de uma única etiqueta por vez	Leitura de múltiplas etiquetas por vez
Protocolos	Formato Simples de Troca NDEF *NFC Data Exchange Format* (Formato de Troca de Dados NFC) (LLCP)	ISO e EPC global
Aplicações	Pagamentos sem contato; embarcado em *smartphones* Android.	Inventário de armazéns, escaneamento de bagagens em aeroportos.

Fonte: [Thanapal, Prabhu e Jakhar 2017]

2.4 Padrões e Especificações

Para garantir a interoperabilidade entre os dispositivos de diferentes fabricantes, os sistemas RFID e NFC são regidos por padrões internacionais, principalmente os definidos pela ISO/IEC. Para aplicações de controle de acesso e identificação, como a proposta neste trabalho, dois padrões são proeminentes:

- **ISO/IEC 14443:** Define o padrão para cartões de proximidade (*proximity cards*), operando a uma distância de até 10 cm. É o padrão mais comum para cartões de identificação pessoal, bilhetes de transporte e cartões de pagamento sem contato. A comunicação NFC com *smartphones* em modo de emulação de cartão e leitor/gravador é compatível com este padrão [Lukito e Utami 2021; Ozdenizci, Coskun e Ok 2015]. Esta norma se divide em dois subtipos, A e B, que diferem nos métodos de modulação e codificação. O módulo RC522 e a etiqueta MIFARE Classic utilizados neste projeto são compatíveis com o padrão **ISO/IEC 14443 Tipo A** [Sartori 2020].

- **ISO/IEC 15693:** Este padrão é utilizado para cartões de vizinhança (*vicinity cards*), que permitem uma distância de leitura maior, de até 1 metro. É frequentemente apli-

cado em sistemas de logística e automação de bibliotecas, onde a leitura de múltiplos itens simultaneamente é vantajosa [Lukito e Utami 2021].

O sistema proposto utilizará etiquetas e leitores compatíveis com o padrão ISO/IEC 14443, garantindo a compatibilidade com a maioria dos cartões de identificação e *smartphones* com NFC disponíveis no mercado.

2.5 Funcionamento do Sistema Proposto

O fluxo operacional do sistema de monitoramento de passagem proposto é projetado para ser simples e focado na coleta de dados de forma eficiente, ocorrendo em etapas sequenciais, conforme detalhado a seguir.

Primeiramente, o processo inicia-se quando um usuário (aluno ou servidor) se aproxima de um ponto de monitoramento estratégico — como a entrada do campus, biblioteca ou refeitório — e apresenta sua credencial de identificação (cartão RFID ou *smartphone* com NFC) ao leitor, conforme ilustrado na Figura 2.6. Esta interação é o ponto de partida para o registro da passagem.

Figura 2.6: *Ilustração da interação do usuário com o leitor RFID.*

Fonte: Elaborado pelo autor (2025).

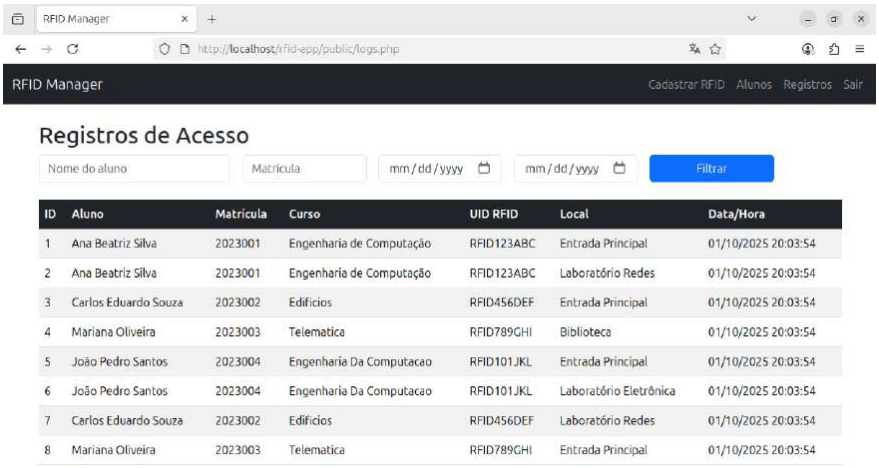
No nível do *hardware*, o módulo leitor RFID-RC522, conectado ao microcontrolador ESP32, gera um campo eletromagnético que energiza a etiqueta passiva e realiza a leitura de seu Identificador Único (UID) [Sartori 2020]. Este UID é então transmitido ao microcontrolador. A principal função do ESP32 neste ponto é atuar como um *gateway*, encaminhando essa informação, juntamente com um identificador do próprio leitor (que define o local), para o servidor central através da rede da universidade, como demonstra o diagrama da Figura 2.7.

Figura 2.7: *Diagrama do fluxo de dados no ponto de monitoramento local.*

Fonte: Elaborado pelo autor (2025).

Uma vez que os dados chegam ao servidor, o sistema de *backend* recebe o UID e realiza uma consulta ao banco de dados para associá-lo à matrícula do usuário correspondente. Com a identidade validada, um novo registro é inserido na Tabela de eventos, contendo a matrícula, o local, a data e o horário exato da passagem como mostrado na Figura 2.8 [Ozdenizci, Coskun e Ok 2015; Brumercikova e Bukova 2020]. O sistema também está preparado para lidar com falhas: caso uma leitura não seja bem-sucedida ou o UID não esteja cadastrado, um evento de "falha de identificação"é registrado com o local e o horário do erro.

Figura 2.8: *Tela de visualização e filtragem dos registros de acesso.*



ID	Aluno	Matrícula	Curso	UID RFID	Local	Data/Hora
1	Ana Beatriz Silva	2023001	Engenharia de Computação	RFID123ABC	Entrada Principal	01/10/2025 20:03:54
2	Ana Beatriz Silva	2023001	Engenharia de Computação	RFID123ABC	Laboratório Redes	01/10/2025 20:03:54
3	Carlos Eduardo Souza	2023002	Edificios	RFID456DEF	Entrada Principal	01/10/2025 20:03:54
4	Mariana Oliveira	2023003	Telematica	RFID789GHI	Biblioteca	01/10/2025 20:03:54
5	João Pedro Santos	2023004	Engenharia Da Computacao	RFID101JKL	Entrada Principal	01/10/2025 20:03:54
6	João Pedro Santos	2023004	Engenharia Da Computacao	RFID101JKL	Laboratório Eletrônica	01/10/2025 20:03:54
7	Carlos Eduardo Souza	2023002	Edificios	RFID456DEF	Laboratório Redes	01/10/2025 20:03:54
8	Mariana Oliveira	2023003	Telematica	RFID789GHI	Entrada Principal	01/10/2025 20:03:54

Fonte: Elaborado pelo autor (2025).

Finalmente, este processo contínuo de coleta de dados de "*check-in*"em múltiplos pontos do campus forma a base para as análises subsequentes, permitindo mapear o fluxo de pessoas, identificar horários de pico e gerar dados quantitativos para a otimização da gestão dos espaços físicos da instituição.

Capítulo 3

Proposta de Arquitetura do Sistema

Com base no referencial teórico, este capítulo detalha a arquitetura técnica proposta para o sistema de monitoramento de passagem no IFPB - Campus Campina Grande. A escolha dos componentes foi guiada pelos pilares definidos nos objetivos: baixo custo econômico, baixa complexidade técnica e ampla disponibilidade de documentação [Sartori 2020].

Para facilitar a análise de viabilidade, a proposta é dividida em duas arquiteturas:

- **Protótipo A:** Uma arquitetura de baixo custo e implementação imediata, focada em validar a estabilidade e a confiabilidade da coleta de dados na entrada principal do campus.
- **Protótipo B:** Uma proposta de evolução da arquitetura A, focada em alta segurança, que substitui componentes vulneráveis para mitigar riscos de segurança conhecidos.

O sistema é dividido em dois módulos principais: o módulo de **Controle**, que abrange os componentes físicos no ponto de monitoramento, e o módulo de **Comando**, que corresponde à infraestrutura de backend (servidor e banco de dados) [Sartori 2020].

3.1 Arquitetura de *Hardware* (Módulo de Controle)

Esta seção detalha os equipamentos físicos que compõem o Módulo de Controle. Estes são os componentes diretamente ligados ao ponto de monitoramento, responsáveis por realizar a captura dos dados de passagem [Sartori 2020].

3.1.1 Protótipo A: Arquitetura de Baixo Custo

Esta arquitetura representa a implementação fundamental para a prova de conceito e validação do sistema, utilizando os componentes de *hardware* mais acessíveis.

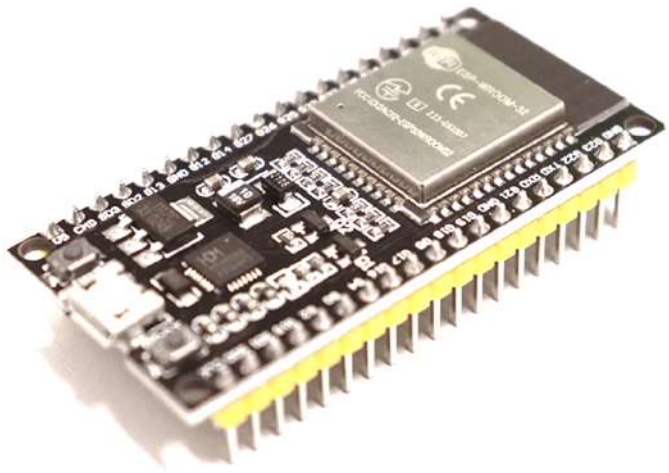
ESP32 (Microcontrolador)

Para o Protótipo A, propõe-se o uso do microcontrolador ESP32 (Figura 3.1) como unidade central de processamento do ponto de leitura. O ESP32 é uma placa de desenvolvimento de baixo custo e alta performance, amplamente utilizada em projetos IoT (*Internet of Things* - Internet das Coisas) [Espressif Systems].

Sua principal vantagem, e a razão de sua escolha, é a inclusão de conectividade *Wi-Fi* e *Bluetooth* nativas no próprio chip. Isso elimina a necessidade de módulos de rede adicionais (como os *"shields"* Ethernet ou Wi-Fi), simplificando drasticamente o design do hardware, reduzindo o custo total e o consumo de energia do ponto de monitoramento [Sartori 2020].

Apesar de ser um hardware mais potente, o ESP32 é totalmente compatível com o ecossistema de software do Arduino. Sua programação pode ser realizada utilizando a mesma Arduino IDE e a linguagem C/C++, mantendo a simplicidade de desenvolvimento e aproveitando a vasta comunidade e bibliotecas existentes [Chairunnas e Abdurrasyid 2018].

Figura 3.1: *Placa de desenvolvimento ESP32 com módulo Wi-Fi integrado.*



Fonte: [Espressif Systems]

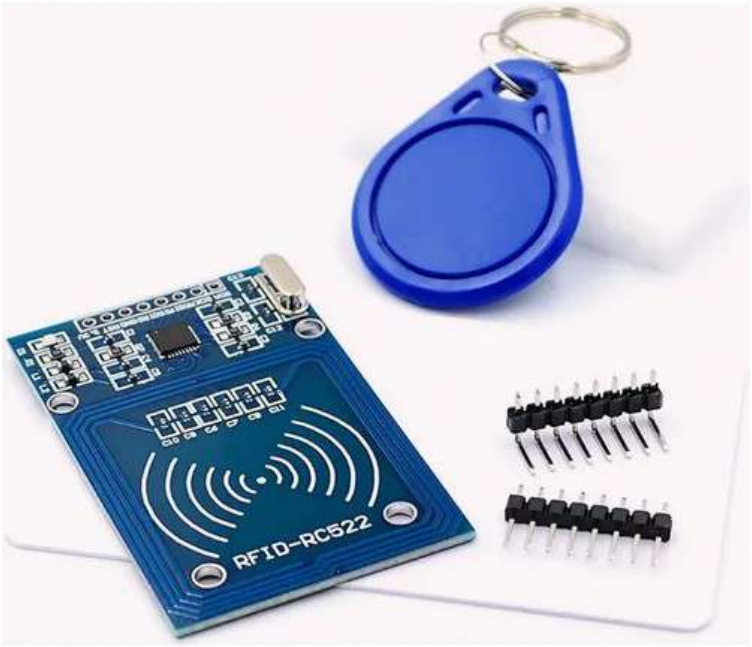
Módulo RFID-RC522

O Módulo RFID-RC522 é um leitor e gravador de baixo custo para etiquetas que operam na frequência de 13,56 MHz [Sartori 2020; SunFounder]. Ele é baseado no circuito integrado MFRC522 da NXP Semicondutores e se destaca pela sua versatilidade e facilidade de integração com microcontroladores como o ESP32 [Sartori 2020; Melo 2021]. O módulo se

comunica com o microcontrolador através de diferentes interfaces, sendo a SPI (*Serial Peripheral Interface* - Interface Periférica Serial) a mais comumente utilizada em projetos com ESP32, permitindo uma taxa de transferência de dados bidirecional de até 424 kbit/s [Sartori 2020]. Sua principal função no projeto é gerar o campo de radiofrequência para energizar e comunicar-se com as etiquetas MIFARE Classic 1K, ler o UID (*Unique Identifier* - Identificador Único) das credenciais apresentadas pelos usuários e transmitir essa informação ao ESP32 para processamento. A popularidade deste módulo em projetos de eletrônica garante uma vasta disponibilidade de bibliotecas e tutoriais, o que simplifica significativamente sua implementação e o desenvolvimento do *software* de controle [Sartori 2020].

A Figura 3.2 exibe o kit do Módulo RFID-RC522, que atua como o leitor e gravador de etiquetas para o sistema proposto [Mercado Livre]. Este módulo, baseado no chip MFRC522 e operando na frequência de 13,56 MHz, é a interface de comunicação entre as credenciais de identificação dos usuários e o microcontrolador ESP32 [Mercado Livre]. Sua escolha se deve à sua compatibilidade com as etiquetas MIFARE Classic 1K, bem como ao baixo custo, ampla documentação e popularidade em projetos de prototipagem, o que simplifica a implementação da etapa de leitura do sistema [Sartori 2020].

Figura 3.2: *Modulo RFID-RC522.*



Fonte: [Mercado Livre]

Etiqueta MIFARE Classic 1K

A MIFARE Classic 1K é um tipo de etiqueta RFID passiva que funciona como um cartão inteligente sem contato (smart card), operando na frequência de 13,56 MHz (HF) [Sartori

2020; NXP Semiconductors]. Ela é totalmente compatível com o padrão ISO/IEC 14443 Tipo A, o que garante sua interoperabilidade com uma vasta gama de leitores, incluindo o módulo RC522 e *smartphones* com tecnologia NFC [Sartori 2020]. O nome "1K" refere-se à sua capacidade de armazenamento de 1024 bytes de memória, que é organizada em 16 setores, cada um contendo 4 blocos de 16 bytes. Essa estrutura permite não apenas o armazenamento do identificador único (UID) não gravável, mas também a leitura e gravação de dados em blocos específicos, protegidos por chaves de acesso (Keys A e B) em cada setor [Sartori 2020]. No contexto do projeto de monitoramento, a etiqueta será utilizada como a credencial de identificação dos usuários (em formato de cartão ou chaveiro), onde seu UID será o dado principal para o registro de passagem [Sartori 2020].

A Figura 3.3 ilustra uma etiqueta RFID passiva no formato de cartão, do padrão MIFARE, que será utilizada como a credencial de identificação no sistema proposto [ABC-RFID]. A imagem detalha sua estrutura em camadas, onde é possível visualizar a antena interna, responsável pela comunicação, e o *microchip*, que armazena o identificador único do usuário [Sartori 2020]. Este formato é ideal para a identificação pessoal, podendo ser facilmente portado por alunos e servidores.

Figura 3.3: *Etiqueta MIFARE.*

Fonte: [ABC-RFID]

3.1.2 Protótipo B: Proposta de Alta Segurança (Evolução)

Esta arquitetura é proposta como a evolução natural do Protótipo A, focada em mitigar os riscos de segurança (detalhados na Seção 3.3) para uma implementação em larga escala.

Etiqueta MIFARE DESFire Light

Para solucionar a vulnerabilidade da cifra Crypto-1 (presente no MIFARE Classic 1K), a arquitetura do Protótipo B propõe a substituição dessas etiquetas pelo MIFARE DESFire Light [NXP Semiconductors]. Esta etiqueta é um circuito integrado sem contato que opera na frequência de 13,56 MHz e é totalmente compatível com o padrão ISO/IEC 14443 Tipo A [NXP Semiconductors].

Sua principal vantagem, alinhada com as recomendações de segurança [Sartori 2020], é a implementação de cifras criptográficas robustas e padronizadas, notavelmente o AES-128bits (*Advanced Encryption Standard* - Padrão de Criptografia Avançado), para a autenticação e a confidencialidade dos dados [NXP Semiconductors]. A utilização de etiquetas com AES resolve o problema da clonagem de credenciais, oferecendo proteção significativamente superior. No entanto, essa melhoria em segurança implica um aumento no custo unitário por etiqueta e uma maior complexidade na implementação do software para o gerenciamento das chaves criptográficas [Sartori 2020].

3.2 Arquitetura de *Software* (Módulo de Comando)

A arquitetura de software, composta pela infraestrutura de backend e pelo código embarcado, é projetada para ser modular e pode servir a ambos os protótipos de *hardware*.

3.2.1 O Papel do *Middleware* RFID

A comunicação entre o *hardware* de leitura (leitores e antenas) e o sistema de aplicação principal (banco de dados e interface de gerenciamento) é gerenciada por um *software* intermediário conhecido como *Middleware* [Melo 2021]. O *Middleware* é responsável por controlar os periféricos, depurar as informações brutas capturadas pelos leitores e convertê-las em dados que o sistema possa interpretar como eventos de negócio. Essencialmente, ele filtra os dados brutos das leituras de etiquetas e os transforma em informações úteis para a aplicação principal [Melo 2021].

3.2.2 *Software* no Servidor Central (*Backend* e Banco de Dados)

Para armazenar e gerenciar os dados de matrículas, nomes de usuários e registros de passagem, a implementação de um servidor de banco de dados central é fundamental.

- **SGBD (Sistema de Gerenciamento de Banco de Dados):** Baseado em trabalhos práticos de referência, optou-se pelo uso do **MariaDB Server**. Trata-se de um SGBD de código aberto derivado do MySQL, conhecido por sua popularidade e robustez [Sartori 2020; MariaDB Foundation]. O banco de dados é projetado para armazenar informações de usuários, dados de operadores e um histórico detalhado de todas as passagens [Sartori 2020].

- **Aplicação de Gerenciamento e Servidor *Web*:** Para permitir que operadores autorizados gerenciem os dados, propõe-se uma aplicação *web* desenvolvida em PHP e hospedada em um servidor *web* Apache [The PHP Group; The Apache Software Foundation]. Esta aplicação serve como uma interface amigável para o gerenciamento do sistema [Sartori 2020].

- **Interface do Frontend:** Para a construção da interface gráfica da aplicação *web* de gerenciamento, foi utilizado o *Bootstrap 5*, um *framework* de *frontend* popular que agiliza o desenvolvimento de interfaces modernas e responsivas (adaptáveis a celulares e tablets) [The Bootstrap Team].

- **Sistema Operacional do Servidor:** Para hospedar o banco de dados e a aplicação *web*, optou-se o uso do **Ubuntu Server 24.04 LTS**, um sistema operacional Linux livre, de código aberto e com suporte de longo prazo [Sartori 2020; Canonical].

3.2.3 *Software* no Ponto de Leitura (Microcontrolador)

O *software* embarcado no microcontrolador (ESP32) em cada ponto de monitoramento é projetado para ser simples e focado na operação em tempo real. A programação do dispositivo é realizada utilizando a Arduino IDE (*Integrated Development Environment* - Ambiente de Desenvolvimento Integrado), que utiliza uma linguagem de programação baseada em C/C++ [Chairunnas e Abdurrasyid 2018; Arduino].

Para a comunicação com o Módulo RFID-RC522, são utilizadas bibliotecas específicas para o ambiente Arduino que implementam o protocolo de comunicação SPI (*Serial Peripheral Interface* - Interface Periférica Serial) e facilitam a leitura dos identificadores das etiquetas MIFARE [SunFounder]. O código desenvolvido no ESP32 é responsável por gerenciar o leitor, capturar o UID da etiqueta apresentada e, em seguida, transmitir esse dado (via módulo de rede adicional, como um *Ethernet* ou *Wi-Fi Shield*) para o servidor central onde o banco de dados está hospedado.

3.3 Análise de Segurança da Arquitetura Proposta

A implementação de um sistema de monitoramento baseado em RFID e NFC, embora traga inúmeros benefícios operacionais, introduz desafios de segurança e privacidade que devem ser cuidadosamente analisados. A natureza sem fio da tecnologia torna a comunicação suscetível a uma variedade de ataques que, se não mitigados, podem comprometer a integridade do sistema e a privacidade dos usuários [Sartori 2020]. Esta seção detalha as principais vulnerabilidades e ameaças aplicáveis à arquitetura proposta, com base na literatura de referência.

3.3.1 Vulnerabilidades da Comunicação e da Credencial

Os riscos de segurança podem ser divididos em duas categorias principais: aqueles que exploram a natureza da comunicação sem fio e aqueles que exploram as fraquezas da credencial (etiqueta) escolhida.

Eavesdropping (Interceptação de Dados)

O *eavesdropping* é uma das ameaças mais diretas, onde um atacante, utilizando uma antena apropriada, intercepta e lê os dados transmitidos pelo ar entre a etiqueta e o leitor [Sartori 2020; Thammarat 2020]. Como muitas etiquetas RFID de baixo custo não possuem criptografia forte na comunicação, informações como o UID podem ser capturadas em texto claro.

Um risco adicional e frequentemente negligenciado é o vazamento de informações por meio de emissões eletromagnéticas não intencionais. Estudos demonstram que os próprios componentes do sistema, como o leitor e sua fiação, podem irradiar sinais que contêm os dados da transação. Esses sinais podem ser capturados a distâncias consideravelmente maiores (de 2 a 3 metros) do que o alcance nominal da comunicação NFC, representando uma falha de segurança física grave [Firlej, Musial e Kubiak 2024].

Clonagem de Credenciais e a Vulnerabilidade do Crypto-1

A principal ameaça à integridade do Protótipo A é a clonagem de etiquetas. Este ataque consiste em copiar os dados de uma credencial válida (principalmente seu UID) e gravá-los em uma etiqueta em branco, criando uma cópia funcional [Sartori 2020]. Com uma etiqueta clonada, um atacante pode realizar um ataque de *spoofing* (falsificação), no qual a credencial falsa se passa por uma legítima, enganando o sistema e fraudando os registros de passagem.

A viabilidade desse ataque está diretamente ligada à vulnerabilidade da cifra criptográfica da etiqueta escolhida (MIFARE Classic 1K). Este modelo utiliza a cifra de fluxo proprietária *Crypto-1* para proteger o acesso à sua memória interna. No entanto, essa cifra possui falhas de segurança publicamente conhecidas, o que a torna suscetível a ataques que permitem a quebra da criptografia e a extração dos dados necessários para a clonagem [Sartori 2020].

3.3.2 Desafios de Privacidade no Monitoramento de Fluxo

Como o objetivo central do projeto é o monitoramento, a privacidade do usuário é uma preocupação fundamental. A coleta contínua de dados de passagem, mesmo que o nome do usuário não seja armazenado diretamente, gera um banco de dados de trajetórias que pode ser explorado [Terrovitis *et al.* 2017].

O principal risco é a reidentificação de usuários a partir de dados supostamente anônimos. Um adversário com conhecimento parcial sobre a rotina de um indivíduo (por exemplo, "o servidor X sempre acessa a biblioteca às 10h") pode cruzar essa informação externa com o

banco de dados de passagens. Ao encontrar um padrão correspondente, ele pode conseguir reidentificar toda a trajetória daquele usuário, descobrindo todos os outros locais e horários registrados, violando sua privacidade [Terrovitis *et al.* 2017]. Portanto, a simples remoção de nomes não é suficiente para garantir o anonimato [Terrovitis *et al.* 2017].

3.3.3 Considerações Finais sobre a Segurança

É fundamental ressaltar que, em uma implementação final, toda a comunicação entre o microcontrolador no ponto de leitura e o servidor central de banco de dados deve ser criptografada, utilizando protocolos padrão como TLS/SSL (*Transport Layer Security/Secure Sockets Layer* - Segurança da Camada de Transporte/Camada de Soquetes Seguros) (HTTPS - *Hypertext Transfer Protocol Secure* - Protocolo de Transferência de Hipertexto Seguro) para proteger os dados em trânsito contra interceptação.

Dado que o escopo deste projeto se limita ao monitoramento de passagem e não envolve o controle de acesso físico a áreas restritas (como no Protótipo A), o impacto imediato de algumas das vulnerabilidades discutidas, como a clonagem de credenciais, é consideravelmente reduzido. Um cartão clonado, neste contexto, poderia no máximo gerar um registro de passagem fraudulento, mas não concederia acesso físico a locais sensíveis. No entanto, é crucial compreender que os riscos à privacidade dos dados de trajetória e à integridade do sistema de registro permanecem relevantes. A análise de segurança apresentada, portanto, serve como um alicerce fundamental, delineando as ameaças que devem ser obrigatoriamente mitigadas para que o sistema possa evoluir de forma segura (como proposto no Protótipo B).

Capítulo 4

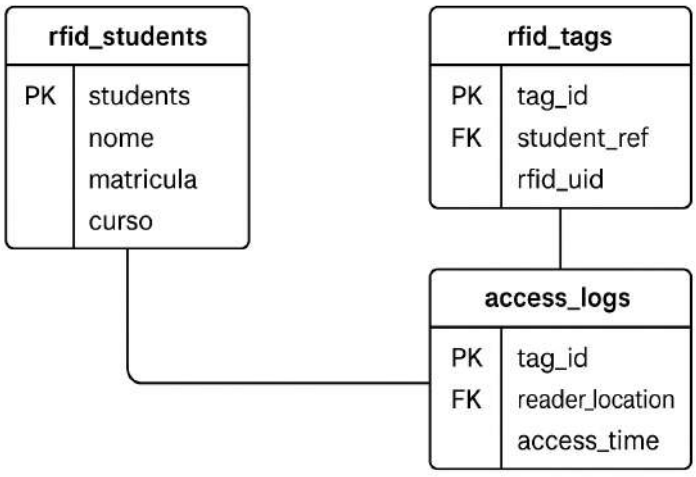
Aplicação *Web* de Gerenciamento

Para complementar a arquitetura de *hardware* e *software* definida no capítulo anterior, foi desenvolvida uma aplicação *Web* que centraliza o gerenciamento de todo o sistema. Esta aplicação é responsável por permitir a administração de usuários e a visualização dos registros de passagem [The PHP Group; MariaDB Foundation; The Bootstrap Team].

4.1 Arquitetura do Banco de Dados (Modelo Segregado)

A arquitetura de banco de dados do sistema foi projetada com foco em segurança e privacidade, adotando um modelo de bancos de dados segregados. Esta abordagem, ilustrada na Figura 4.1, utiliza duas bases de dados distintas para isolar fisicamente as informações pessoais dos alunos dos dados operacionais de monitoramento.

Figura 4.1: *Diagrama da Arquitetura de Bancos de Dados Segregados.*



Elaborado pelo autor (2025).

4.1.1 Base de Dados: `rfid_students`

Esta base de dados atua como o repositório central de PII (*Personally Identifiable Information* - Informações Pessoalmente Identificáveis). Ela contém apenas a tabela `students`, que armazena os dados acadêmicos: `nome`, `matricula` e `curso`. Esta base de dados é projetada para ser altamente protegida e acessada apenas pela aplicação de gerenciamento para tarefas administrativas, como o cadastro de um novo aluno (conforme demonstrado no script `register.php` [Máximo 2025]).

4.1.2 Base de Dados: `rfid_tags`

Esta base de dados operacional gerencia todo o fluxo de monitoramento. Ela é composta por duas tabelas:

- **`tags`:** Armazena o `rfid_uid` da etiqueta e o associa a uma referência numérica (`student_ref`) do aluno correspondente na base `rfid_students`.
- **`access_logs`:** Registra cada evento de passagem, vinculando-o apenas ao `tag_id` (e não diretamente ao aluno), junto com a localização e o horário.

A aplicação se conecta a ambas as bases de dados simultaneamente, conforme demonstrado no arquivo de configuração `db.php`.

4.1.3 Vantagens de Segurança da Arquitetura Segregada

A decisão de separar os bancos de dados é a medida de segurança proativa mais importante da aplicação, atendendo diretamente aos princípios da LGPD (Lei Geral de Proteção de Dados) e oferecendo múltiplas vantagens:

- **Segurança e Conformidade (LGPD):** Os dados pessoais sensíveis (nome, matrícula) são fisicamente separados dos dados de monitoramento (UIDs e logs de acesso). O acesso aos dados pessoais só ocorre em operações administrativas (ex: `register.php` [Máximo 2025]), e não durante as operações de leitura.
- **Anonimização por Design:** O sistema de registro de passagens (`api_log.php` [Máximo 2025]) opera exclusivamente na base `rfid_tags`. A tabela `access_logs` é, portanto, anônima por padrão, registrando apenas um `tag_id` numérico. Para re-identificar um log de acesso, é necessário acesso autorizado a ambas as bases de dados para cruzar as informações.
- **Redução de Risco de Vazamento:** Esta arquitetura minimiza o impacto de um eventual incidente de segurança. Se a base de dados operacional (`rfid_tags`), que é mais exposta por receber requisições da API, for comprometida, o atacante não obterá a lista de alunos, matrículas ou cursos.

- **Modularidade e Escalabilidade:** O módulo de controle (banco `rfid_tags`) pode ser gerenciado, otimizado ou até mesmo migrado de servidor de forma independente, sem afetar ou expor a base de dados acadêmica.

4.2 Política de Gerenciamento e Retenção de Dados

A implementação de um sistema que coleta dados de passagem gera obrigações legais e éticas sobre como essa informação é tratada, armazenada e descartada. A simples coleta e armazenamento indefinido de dados não é uma prática viável, pois aumenta os riscos de privacidade [Terrovitis *et al.* 2017] e o custo de armazenamento do servidor. Esta seção propõe uma política de gerenciamento para os dados coletados.

4.2.1 Tratamento e Acesso aos Dados

Conforme a arquitetura de segurança da aplicação (Seção 4.4), o acesso aos dados brutos de passagem, armazenados na tabela `access_logs`, deve ser altamente restrito.

- **Acesso Restrito:** Somente operadores de sistema autenticados, com nível de permissão de administrador, devem ter acesso à visualização dos registros de passagem que associam um indivíduo a um local e horário [Sartori 2020].
- **Finalidade do Tratamento:** O tratamento primário dos dados deve ser para fins estatísticos e agregados (análise de fluxo, horários de pico), conforme a justificativa deste trabalho [Sartori 2020]. O acesso a registros individuais deve ser reservado apenas para fins de auditoria de segurança ou verificação de falhas no sistema.
- **Conformidade Legal:** Todo o tratamento deve seguir os princípios da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo a transparência e a segurança das informações pessoais.

4.2.2 Política de Retenção e Descarte

Para mitigar os riscos de privacidade e gerenciar o crescimento do banco de dados (estimado em um servidor de 500GB), é crucial definir um ciclo de vida para os dados:

1. **Período de Retenção (Dados Identificáveis):** Propõe-se que os dados brutos na tabela `access_logs`, que vinculam um `student_id` a um registro de passagem, sejam mantidos por um período de 12 (doze) meses. Este período é suficiente para realizar análises de fluxo sazonais (comparação entre semestres) sem reter indefinidamente dados sensíveis de trajetória [Terrovitis *et al.* 2017].

2. **Processo de Anonimização (Após 12 meses):** Após o término do período de retenção, sugere-se a execução de um script de banco de dados automatizado. Este script deve anonimizar os registros antigos, por exemplo, removendo (setando para `NULL`) o campo `student_id` da tabela `access_logs`.

3. **Benefício da Anonimização:** Ao desassociar o registro de passagem do indivíduo, o risco de reidentificação de trajetória é eliminado [Terrovitis *et al.* 2017]. No entanto, os dados estatísticos (localização, data e hora) são preservados, permitindo que a instituição continue a realizar análises históricas de fluxo e a gerar "mapas de calor"de longo prazo, cumprindo o objetivo primário do sistema sem violar a privacidade dos usuários.

Esta política de retenção e anonimização garante que o sistema permaneça útil para a gestão e, ao mesmo tempo, em conformidade com as melhores práticas de privacidade e segurança de dados.

4.3 API para Registro de Passagens

A comunicação entre o *hardware* (microcontrolador ESP32) e o sistema central é realizada através de uma API (*Application Programming Interface* - Interface de Programação de Aplicações) simples e direta. Esta API funciona como um *endpoint* que aguarda requisições HTTP (Hypertext Transfer Protocol - Protocolo de Transferência de Hipertexto). Quando o microcontrolador lê uma etiqueta, ele envia uma requisição para a API contendo o UID lido e a localização do leitor. O backend então verifica se o UID está cadastrado na Tabela de alunos. Em caso afirmativo, um novo registro de passagem é criado na Tabela de registros; caso contrário, uma resposta de erro é retornada, indicando que a credencial não é válida.

4.4 Segurança da Aplicação e dos Dados

Além da segurança física do *hardware* RFID (discutida no Capítulo 3), a aplicação web que gerencia os dados implementa camadas cruciais de segurança de *software* para proteger a integridade do sistema e a privacidade dos dados dos alunos.

4.4.1 Controle de Acesso ao Painel (Autenticação)

O acesso ao painel de gerenciamento é protegido por um sistema de autenticação de operador. O script de *login* verifica o nome de usuário e a senha fornecidos. Crucialmente, as senhas no banco de dados são armazenadas de forma criptografada, utilizando *hashes* seguros gerados pela função `password_hash()` do PHP. No momento do *login*, a senha digitada é validada usando a função `password_verify()`, que compara a entrada com o

hash armazenado. Esta abordagem impede que, mesmo em caso de vazamento do banco de dados, as senhas originais dos operadores sejam expostas.

Uma vez autenticado, o sistema inicia uma sessão de usuário. Todas as páginas administrativas subsequentes verificam ativamente a existência desta sessão. Caso um usuário não autenticado tente acessar uma página restrita, ele é automaticamente redirecionado de volta para a tela de login, garantindo que apenas operadores autorizados possam visualizar ou manipular os dados.

4.4.2 Proteção Contra Injeção de SQL

A maior vulnerabilidade em aplicações *web* que interagem com bancos de dados é o ataque de Injeção de SQL (SQL Injection). Para prevenir esta ameaça, todas as operações de banco de dados na aplicação (cadastro, edição, exclusão, login e registro de logs) são implementadas utilizando *Prepared Statements* (Declarações Preparadas) com parâmetros vinculados (*bind_param*).

Esta técnica separa a instrução SQL da inserção dos dados do usuário. Ao fazer isso, o SGBD trata os dados recebidos (como um nome de aluno ou um UID vindo da API) puramente como texto, e não como parte do comando SQL. Isso torna impossível para um atacante "injetar"comandos maliciosos para apagar tabelas ou escalar privilégios, garantindo a integridade e a segurança do banco de dados.

4.4.3 Segurança na Transmissão de Dados

Conforme discutido no Capítulo 3, a comunicação entre o ESP32 e a API, bem como entre o navegador do operador e o painel web, deve ser criptografada. Em uma implementação de produção, é mandatório que o servidor Apache seja configurado para operar sobre HTTPS (HTTP sobre TLS/SSL). Isso garante que todos os dados, incluindo UIDs, matrículas e senhas de operadores, sejam criptografados durante a transmissão, prevenindo ataques de interceptação (*eavesdropping* ou *man-in-the-middle*) na rede da instituição [Thammarat 2020].

4.5 Painel de Gerenciamento *web*

O painel de gerenciamento é a interface gráfica que permite a um operador autenticado administrar o sistema. Ele é protegido por um sistema de sessão e oferece as seguintes funcionalidades principais:

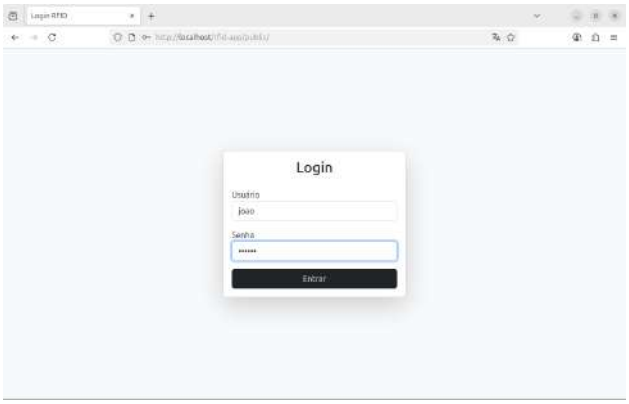
- Autenticação e Acesso ao Painel.
- *Dashboard* e Navegação Principal.
- Gerenciamento de Alunos e Etiquetas.

- Monitoramento e Análise de Passagens.

4.5.1 Autenticação e Acesso ao Painel

O acesso ao sistema é iniciado por uma tela de *login* (Conexão), ilustrada na Figura 4.2, onde o operador deve fornecer seu nome de usuário e senha. O sistema valida as credenciais e, em caso de sucesso, concede acesso ao painel principal.

Figura 4.2: *Tela de login do sistema de gerenciamento.*



Fonte: Elaborado pelo autor (2025).

4.5.2 *Dashboard* e Navegação Principal

Após a autenticação, o operador é direcionado para a tela principal, ou *dashboard* (Figura 4.3). Esta interface apresenta uma visão geral e acesso rápido às três funcionalidades centrais do sistema: cadastro de novas credenciais, gerenciamento de usuários existentes e visualização dos registros de passagem.

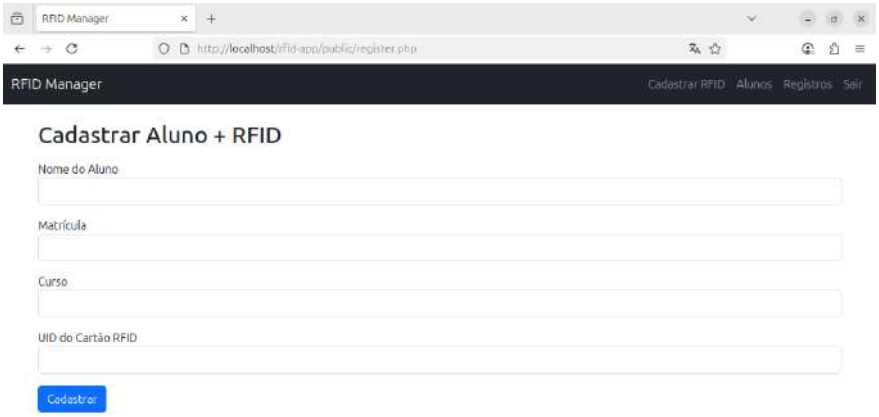
Figura 4.3: *Dashboard principal da aplicação web.*

Fonte: Elaborado pelo autor (2025).

4.5.3 Gerenciamento de Alunos e Etiquetas

Esta seção abrange as operações de cadastro e manutenção dos usuários do sistema. A funcionalidade de cadastro, apresentada na Figura 4.4, consiste em um formulário para inserir os dados de um novo aluno (nome, matrícula, curso) e associá-los ao UID da sua etiqueta RFID.

Figura 4.4: *Formulário para cadastro de um novo aluno e sua etiqueta RFID.*



Fonte: Elaborado pelo autor (2025).

A gestão dos cadastros existentes é realizada através de uma Tabela que lista todos os alunos, como mostrado na Figura 4.5. A partir desta tela, o operador pode editar as informações de um usuário ou excluí-lo do sistema.

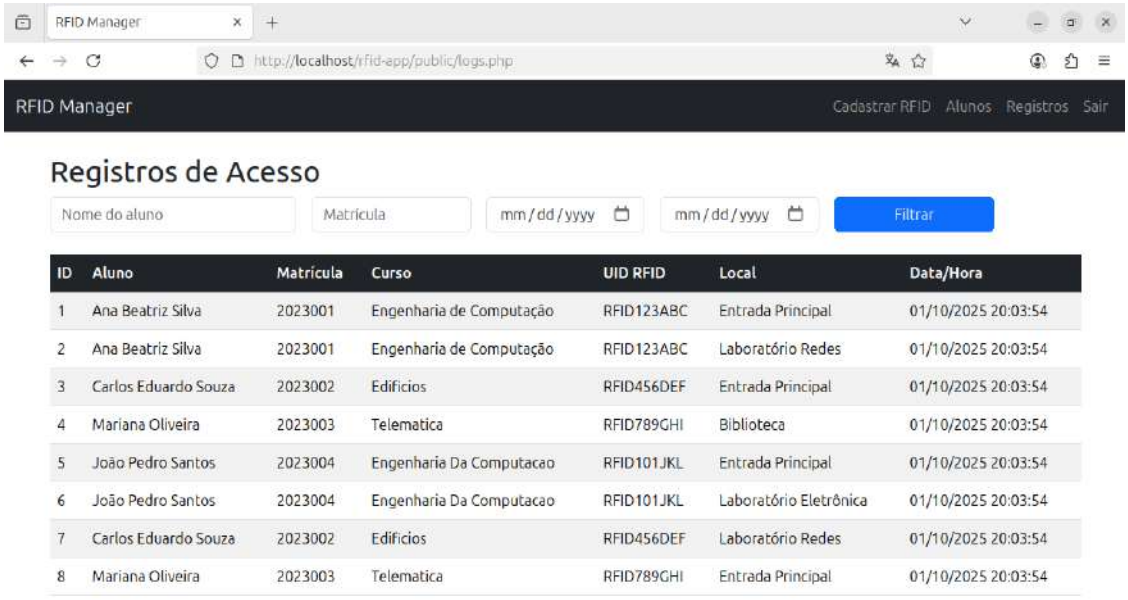
Figura 4.5: *Tabela de listagem dos alunos e RFIDs cadastrados.*

Fonte: Elaborado pelo autor (2025).

4.5.4 Monitoramento e Análise de Passagens

A funcionalidade de visualização de registros de acesso é a ferramenta principal para a análise de dados de fluxo Figura 4.6. Ela exibe um histórico detalhado de todas as passagens capturadas pelos leitores, ordenadas cronologicamente. Para facilitar a consulta, a interface inclui um sistema de filtros que permite ao operador pesquisar registros por nome do aluno, número de matrícula ou por um intervalo de datas específico.

Figura 4.6: *Tela de visualização e filtragem dos registros de acesso.*



ID	Aluno	Matrícula	Curso	UID RFID	Local	Data/Hora
1	Ana Beatriz Silva	2023001	Engenharia de Computação	RFID123ABC	Entrada Principal	01/10/2025 20:03:54
2	Ana Beatriz Silva	2023001	Engenharia de Computação	RFID123ABC	Laboratório Redes	01/10/2025 20:03:54
3	Carlos Eduardo Souza	2023002	Edificios	RFID456DEF	Entrada Principal	01/10/2025 20:03:54
4	Mariana Oliveira	2023003	Telematica	RFID789GHI	Biblioteca	01/10/2025 20:03:54
5	João Pedro Santos	2023004	Engenharia Da Computacao	RFID101JKL	Entrada Principal	01/10/2025 20:03:54
6	João Pedro Santos	2023004	Engenharia Da Computacao	RFID101JKL	Laboratório Eletrônica	01/10/2025 20:03:54
7	Carlos Eduardo Souza	2023002	Edificios	RFID456DEF	Laboratório Redes	01/10/2025 20:03:54
8	Mariana Oliveira	2023003	Telematica	RFID789GHI	Entrada Principal	01/10/2025 20:03:54

Fonte: Elaborado pelo autor (2025).

Capítulo 5

Estimativa de Custos e Orçamento

A viabilidade de um projeto tecnológico em uma instituição pública está intrinsecamente ligada aos custos de sua implementação. Conforme um dos pilares deste trabalho, a solução proposta foi concebida para ser economicamente acessível, utilizando componentes de *hardware* de menor custo e *software* de código aberto [Sartori 2020]. Esta seção apresenta uma estimativa de orçamento para as duas arquiteturas de monitoramento propostas (Protótipo A e B) para a entrada principal do IFPB, cobrindo quatro pontos de leitura (sendo 3 nas catracas da entrada principal e o outro na entrada de veículos) e a infraestrutura de servidor. Adicionalmente, apresenta um orçamento independente para um sistema de menor escala, focado na Central de Chaves.

5.1 Custos de *Hardware*

O *hardware* representa o principal investimento inicial do projeto. Os componentes foram selecionados com base em sua funcionalidade, custo-benefício e ampla documentação, conforme detalhado no Capítulo 3.

5.1.1 Pontos de Monitoramento (Microcontroladores e Leitores)

Cada ponto de monitoramento, em ambas as propostas, será composto por um microcontrolador ESP32 e um módulo leitor RFID-RC522. Para uma implementação inicial cobrindo quatro locais distintos, serão necessários:

- 4x ESP32: A unidade de processamento local, responsável por gerenciar o leitor e comunicar-se com o servidor [Eletrogate].
- 4x Módulo RFID-RC522: O leitor de radiofrequência para a captura do UID das etiquetas [Mercado Livre].

Os custos unitários são baseados em pesquisas de mercado em varejistas online nacionais.

5.1.2 Credenciais de Identificação (Etiquetas)

Este é o ponto de variação entre as duas arquiteturas propostas. A estimativa considera um volume inicial de 2.000 etiquetas para cobrir a demanda inicial da entrada principal do campus.

- **Proposta A (Menor Custo):** 2000x Etiquetas MIFARE Classic 1K. Compatíveis com o leitor RC522, porém possuem a vulnerabilidade de segurança conhecida (Crypto-1) [NXP Semiconductors; Sartori 2020].
- **Proposta B (Alta Segurança):** 2000x Etiquetas MIFARE DESFire Light. Estas etiquetas utilizam criptografia robusta (AES) e são recomendadas para mitigar o risco de clonagem [NXP Semiconductors; Sartori 2020]. O custo unitário é superior, refletindo a maior segurança.

5.1.3 Servidor Central

A aplicação *web* e o banco de dados serão hospedados em um servidor dedicado. Para esta estimativa, consideramos os requisitos mínimos para rodar o sistema operacional Ubuntu Server 24.04 LTS e o SGBD MariaDB, com capacidade de armazenamento suficiente.

- **1x Servidor de Entrada:** Um computador ou mini-PC com, no mínimo, 4GB de RAM, processador dual-core e um SSD de 500 GB. Esta configuração garante bom desempenho para a aplicação e escalabilidade para o banco de dados.

5.2 Custos de *Software* e Implementação

Uma das maiores vantagens da arquitetura proposta reside nos custos de *software*.

- ***Software* (Licenciamento):** A pilha de *software* selecionada, composta pelo sistema operacional Ubuntu Server, o SGBD MariaDB, o servidor *web* Apache e as linguagens PHP e C/C++ (para o ESP32), é inteiramente baseada em tecnologias de código aberto e gratuitas [Canonical; MariaDB Foundation; The Apache Software Foundation; The PHP Group]. Portanto, o custo de licenciamento de *software* é nulo.
- **Desenvolvimento e Mão de Obra:** Em um contexto comercial, o custo de desenvolvimento do *software* e a mão de obra para instalação e configuração da infraestrutura seriam os itens mais significativos do orçamento [Melo 2021]. No entanto, para este trabalho de conclusão de curso, este custo é abstraído, uma vez que o desenvolvimento constitui o próprio escopo acadêmico do projeto.

5.3 Resumo do Orçamento (Propostas A e B)

A Tabela 5.1 ilustra a estimativa de custos comparativa para a implementação inicial do sistema de monitoramento no IFPB, detalhando os valores para o Protótipo A (Menor Custo) e o Protótipo B (Alta Segurança).

Quadro 5.1: *Tabela de Orçamento Comparativo (Protótipo A vs. B).*

Item	**Qtd.**	**Valor Unit. (Est.)**	**Total (Proposta A)**	**Total (Proposta B)**
Hardware				
ESP32	4	R$ 75,00	R$ 300,00	R$ 300,00
Módulo RFID-RC522	4	R$ 25,00	R$ 100,00	R$ 100,00
Etiqueta MIFARE Classic 1K	2000	R$ 2,50	R$ 5.000,00	N/A
Etiqueta MIFARE DESFire Light	2000	R$ 7,50	N/A	R$ 15.000,00
Servidor de Entrada (Mini-PC)	1	R$ 2.000,00	R$ 2.000,00	R$ 2.000,00
Fontes de Alimentação e Cabos	-	R$ 150,00 (lote)	R$ 150,00	R$ 150,00
Software e Serviços				
Software (Licenciamento)	-	R$ 0,00	R$ 0,00	R$ 0,00
Desenvolvimento	-	N/A	N/A	N/A
TOTAL ESTIMADO			**R$ 7.550,00**	**R$ 17.550,00**

Elaborado pelo autor (2025).

A análise orçamentária demonstra que a implementação do Protótipo A (Baixo Custo) é financeiramente viável, com um custo total estimado em **R$ 7.550,00**. Este valor confirma a premissa do projeto de utilizar tecnologias acessíveis para a validação do sistema. O Protótipo B (Alta Segurança), embora represente um investimento significativamente maior, na ordem de **R$ 17.550,00**, devido majoritariamente ao custo das etiquetas seguras, é a arquitetura recomendada para uma implementação definitiva que vise segurança e conformidade a longo prazo.

5.4 Estimativa de Custos para a Central de Chaves

Seguindo a mesma premissa de utilizar componentes acessíveis e *software* livre, esta seção apresenta uma estimativa de custos para a implementação de um sistema simplificado de controle e registro de chaves, utilizando a tecnologia RFID. O orçamento contempla um único ponto de leitura/gerenciamento e um lote inicial de 100 etiquetas em formato de chaveiro. Para esta aplicação, a vulnerabilidade do MIFARE Classic 1K não é considerada crítica, visto que o sistema é de uso interno e restrito.

5.4.1 Componentes e Custos Estimados

A Tabela 5.2 detalha os itens necessários e seus custos aproximados, baseados em valores de mercado para componentes de varejo.

Quadro 5.2: *Tabela de Orçamento Estimativo para a Central de Chaves.*

Item	**Qtd.**	**Valor Unitário (Est.)**	**Valor Total (Est.)**
Hardware			
Computador (Servidor/Gerenciamento)	1	R$ 2.000,00	R$ 2.000,00
ESP32	1	R$ 75,00	R$ 75,00
Módulo RFID-RC522	1	R$ 25,00	R$ 25,00
Etiqueta MIFARE 1K (Chaveiro)	100	R$ 2,50	R$ 250,00
Fontes de Alimentação e Cabos	-	R$ 150,00 (lote)	R$ 150,00
Software e Serviços			
Software (Licenciamento - Código Aberto)	-	R$ 0,00	R$ 0,00
Desenvolvimento e Implementação	-	N/A (escopo acadêmico)	
TOTAL ESTIMADO			**R$ 2.500,00**

Elaborado pelo autor (2025).

O custo total estimado para a implementação do sistema na Central de Chaves é de R$ 2.500,00. Este valor demonstra a alta viabilidade econômica de aplicar a tecnologia RFID mesmo em projetos de menor escala, automatizando o controle e o registro de itens importantes com um investimento inicial reduzido.

Capítulo 6

Considerações Finais e Sugestões para Trabalhos Futuros

Ao término deste trabalho, é possível consolidar os resultados alcançados e refletir sobre o impacto da proposta, bem como delinear os próximos passos para a evolução do sistema. Este capítulo apresenta as conclusões obtidas através da pesquisa e análise de viabilidade, seguidas por sugestões para futuras implementações que podem expandir e aprimorar a solução aqui proposta.

6.1 Considerações Finais

O objetivo geral deste trabalho foi propor e analisar a viabilidade de um sistema de monitoramento de passagem para o IFPB - Campus Campina Grande, utilizando as tecnologias RFID e NFC. Pode-se concluir que este objetivo foi plenamente alcançado. A pesquisa demonstrou que a implementação de tal sistema é uma solução promissora, viável e estratégica para a instituição, alinhando-se à necessidade de uma gestão moderna e baseada em dados [Sartori 2020; Melo 2021].

A metodologia adotada, focada na revisão da literatura e na análise de arquiteturas, permitiu atingir os objetivos específicos. Foi realizado um levantamento aprofundado dos componentes de *hardware* e *software*, resultando na proposta de duas arquiteturas distintas: um Protótipo A (Menor Custo), focado na validação imediata da coleta de dados usando componentes acessíveis como o ESP32 e etiquetas MIFARE Classic 1K; e um Protótipo B (Alta Segurança), que endereça as vulnerabilidades de segurança do Protótipo A através da adoção de etiquetas com criptografia AES, como a MIFARE DESFire Light [Sartori 2020; NXP Semiconductors].

A análise de custos demonstrou a alta viabilidade financeira de ambas as propostas, especialmente o Protótipo A (com custo estimado em R$ 7.550,00 para uma implementação inicial), que confirma a premissa de criar uma solução de baixo custo. A proposta de uma aplicação web de gerenciamento, baseada inteiramente em software de código aberto (PHP,

MariaDB, Apache), também contribui para a acessibilidade do projeto [Sartori 2020].

Além disso, o trabalho identificou os desafios críticos, como os riscos de clonagem de credenciais associados à cifra Crypto-1 e as questões de privacidade na análise de dados de trajetória [Sartori 2020; Terrovitis *et al.* 2017]. Ao contextualizar esses riscos, concluiu-se que, para o escopo inicial de monitoramento (sem controle de acesso físico), as vulnerabilidades são gerenciáveis, embora a evolução para o Protótipo B seja fundamental para uma implementação definitiva e segura.

Em suma, este trabalho entrega uma proposta de arquitetura completa e funcional, que se provou viável técnica e economicamente, servindo como um alicerce sólido para a futura implementação de um sistema que irá automatizar a coleta de dados de fluxo e auxiliar a gestão de espaços no IFPB.

6.2 Sugestões para Trabalhos Futuros

A arquitetura proposta neste TCC serve como um ponto de partida para um sistema muito mais robusto e integrado. As seguintes sugestões são apresentadas para a sua evolução:

- **Implementação do Controle de Acesso Físico:** A evolução mais natural do sistema é transcender o monitoramento e implementar o controle de acesso ativo. Isso envolveria a integração do Protótipo B (com etiquetas seguras baseadas em AES) a atuadores como travas eletromagnéticas, solenoides ou catracas. Esta expansão permitiria o gerenciamento de acesso a locais restritos, como laboratórios, salas de servidores e áreas administrativas, aumentando significativamente a segurança física da instituição [Sartori 2020; Chairunnas e Abdurrasyid 2018].

- **Integração com o SUAP via API:** Para garantir a validação de dados de forma segura, propõe-se o desenvolvimento de uma API que integre a aplicação *web* do sistema ao SUAP (Sistema Unificado de Administração Pública). Isso permitiria ao sistema consultar diretamente o banco de dados acadêmico, validando matrículas em tempo real e automatizando o cadastro, a atualização e a remoção de usuários (alunos e servidores), eliminando a necessidade de gerenciamento manual na aplicação *web*.

- **Análise de Dados com Inteligência Artificial:** O sistema proposto é um grande gerador de dados de fluxo. Sugere-se o desenvolvimento de um módulo de BI (*Business Intelligence* - Inteligência de Negócios) ou a aplicação de técnicas de Inteligência Artificial e *Machine Learning* (Aprendizado de Máquina) sobre o banco de dados de registros. Esses modelos poderiam identificar padrões complexos, prever congestionamentos, sugerir otimizações de horários e auxiliar a gestão na tomada de decisões estratégicas sobre o uso dos espaços, concretizando o objetivo de "otimização da gestão de espaços físicos" [Ozdenizci, Coskun e Ok 2015].

- **Implementação de Credenciais Móveis (NFC):** Explorar o modo de Emulação de Cartão (Card Emulation Mode) da tecnologia NFC [Ozdenizci, Coskun e Ok 2015; Brumercikova e Bukova 2020]. Isso permitiria o desenvolvimento de um aplicativo institucional onde alunos e servidores poderiam utilizar seus próprios *smartphones* como credencial de acesso, reduzindo a dependência e o custo de emissão de milhares de cartões físicos.

- **Implementação de Anonimização Avançada:** Conforme apontado na análise de segurança [Terrovitis *et al.* 2017], a simples remoção de nomes não garante a privacidade. Um trabalho futuro deve implementar técnicas de anonimização mais robustas, como a supressão de locais ou a divisão de trajetórias, diretamente no banco de dados antes que os dados sejam expostos para análise, garantindo a proteção da privacidade dos usuários.

Referências Bibliográficas

[ABC-RFID] ABC-RFID. *White Blank RFID NFC Card*. Disponível em: <https://www.abcrfid.com/product/white-blank-rfid-nfc-card/>. 18

[Arduino] Arduino. *UNO R3*. Disponível em: <https://docs.arduino.cc/hardware/uno-rev3/>. 20

[Brumercikova e Bukova 2020] BRUMERCIKOVA, E.; BUKOVA, B. Proposals for Using the NFC Technology in Regional Passenger Transport in the Slovak Republic. *Open Engineering*, v. 10, n. 1, p. 238–244, 2020. 2, 11, 14, 37

[Canonical] Canonical. *Ubuntu 24.04 LTS*. Disponível em: <https://ubuntu.com/blog/tag/ubuntu-24-04-lts>. 20, 32

[Chairunnas e Abdurrasyid 2018] CHAIRUNNAS, A.; ABDURRASYID, I. Near field communication (NFC) model for arduino uno based security systems office system. In: *IOP Conference Series: Materials Science and Engineering*. [S.l.: s.n.], 2018. v. 332, n. 1, p. 012006. 3, 16, 20, 36

[CPCON Sistemas 2022] CPCON Sistemas. *Sensor RFID: o que é e como funciona?* 2022. Disponível em: <https://www.grupocpcon.com/sensor-rfid-o-que-e-e-como-funciona/>. 6

[Duts Tecnologia] Duts Tecnologia. *ZEBRA LEITOR FIXO DE RFID FX9600*. Disponível em: <https://www.dutstecnologia.com.br/loja/zebra-leitor-fixo-de-rfid-fx9600/>. 10

[Eletrogate] Eletrogate. *Módulo WiFi ESP32 DEVKITC-S1*. Disponível em: <https://www.eletrogate.com/modulo-wifi-esp32-devkitc-s1-modelo-2>. 31

[Espressif Systems] Espressif Systems. *ESP32 Series Datasheet*. Disponível em: <https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf>. 16

[Espressif Systems] Espressif Systems. *Módulo ESP32-WROOM-32*. Imagem de um módulo ESP32 DEVKIT V1 com chip WROOM-32. 16

[Firlej, Musial e Kubiak 2024] FIRLEJ, A.; MUSIAL, S.; KUBIAK, I. Data Immunity in Near Field Radio Frequency Communication Systems—NFC as an Aspect of Electromagnetic Information Security. *Applied Sciences*, v. 14, n. 13, p. 5854, 2024. 1, 2, 3, 4, 6, 10, 21

[Lukito e Utami 2021] LUKITO, R. B.; UTAMI, V. R. Optimized use of RFID at XYZ University Library in Doing Auto Borrowing Book by Utilizing NFC Technology on Smartphone. *Advances in Science, Technology and Engineering Systems Journal*, v. 6, n. 1, p. 532–537, 2021. 1, 2, 4, 5, 6, 12, 13

[MariaDB Foundation] MariaDB Foundation. *MariaDB.org*. Disponível em: <https://mariadb.org/>. 19, 23, 32

[Melo 2021] MELO, C. d. S. *Tecnologia RFID: uma proposta para automação de um centro de distribuição em uma metalúrgica*. Dissertação (Trabalho de Conclusão de Curso) — Centro Universitário UniFacisa, Campina Grande, PB, 2021. 3, 5, 6, 7, 8, 9, 10, 16, 19, 32, 35

[Mercado Livre] Mercado Livre. *Kit Módulo Leitor Rfid Mfrc522 Aproximação Arduino Raspberry*. Disponível em: <https://www.mercadolivre.com.br/kit-modulo-leitor-rfid-mfrc522-aproximaco-arduino-raspberry/p/MLB32625634>. 17, 31

[Máximo 2025] MáXIMO, J. V. N. *Sistema de Monitoramento de Acesso Baseado em RFID: Código Fonte da Aplicação Web*. 2025. Repositório no GitHub. Disponível em: <https://github.com/JoaoVitorNM/rfid-app>. 24

[NXP Semiconductors] NXP Semiconductors. *MIFARE Classic EV1 1K/4K*. Disponível em: <https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-classic/mifare-classic-ev1-1k-4k:MF1S50YYX_V1>. 17, 32

[NXP Semiconductors] NXP Semiconductors. *MIFARE DESFire Light*. Disponível em: <https://www.nxp.com/products/MF3DHx3>. 19, 32, 35

[Ozdenizci, Coskun e Ok 2015] OZDENIZCI, B.; COSKUN, V.; OK, K. NFC Internal: An Indoor Navigation System. *Sensors*, v. 15, n. 4, p. 7571–7595, 2015. 2, 4, 10, 11, 12, 14, 36, 37

[RFIDHY] RFIDHY. *O que é RFID passivo?* Disponível em: <https://www.rfidhy.com/pt/what-is-passive-rfid/>. 7

[Sartori 2020] SARTORI, O. A. A. *Identificação por Radiofrequência: Estudo teórico e prática aplicada ao controle de acesso*. Dissertação (Trabalho de Conclusão de Curso) — Universidade Federal do Rio de Janeiro, 2020. 1, 3, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 19, 20, 21, 25, 31, 32, 35, 36

[SunFounder] SunFounder. *8. Basic MFRC522*. Disponível em: <https://docs.sunfounder.com/projects/elite-explorer-kit/en/latest/basic_projects/08_basic_mfrc522.html>. 16, 20

[Tabuenca, Kalz e Specht 2015] TABUENCA, B.; KALZ, M.; SPECHT, M. Tap it again, Sam: Harmonizing Personal Environments towards Lifelong Learning. *International Journal of Advanced Corporate Learning (iJAC)*, v. 8, n. 1, p. 16–23, 2015. 4

[Terrovitis *et al.* 2017] TERROVITIS, M. *et al.* Local Suppression and Splitting Techniques for Privacy Preserving Publication of Trajectories. *IEEE Transactions on Knowledge and Data Engineering*, v. 29, n. 7, p. 1466–1479, 2017. 2, 3, 4, 21, 22, 25, 26, 36, 37

[Thammarat 2020] THAMMARAT, C. Efficient and Secure NFC Authentication for Mobile Payment Ensuring Fair Exchange Protocol. *Symmetry*, v. 12, n. 10, p. 1649, 2020. 1, 2, 4, 10, 21, 27

[Thanapal, Prabhu e Jakhar 2017] THANAPAL, P.; PRABHU, J.; JAKHAR, M. A survey on barcode RFID and NFC. In: *IOP Conference Series: Materials Science and Engineering*. [S.l.: s.n.], 2017. v. 263, n. 4, p. 042049. 1, 2, 5, 6, 11, 12

[The Apache Software Foundation] The Apache Software Foundation. *Welcome to The Apache Software Foundation!* Disponível em: <https://www.apache.org/>. 20, 32

[The Bootstrap Team] The Bootstrap Team. *Bootstrap.* Disponível em: <https://getbootstrap.com/>. 20, 23

[The PHP Group] The PHP Group. *PHP: Hypertext Preprocessor.* Disponível em: <https://www.php.net/>. 20, 23, 32

[Visioshop] Visioshop. *Tag Veicular Ativo 125khz/433mhz P/controle De Acesso Linear.* Disponível em: <https://www.visioshop.com.br/tag-veicular-ativo-125khz433mhz-pcontrole-de-acesso-linear/p/MLB37459056>. 8

[Zebra Technologies] Zebra Technologies. *Antenas RFID da série AN4X.* Disponível em: <https://www.zebra.com/br/pt/products/rfid/rfid-reader-antennas/an4x-series.html>. 9