Instituto Federal de Brasília
Campus Brasília
Tecnologia em Sistemas para Internet

ARTHUR DAMACENA SILVA, JOÃO PEDRO DELLA ROCCA DE CAMARGOS

IFB ACCESS:

sistema para controle de acesso à instituição utilizando NFC

Brasília
2025

ARTHUR DAMACENA SILVA, JOÃO PEDRO DELLA ROCCA DE CAMARGOS

IFB ACCESS:

sistema para controle de acesso à instituição utilizando NFC

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do *Campus* Brasília do Instituto Federal de Brasília como requisito parcial para obtenção do título de tecnólogo.

Orientador: Prof. Dr. Fábio Henrique M. Oliveira

Brasília
2025

S586 Silva, Arthur Damacena
IFB ACCESS: sistema para controle de acesso à instituição utilizando NFC. / Arthur Damacena Silva, João Pedro Della Rocca de Camargos. – Brasília, 2025.
85 f.: il.

Orientador: Fábio Henrique Monteiro Oliveira.
Trabalho de conclusão de curso (Graduação) – Instituto Federal de Educação, Ciência e Tecnologia de Brasília, Tecnologia em Sistemas para Internet, 2025.

1. Controle de acesso. 2. Arduino (Controlador programável). 3. Android (Recurso eletrônico). I. Camargos, João Pedro Della Rocca de. II. Oliveira, Fábio Henrique Monteiro (orient.). II. Título.

CDU 004.453

Ficha catalográfica elaborada com os dados fornecidos pelo autor.

ARTHUR DAMACENA SILVA, JOÃO PEDRO DELLA ROCCA DE CAMARGOS

IFB ACCESS:

sistema para controle de acesso à instituição utilizando NFC

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do *Campus* Brasília do Instituto Federal de Brasília como requisito parcial para obtenção do título de tecnólogo.

Aprovado em 24 de julho de 2025

BANCA EXAMINADORA

Prof. Dr. Fábio Henrique M. Oliveira
Orientador

Prof. Dr. Caio Moura Daoud
Membro interno

Prof. Dr. João Gabriel Rocha Silva
Membro interno

Ricardo Soares de Brito
Membro externo

AGRADECIMENTOS

Agradecemos às nossas famílias, por toda a paciência e apoio que foram a base para a realização deste trabalho. Aos nossos amigos e namoradas, pela compreensão nas ausências e pelo incentivo constante que nos fortaleceu ao longo desta jornada. Expressamos nossa profunda gratidão ao nosso orientador, Prof. Dr. Fábio Henrique M. Oliveira, não só pela orientação técnica, mas pela paciência e por acreditar em nosso potencial desde o início.

Um agradecimento especial ao Grupo de Pesquisa em Computação Aplicada (GPCA), por fomentar um ambiente de pesquisa e inovação que foi crucial para o desenvolvimento deste projeto. Somos gratos também ao IFMaker CBRA, pelo espaço, ferramentas e suporte que viabilizaram a prototipagem e a construção prática de nossas ideias.

Agradecemos à comissão do projeto e a todos que se disponibilizaram a testar nosso sistema, pois suas contribuições e *feedbacks* foram fundamentais para o aprimoramento do projeto. Por fim, agradecemos à banca examinadora, pela disponibilidade e valiosas considerações, e à instituição, pela parceria e apoio essenciais ao desenvolvimento deste trabalho.

RESUMO

CAMARGOS, João Pedro Della Rocca de; SILVA, Arthur Damacena. **IFB ACCESS:** sistema para controle de acesso à instituição utilizando NFC. 2025. Trabalho de Conclusão de Curso (Graduação) – Tecnologia em Sistemas para Internet. Instituto Federal de Brasília – Campus Brasília. Brasília/DF, 2025.

Diante da crescente preocupação com a segurança em instituições de ensino e da vulnerabilidade gerada por um sistema de controle de acesso inoperante no Instituto Federal de Brasília (IFB), este trabalho teve como objeto de estudo o desenvolvimento e a avaliação do sistema proprietário IFB ACCESS, que utiliza a tecnologia *Near Field Communication* (NFC). O objetivo principal foi desenvolver, implementar e testar um protótipo funcional para aprimorar a segurança no campus, reaproveitando a infraestrutura de catracas existente. A metodologia envolveu a criação de um sistema com hardware baseado em *Arduino* e software composto por um aplicativo *Android* e um servidor com *Docker* e *Flask*. Realizou-se um teste-piloto com 15 usuários da comunidade acadêmica, utilizando o questionário *System Usability Scale* (SUS) e perguntas específicas sobre desempenho para a coleta de dados. Os resultados indicaram excelente usabilidade, com 100% dos participantes afirmando que gostariam de usar o sistema frequentemente e que o consideraram fácil de usar. Conclui-se que o sistema IFB ACCESS demonstrou ser uma solução eficaz, eficiente e de alta satisfação para os usuários, validando a abordagem como uma melhoria viável e autônoma para a segurança institucional.

Palavras-chave: controle de acesso; *Near Field Communication*; *Host Card Emulation*; *Arduino*; *Android*.

ABSTRACT

CAMARGOS, João Pedro Della Rocca de; SILVA, Arthur Damacena. **IFB ACCESS:** access control system for the institution utilizing NFC. 2025. Final Course Work – Technology in Internet Systems. Federal Institute of Brasília – Brasília Campus. Brasília/DF, 2025.

Given the growing concern with security in educational institutions and the vulnerability created by an inoperative access control system at the Federal Institute of Brasília (IFB), this study focused on the development and evaluation of the proprietary system IFB ACCESS, which utilizes Near Field Communication (NFC) technology. The main objective was to develop, implement, and test a functional prototype to enhance campus security by reusing the existing turnstile infrastructure. The methodology involved creating a system with Arduino-based hardware and software composed of an Android application and a server using Docker and Flask. A pilot test was conducted with 15 users from the academic community, using the System Usability Scale (SUS) questionnaire and specific performance questions for data collection. The results indicated excellent usability, with 100% of participants stating they would use the system frequently and considered it easy to use. It is concluded that the IFB ACCESS system proved to be an effective, efficient, and highly satisfactory solution for users, validating the approach as a viable and autonomous improvement for institutional security.

Keywords: access control; Near Field Communication; Host Card Emulation; Arduino; Android.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AID	*Application Identifier*
API	*Application Programming Interface*
API REST	*Application Programming Interface Representational State Transfer*
AWS	*Amazon Web Services*
DER	Diagrama Entidade-Relacionamento
DOM	*Document Object Model*
EC2	*Elastic Compute Cloud*
ECR	*Elastic Container Registry*
GPCA	Grupo de Pesquisa em Computação Aplicada
HCE	*Host-based Card Emulation*
HSU	*High Speed Uart*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
I2C	*Inter-Integrated Circuit*
IFB	Instituto Federal de Brasília
IoT	*Internet of Things*
IP	*Internet Protocol*
JWT	*JSON Web Token*
JSON	*JavaScript Object Notation*
LEDs	*Light Emitting Diode*
MQTT	*Message Queuing Telemetry Transport*
MVC	*Model-View-Controller*
NFC	*Near Field Communication*
P2P	*Peer-to-peer*

RFID	*Radio Frequency Identification*
SGBD	Sistema Gerenciador de Banco de Dados
SQL	*Structured Query Language*
SPI	*Serial Peripheral Interface*
SVG	*Scalable Vector Graphics*
TI	Tecnologia da Informação
UART	*Universal Asynchronous Receiver/Transmitter*
URL	*Uniform Resource Locator*
WSGI	*Web Server Gateway Interface*
SO	Sistema Operacional
QR Code	*Quick Response Code*
XML	*Extensible Markup Language*
MVVM	*Model-View-ViewModel*
BaaS	*Backend-as-a-Service*
NDA	Acordo de Não Divulgação
AD	*Active Directory*
MB	*megabyte*

SUMÁRIO

1 INTRODUÇÃO

A segurança é uma grande preocupação em instituições de ensino, especialmente diante das consequências negativas provocadas por entradas não autorizadas em escolas desprovidas de um sistema eficaz para o controle de acesso de pessoas[1]. Segundo dados recentes, apenas em 2023, foram registrados 9 ataques a escolas no país, atingindo um patamar recorde[2]. Desde 2000 até 2022, ocorreram 16 ataques, resultando em 35 óbitos e 72 feridos[3]. Essa ascensão nos casos de violência evidencia uma lacuna crítica na segurança das instituições educacionais brasileiras, incluindo o Instituto Federal de Brasília (IFB), que possui um sistema de controle de acesso fragilizado e subutilizado.

Na área de segurança, o controle de acesso envolve a aplicação de procedimentos, dispositivos e sistemas para gerenciar o fluxo de pessoas, objetos e informações em um meio físico ou digital. Esse controle visa garantir a proteção adequada e a restrição de acesso apenas a indivíduos autorizados[4].

Garantir um ambiente de aprendizado seguro para todos os envolvidos alunos, funcionários, responsáveis e visitantes é uma prioridade fundamental no contexto da segurança acadêmica. Embora as ameaças cibernéticas recebam grande atenção, as medidas de segurança física continuam desempenhando um papel essencial na prevenção de crimes e no controle de acesso às instituições educacionais. A implementação de um sistema de controle de acesso eficaz em escolas e universidades é uma solução indispensável para garantir a segurança e o bem-estar de todos os frequentadores do espaço. Além de proteger a integridade física das pessoas, esse tipo de sistema também contribui para a preservação dos ambientes, a segurança dos equipamentos e a proteção do patrimônio[5].

O IFB demonstra sua preocupação com a segurança ao ter investido no passado em um sistema de controle de acesso baseado em catracas eletrônicas equipadas com leitores *Near Field Communication* (NFC) e *Radio Frequency Identification* (RFID), implantado por uma empresa terceirizada. Contudo, o término do contrato com essa empresa comprometeu a funcionalidade do sistema, uma vez que sua operação e manutenção dependiam diretamente do vínculo contratual. Essa situação evidenciou fragilidades no controle de acesso, levantando preocupações significativas sobre a segurança institucional. Diante deste cenário, surgiu a necessidade de desenvolver uma solução para sanar essas limitações, motivando a realização do presente trabalho.

No atual cenário do IFB, a instituição dispõe de catracas eletrônicas inoperantes que contam com leitores NFC e RFID instalados. As catracas têm o propósito de serem utilizadas para controlar e registrar os acessos; os cartões do tipo RFID existentes são usados apenas quando um visitante da comunidade externa se identifica na portaria. Além disso, o software utilizado para gerenciar as catracas se encontra inacessível para manutenção e alteração na codificação por parte da instituição, por pertencer a uma empresa privada que não

concedeu o acesso.

Com essa realidade, os funcionários que possuem o papel de controlar o acesso não possuem meios automáticos e eficazes para verificar se os indivíduos que entram na instituição possuem autorização para tal, e os desenvolvedores do IFB ACCESS, juntos com a instituição, optaram por criar software e hardware próprios.

É importante ressaltar que a falta de controle de acesso não apenas compromete a segurança das pessoas e dos recursos materiais dentro do Campi, mas também representa um risco potencial para toda a comunidade interna e externa[6]. Nesse sentido, é crucial reaproveitar os recursos já dispostos pela instituição para implementar um sistema de controle de acesso pensado nas particularidades e na realidade da instituição, que seja seguro e eficiente com o propósito de mitigar esses riscos.

Com a expansão e popularização dos dispositivos computadorizados, a tecnologia móvel tem desempenhado um papel crucial na vida de todos os indivíduos no desenvolvimento de um cenário altamente interligado que é popularmente chamado de *Internet of Things* (IoT), que tem como principal característica a conexão entre dispositivos computacionais que estão presentes na rotina das pessoas, não se limitando somente a computadores e *smartphones*, mas também a qualquer aparelho eletroeletrônico que possa de alguma forma receber comandos e gerar informações[7].

Propõe-se, assim, a utilização dos recursos já instalados no IFB como a catraca e a infraestrutura de cabos de energia e rede para criação de um sistema para controle de acesso baseado em IoT utilizando NFC como método de identificação do usuário que utilizará as catracas, permitindo a conexão sem fio entre dispositivos que possuem a tecnologia e o leitor NFC. Essa conexão acontecerá entre as catracas eletrônicas da portaria e os dispositivos móveis dos usuários baseados em *Android*. Ao empregar o NFC, os usuários podem utilizar seus dispositivos móveis para autenticar e autorizar o acesso às dependências do Instituto.

Diante desse cenário, este (TCC) tem como objetivo contribuir para a melhoria da segurança do Instituto Federal de Brasília Campus Brasília, ao desenvolver um sistema de controle de acesso. A proposta inclui projetar, desenvolver um protótipo, implantar e testar um sistema próprio, utilizando os recursos já disponíveis na instituição, para garantir maior autonomia na manutenção, no uso e na gestão do controle de acesso. Assim, buscando solucionar a inutilização das catracas e dos leitores NFC, visando promover melhorias na segurança, na proteção dos usuários e na preservação dos recursos do IFB. Com uma tecnologia desenvolvida internamente, será possível ter controle total sobre o funcionamento do sistema, permitindo adaptações conforme as necessidades da instituição.

1.1 Tema

Qual a contribuição positiva na segurança do IFB ao implementar um sistema de controle de acesso via NFC e a sua viabilidade com base em um estudo de caso realizado

na Instituição por meio do teste de um protótipo funcional.

1.2 Problema

Atualmente, o sistema de controle de acesso do IFB encontra-se inoperante, subutilizado e inacessível tanto no uso quanto na manutenção, impedindo que a instituição aproveite os benefícios esperados desse equipamento. A dependência de uma empresa terceirizada para o funcionamento e manutenção do sistema tornou-se um obstáculo crítico após o encerramento do contrato e do vínculo com o IFB. Essa ausência de um sistema eficaz de controle de acesso configura uma falha significativa que compromete diretamente a segurança do patrimônio e dos usuários nas dependências da instituição.

A situação é ainda mais preocupante diante do aumento expressivo de ataques a escolas no Brasil[2]. A falta de um controle de acesso funcional pode resultar em riscos como acessos não autorizados, ameaças à integridade física de estudantes e funcionários, além de possíveis danos ao patrimônio.

Diante disso, é essencial tornar operante o sistema de controle de acesso já implantado no IFB, utilizando os recursos existentes e desenvolvendo hardware e software próprios para maximizar o aproveitamento dos bens tecnológicos disponíveis, como as catracas e infraestrutura de rede e elétrica, com o fim de permitir uma solução voltada para o contexto específico da instituição e mitigar os riscos que a falta de um sistema de controle de acesso operante traz ao IFB.

1.2.1 Objetivo geral

Contribuir para a melhoria da segurança do Instituto Federal de Brasília - Campus Brasília, ao desenvolver um sistema de controle de acesso baseado na tecnologia NFC.

1.2.2 Objetivos específicos

- Explorar a viabilidade de implementar um sistema tecnológico, levando em consideração os recursos presentes, o custo das tecnologias implementadas, o número de dispositivos que possuem a tecnologia NFC e a adesão do sistema por parte dos usuários.
- Desenvolver um sistema para controle de acesso no IFB utilizando NFC em dispositivos móveis baseados em Android.
- Implementar o protótipo funcional do sistema de controle de acesso no ambiente do IFB.
- Analisar e registrar o impacto da tecnologia NFC no acesso, eficiência e segurança na comunidade do IFB.

1.3 Estrutura do TCC

Este trabalho está estruturado em 5 capítulos, organizados de forma a proporcionar uma compreensão clara e lógica do desenvolvimento do projeto IFB ACCESS. A seguir, apresenta-se um resumo de cada capítulo:

No primeiro capítulo é apresentada a contextualização do tema, destacando a importância da segurança em instituições de ensino, a problemática da ausência de um sistema eficaz de controle de acesso no IFB e como a tecnologia pode contribuir com a segurança. São definidos o tema, o problema de pesquisa, os objetivos gerais e específicos do projeto, bem como a justificativa da escolha do tema e sua relevância.

No segundo capítulo, são apresentados os conceitos teóricos fundamentais para a compreensão do projeto. Este capítulo inclui uma revisão da literatura sobre tecnologias de controle de acesso, com foco em RFID e NFC, além de uma análise de trabalhos similares já existentes. A revisão visa contextualizar o projeto dentro do cenário atual e destacar as contribuições esperadas do IFB ACCESS.

No terceiro capítulo é descrito detalhadamente as metodologias adotadas para o desenvolvimento do sistema IFB ACCESS. São abordados o levantamento de requisitos, a estrutura do sistema e o desenvolvimento do software e hardware. A metodologia é apresentada de forma a garantir a replicabilidade do projeto e a transparência dos processos utilizados.

No quarto capítulo, intitulado Resultados e Discussão, são expostos os resultados práticos do projeto. Esta seção detalha os artefatos desenvolvidos, como o aplicativo móvel e o hardware do leitor, apresenta os dados coletados durante o teste-piloto com os usuários, incluindo a análise de usabilidade, e, por fim, discute os achados, contextualizando-os com os trabalhos correlatos da literatura.

No quinto e último capítulo, são apresentadas as considerações finais, onde se retoma os objetivos do trabalho, sintetiza-se as conclusões alcançadas a partir dos resultados e se destacam as contribuições do projeto. Adicionalmente, são propostas sugestões para trabalhos futuros, indicando possíveis caminhos para a evolução e expansão do sistema IFB ACCESS.

1.3.1 Classificação da Pesquisa

O projeto adota uma abordagem aplicada, buscando implementar e avaliar um sistema de acesso baseado em NFC nas dependências do IFB. Com uma metodologia mista, combinando elementos quantitativos e qualitativos, o estudo se concentra em uma abordagem transversal para analisar a eficiência, segurança, inclusão social e responsabilidade ambiental proporcionadas pelo novo sistema. Com objetivos exploratórios e descritivos, a pesquisa visa entender o contexto do controle de acesso no IFB, descrever o funcionamento e os impactos da tecnologia NFC e estimar sua eficácia após os testes. Os dados serão

obtidos tanto por meio de observações, testes e análises durante a implantação do sistema, quanto por pesquisas, entrevistas e estudo de casos.

2 CONCEITOS GERAIS E REVISÃO DA LITERATURA

Nesta seção, são apresentados os conceitos básicos e revisão de literatura indispensáveis para a compreensão deste trabalho.

2.1 Revisão da literatura

Nesta revisão, são explorados os conceitos e as aplicações do controle de acesso por meio da tecnologia NFC em sistemas semelhantes. O objetivo é não apenas apresentar um panorama das soluções que já existem, mas também destacar as inovações que estão sendo propostas neste estudo. Ao comparar o NFC com outras tecnologias de controle de acesso, oferece-se uma compreensão mais clara das vantagens e limitações de cada uma dessas abordagens.

Os trabalhos correlatos foram levantados por meio de pesquisas realizadas no Google Acadêmico e na base de dados Scopus, utilizando palavras-chave "Controle de acesso", "NFC", "Near Field Communication"e "Host-Card Emulation". As buscas foram realizadas considerando publicações entre os anos de 2013 a 2022. Os resultados dessas pesquisas estão detalhados no Quadro 1.

Quadro 1 – Trabalhos selecionados a partir da revisão da literatura

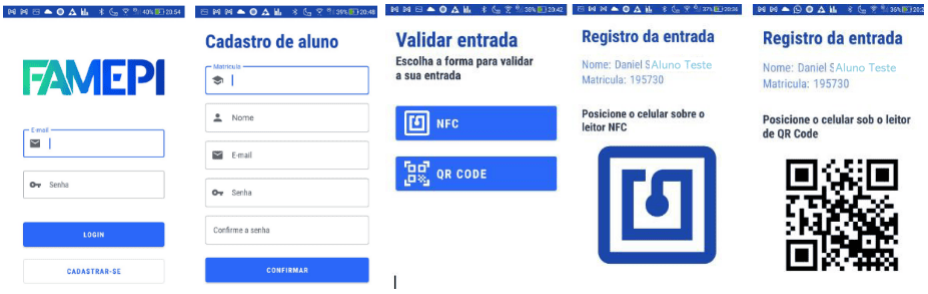
Título	**Ano**	**Palavras-chave**	**Citação**
Controle de acesso para estádios de futebol utilizando tecnologia NFC	2013	NFC, Automação de estádios, Wireless	Palmeira e Fernandes[8]
Implementation of host card emulation mode over Android smartphone as alternative ISO 14443A for Arduino NFC shield	2015	Android smartphone, NFC technology, Host-based Card Emulation mode, Smartcard, ISO 14443A	Basyari *et al.*[9]
Proposta de controle de acesso e rotina hospitalar baseado em NFC e banco de dados	2016	NFC, Tag, Banco de Dados, Rotina Hospitalar	Souza e Martins[10]
Sistema de controle de acesso via RFID/NFC	2019	RFID, NFC, ESP32, MQTT, Internet das Coisas, Android	Bispo[11]
Sistema para controle de acesso à universidade utilizando NFC e QR Code	2022	Arduino, Android, NFC, QR Code, automação do controle de acesso	Silva *et al.*[12]
IF ACCESS: Sistema de controle de acesso eletrônico utilizando tecnologia RFID e Microcontrolador	2022	Controle de Acesso, Microcontrolador, RFID, Sistemas Embarcados	Silva[13]

Fonte: elaborado pelos autores.

2.1.1 Trabalhos similares

O artigo publicado em 2022 na revista *Brazilian Journal of Development* intitulado Sistema para controle de acesso à universidade utilizando NFC e *Quick Response Code (QR Code)*[12], visa desenvolver um sistema de controle de acesso para universidades utilizando as tecnologias NFC e QR Code. A Figura 1 ilustra telas do sistema de controle de acesso móvel, incluindo etapas de cadastro, validação de entrada via NFC ou QR Code, e confirmação de acesso. O projeto foi implementado com o uso do da placa de prototipagem Arduino e programação em linguagem C. O sistema permite a identificação e autenticação de usuários por meio de dispositivos móveis, oferecendo duas opções de acesso: via leitura de QR Codes ou por meio de dispositivos NFC. Esse artigo indica que as tecnologias RFID e NFC têm sido efetivamente aplicadas em sistemas de controle de acesso no Brasil, oferecendo soluções que aumentam a segurança, automatizam processos e permitem o monitoramento em tempo real. A integração dessas tecnologias com plataformas da Internet das Coisas e sistemas de gerenciamento demonstra seu potencial benéfico para atender às diferentes demandas institucionais e corporativos.

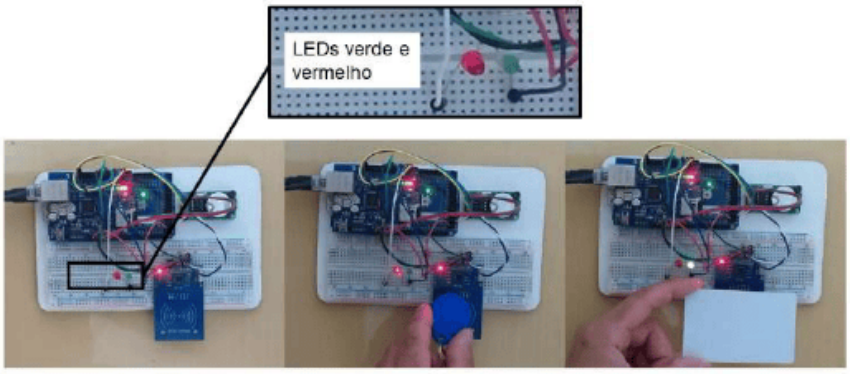
Figura 1 – Telas do aplicativo de acesso



Fonte: Silva *et al.*[12].

Em 2022, Silva[13] desenvolveu o projeto IF Access, visando otimizar o controle de acesso no Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande. O IF Access propõe o desenvolvimento de um sistema para o controle de acesso no ambiente institucional, utilizando RFID em conjunto com microcontroladores. A proposta se insere em um contexto em que soluções eletrônicas para autenticação e restrição de acesso têm se diversificado, com o NFC ganhando crescente destaque por sua praticidade e integração com dispositivos móveis. O IF Access é constituído por pontos de acesso microcontrolados (baseados no Arduino Mega ADK), leitores RFID (modelo MFRC522) e uma infraestrutura de comunicação que utiliza um protocolo de mensagens leve para dispositivos da internet das coisas intitulado *Message Queuing Telemetry Transport* (MQTT) para troca de dados com um sistema de gerenciamento *web*. A Figura 2 ilustra o protótipo com um leitor RFID demonstrando o uso de um cartão e um chaveiro RFID para acionar LEDs indicativos. Cada usuário possui uma tag RFID (cartão ou chaveiro) previamente cadastrada no sistema, a qual é lida no momento da autenticação. Com base no horário e na permissão atribuída ao usuário, o sistema libera ou nega o acesso ao ambiente correspondente. A principal inovação do IF Access está na sua arquitetura distribuída com microcontroladores e integração via MQTT, permitindo escalabilidade, independência da rede central em casos de falha e gestão *web* eficiente. Sua estrutura de código aberto e uso de hardware de fácil aquisição viabiliza adaptações futuras, como a substituição de leitores RFID por módulos NFC, tornando possível a autenticação direta via *smartphones*. O IF Access se mostra solução inovadora no controle de acesso em instituições públicas, ao combinar flexibilidade técnica, acessibilidade e segurança. Sua infraestrutura baseada em RFID já se mostra funcional, e sua compatibilidade com a tecnologia NFC amplia suas possibilidades de aplicação.

Figura 2 – Circuito e testes realizados



Fonte: Silva[13].

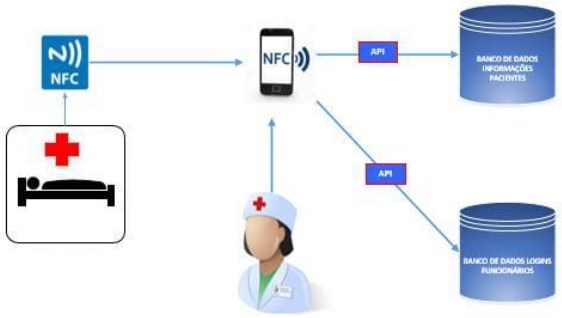
O trabalho desenvolvido por Bispo[11] em 2019, é um sistema de controle de acesso que integra tecnologias RFID e NFC com conceitos modernos da Internet das Coisas (IoT) e na utilização do NFC como meio de autenticação via *smartphones*. O sistema é composto por um ESP32, leitores PN532, protocolo MQTT para comunicação em rede, e interface gráfica construída com Node-RED. A integração com banco de dados MySQL permite o registro e controle dos acessos em tempo real. Um dos principais diferenciais do sistema é o uso do aplicativo *Android* iTAG, que utiliza a funcionalidade de Emulação de Cartão via *Host-based Card Emulation* (HCE), permitindo que o usuário utilize seu *smartphone* como uma credencial NFC válida para acessar ambientes controlados. A Figura 3 ilustra a aplicação do projeto no Laboratório de Interface Homem-Máquina (LIHOM) da UFPE, onde professores e alunos utilizaram etiquetas RFID e o aplicativo iTAG para acessar o laboratório. Os testes realizados no LIHOM demonstraram o funcionamento do sistema em um ambiente real, isolado e controlado, destacando sua capacidade de registrar e gerenciar o acesso de usuários de forma eficiente e segura. As principais inovações apresentadas no sistema é a emulação de cartão via *smartphone*, utilizando o protocolo HCE, eliminando a necessidade de credenciais físicas como TAG e Cartões RFID, a arquitetura modular baseada em fila com o protocolo MQTT, o uso de Node-RED como solução para criação de uma interface de supervisão administrativa, e por fim, a topologia do servidor pode ser embarcada, o que torna o sistema simples e barato de ser produzido, no que diz respeito ao valor comercial de todo o sistema, incluindo *hardware* e *software* utilizados.

Figura 3 – Implantação do sistema de controle de acesso na porta do laboratório

Fonte: Bispo[11]

O trabalho de Souza e Martins[10] realizado em 2016, propõe um sistema de controle de acesso e gerenciamento de rotina hospitalar fundamentado na tecnologia NFC, com suporte de um banco de dados remoto. Seu foco é específico no ambiente hospitalar, mais precisamente na automação da rotina de trabalho da enfermaria, tornando mais ágil, segura e rastreável a coleta e consulta de dados clínicos dos pacientes. O sistema é pensado para funcionar em um hospital, onde cada leito possui uma *tag* NFC associada. O acesso às informações clínicas é realizado por profissionais autorizados por dispositivos móveis com NFC, os quais interagem com as *tags* dos leitos para consultar ou inserir dados no banco de dados, como pode ser observado na Figura 4. Este ambiente foi escolhido por ser sensível à necessidade de controle rigoroso, rapidez no acesso à informação e segurança de dados. Embora o sistema não tenha sido plenamente implementado em ambiente real por limitações de desenvolvimento do aplicativo, foram realizados testes simulando a leitura e gravação de *tags* NFC. Foi utilizado o aplicativo *NFC Tools* para demonstrar a gravação de identificadores únicos em cada *tag*, a leitura bem sucedida dessas informações por diferentes dispositivos capazes de se comunicar por NFC e a proteção das informações da *tag* via senha. Na conclusão, foi destacado que o sistema, mesmo em nível de protótipo, demonstrou potencial para ser expandido e aplicado de forma prática. A utilização de tecnologias acessíveis e de fácil integração utilizadas no trabalho tornam o sistema replicável e adaptável a outras instituições. É sugerido como trabalhos futuros o desenvolvimento de um aplicativo próprio que integre a leitura das *tags* ao banco de dados de forma automatizada e segura.

Figura 4 – Diagrama do sistema de controle de acesso às informações dos pacientes e rotina hospitalar

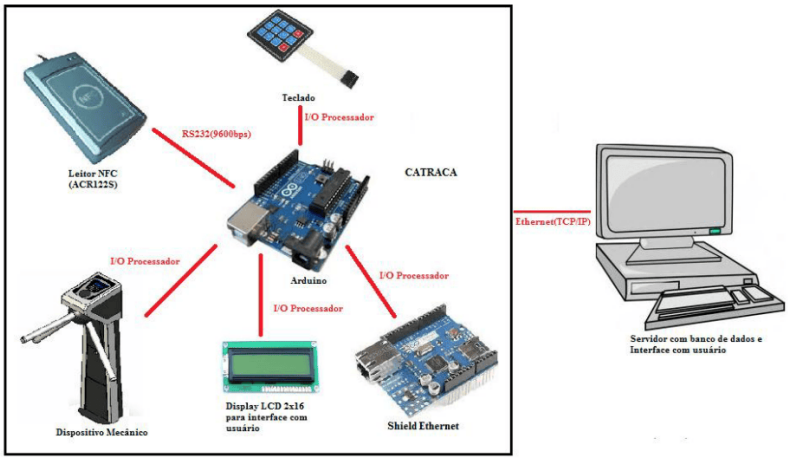


Fonte: Souza e Martins[10]

Outro artigo encontrado intitulado *Implementation of Host Card Emulation Mode Over Android Smartphone as Alternative ISO 14443A for Arduino NFC Shield* de Basyari *et al.*[9], apresentado na *International Conference on Control, Electronics, Renewable Energy and Communications* (ICCEREC) em 2015, teve como objetivo desenvolver um sistema de substituição de cartões inteligentes e chaves físicas por *smartphones* habilitados com a tecnologia NFC em modo de *Host-based Card Emulation* (HCE). O estudo detalha a implementação de um aplicativo Android que permite que o smartphone funcione como um cartão inteligente, comunicando-se com um leitor NFC construído com a placa de prototipagem Arduino UNO e um *shield* NFC PN532, utilizando o padrão ISO 14443A. O principal benefício identificado é a conveniência e a praticidade para os usuários, que podem utilizar seus *smartphones* em vez de múltiplos cartões ou chaves físicas. A implementação do modo HCE no *Android* a partir da versão 4.4 (KitKat) foi fundamental para o desenvolvimento deste sistema.

Em 2013, Palmeira e Fernandes[8] propôs um sistema de controle de acesso para estádios de futebol utilizando a tecnologia NFC. O projeto, cuja arquitetura é apresentada na Figura 5, apresenta uma solução completa que envolve o cadastro prévio dos usuários, cujas informações são armazenadas em um banco de dados. O sistema é composto por três pilares principais: um banco de dados, um sistema gerenciador que realiza a interface com as catracas e as próprias catracas. A comunicação entre as catracas e o sistema gerenciador ocorre via rede Ethernet, utilizando o protocolo *TCP/IP*. A aplicação é desenvolvida em C#, o *firmware* em C e o banco de dados em *Structured Query Language* (SQL).

Figura 5 – Representação ilustrativa do sistema



Fonte: Palmeira e Fernandes[8]

Os trabalhos revisados apresentam boas soluções para controle de acesso em diversos contextos, utilizando as tecnologias RFID e NFC. Entretanto, o IFB ACCESS destaca-se por características únicas. Enquanto os projetos analisados concentram-se em propostas, protótipos ou testes em ambientes isolados, o IFB ACCESS será implementado e avaliado em um cenário próximo ao funcionamento real do Instituto. Isso permitirá uma análise prática da viabilidade e da eficiência do sistema, além de medir seu impacto no controle de acesso e na segurança do IFB. Serão avaliadas a capacidade de reconhecimento de credenciais, a satisfação e adoção pelos usuários, bem como o monitoramento da disponibilidade do sistema e do consumo de recursos.

Uma das inovações do IFB ACCESS é a integração completa com dispositivos móveis *Android*, que utilizará a tecnologia NFC para autenticação e autorização de acesso. Essa abordagem não apenas moderniza o sistema, mas também aumenta a conveniência para os usuários, eliminando a necessidade de cartões físicos para o funcionamento íntegro do sistema.

Além do desenvolvimento e da implementação do sistema, este trabalho busca realizar uma análise do impacto da tecnologia NFC na segurança e eficiência da instituição. Serão considerados aspectos como custo de implementação, número de dispositivos compatíveis e a adoção do sistema pelos usuários, proporcionando uma visão abrangente sobre a viabilidade do projeto.

2.2 Tecnologias

Nesta seção, são apresentadas as tecnologias utilizadas para o desenvolvimento de um sistema de acesso utilizando NFC.

2.2.1 Near Field Communication (NFC)

A tecnologia *Near Field Communication*, traduzida como comunicação por campo de proximidade, representa uma das inovações mais relevantes da comunicação sem fio de curta distância, tendo sido oficialmente desenvolvida em 2002 como resultado de um esforço conjunto de empresas líderes no setor tecnológico, mais especificamente a *Sony Corporation*, do Japão, e a *NXP Semiconductors*, dos Países Baixos, anteriormente uma divisão da *Philips*[14].

O NFC é uma evolução direta da tecnologia RFID, projetada para *smartphones* e dispositivos capazes de trocar dados por meio de ondas de rádio. No entanto, ao contrário do RFID, o NFC oferece um nível mais elevado de segurança. A comunicação ocorre a uma distância máxima de apenas alguns centímetros. Os dispositivos equipados com essa tecnologia contêm um *microchip* com memória suficiente para armazenar dados, o que possibilita uma ampla gama de aplicações[15].

Nos últimos anos, a tecnologia NFC tem ganhado destaque devido às suas aplicações inovadoras em diversos setores[16]. Sua versatilidade é especialmente evidente na área de segurança, destacando-se em duas frentes principais: a otimização de processos gerenciais, permitindo o cadastramento automático e a identificação em tempo real de usuários; e os sistemas de controle de acesso, que revolucionam a entrada segura em edifícios e áreas restritas por meio do uso de smartphones ou cartões inteligentes[17]. Essas aplicações demonstram como o NFC está transformando a gestão de segurança e acesso em ambientes corporativos e institucionais, ao oferecer soluções mais eficientes e seguras que combinam praticidade e proteção avançada.

O NFC pode operar de três maneiras distintas: leitura/gravação, *peer-to-peer* (P2P) e HCE. No modo emulação HCE[18], que será utilizado no desenvolvimento deste projeto, o *smartphone* pode atuar como um cartão, armazenando dados únicos e interagindo com um leitor NFC. Na Figura 6 pode se observar os funcionamentos possíveis da tecnologia NFC.

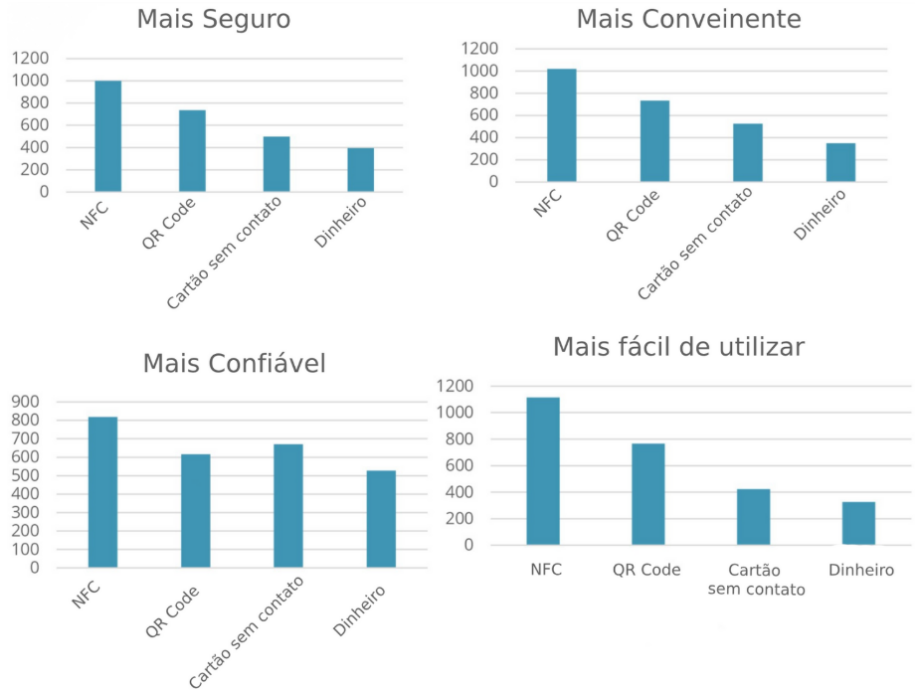
Figura 6 – Modos de funcionamento do NFC

Fonte: Adaptado de Bispo[11].

A escolha do NFC como tecnologia central para o IFB ACCESS foi motivada, primeiramente, pela infraestrutura já existente na instituição, que contava com catracas equipadas com leitores NFC inoperantes. A decisão de desenvolver um novo sistema próprio, reaproveitando este *hardware*, é fortemente justificada pela crescente adoção e percepção positiva do NFC por parte dos usuários, em detrimento de alternativas como cartões físicos (RFID) ou *QR Codes*.

Uma pesquisa de 2024 realizada pela *ABI Research* para o *NFC Forum*, que ouviu 2.632 usuários de tecnologia sem contato em 9 países (incluindo EUA, Europa, China, Japão e Coreia do Sul), comparou a percepção de diferentes métodos de transação. É importante notar que a pesquisa filtrou os participantes, incluindo apenas aqueles que já utilizavam pagamentos por aproximação com *smartphone*[19]. Os resultados, apresentados na Figura 7, demonstram uma clara preferência pelo NFC.

Figura 7 – Gráficos comparativos da percepção de usuários sobre diferentes métodos de pagamento



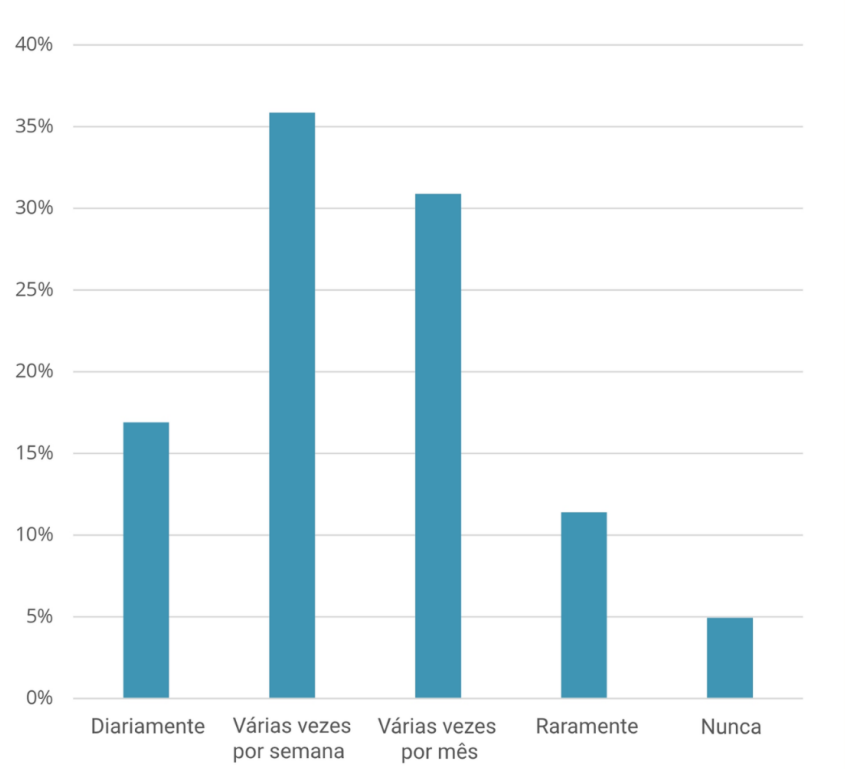
Fonte: Traduzido de NFC Forum Survey Results[19].

Como os gráficos ilustram, os pagamentos por NFC (utilizando *smartphones*) foram classificados em primeiro lugar em todas as quatro categorias avaliadas, superando *QR Code*, cartão sem contato e dinheiro:

- **Mais Seguro:** 38% dos entrevistados classificaram o NFC como o método mais seguro, contra 28% do *QR Code* e 19% do cartão sem contato.
- **Mais Conveniente:** 39% dos entrevistados preferiram o NFC, comparado a 28% do *QR Code* e 20% do cartão sem contato.
- **Mais Fácil de Utilizar:** 42% dos entrevistados consideraram o NFC o mais fácil, contra 29% do *QR Code* e 16% do cartão sem contato.
- **Mais Confiável:** 31% dos entrevistados classificaram o NFC como o mais confiável, superando o cartão sem contato (25%) e o *QR Code* (23%).

Essa percepção de superioridade em segurança, conveniência e facilidade de uso é um indicador crucial, pois esses são atributos essenciais para um sistema de controle de acesso. A confiança do usuário na tecnologia é fundamental para a adesão ao sistema. A pesquisa também mediu a dependência dos usuários de suas credenciais digitais. A Figura 8 demonstra a frequência com que os entrevistados relataram sair de casa levando apenas seus dispositivos móveis (*smartphone*) e deixando a carteira física.

Figura 8 – Frequência em que os usuários deixam a carteira em casa



Fonte: Traduzido de NFC Forum Survey Results[19].

Os dados revelam uma forte migração para soluções digitais. A pesquisa apontou que 95% dos entrevistados já saíram de casa sem a carteira física ao menos uma vez, e mais da metade (53%) faz isso "várias vezes por semana"ou "diariamente".

2.2.2 Plataforma de prototipagem

O Arduino é uma plataforma de prototipagem amplamente utilizada em projetos eletrônicos, composta por um microcontrolador e um ambiente de desenvolvimento integrado que facilita tanto a programação quanto a transferência de códigos para o microcontrolador. É capaz de controlar desde simples *Light Emitting Diode* (LEDs) até sensores e motores. Isso torna o Arduino uma ferramenta versátil para prototipagem e desenvolvimento de sistemas embarcados[20].

2.2.3 Linguagem de programação Python

O Python é uma linguagem de programação, amplamente utilizada em várias áreas, como desenvolvimento *web*, ciência de dados, automação, inteligência artificial e educação. É conhecido por sua facilidade de uso e legibilidade de código. Permite a criação de programas de forma eficiente e fácil de entender, é uma escolha popular tanto para programadores iniciantes quanto para programadores experientes[21]. Além disso, o Python

é uma ferramenta poderosa para uma variedade de aplicações devido aos seus frameworks, como, por exemplo, o Flask para desenvolvimento *web* e à abundância de bibliotecas disponíveis[22].

2.2.4 Framework Flask

O Flask é um *framework* eficaz para o desenvolvimento de aplicações *web* em Python. Ele é conhecido por sua facilidade de uso e simplicidade, o que o torna ideal para criar desde *Application Programming Interface* (APIs) simples até aplicações *web* complexas. O Flask permite a criação de rotas para vários *Uniform Resource Locator* (URLs), criação de *templates HyperText Markup Language* (HTML), gerenciamento de formulários, autenticação de usuários e conexão a bancos de dados. Sua estrutura extensível e modular permite a integração de várias extensões para funcionalidades adicionais como autenticação *JSON Web Token* (JWT) e envio de e-mails[23].

2.2.5 Desenvolvimento móvel com Kotlin

Kotlin é uma linguagem de programação moderna, concisa e de código-aberto desenvolvida pela JetBrains que surgiu em meados de 2011, com sua primeira versão estável em 2016. Tem-se tornado popular, especialmente no contexto do desenvolvimento de aplicativos Android, devido à sua integração perfeita com a plataforma, melhor legibilidade e redução dos códigos em comparação com o Java. O seu uso foi expandido especialmente a partir de 2017, quando havia sido anunciado pelo Google como nova linguagem oficial para o desenvolvimento de aplicativos Android[24]. Outra característica é sua capacidade de ser multiplataforma. Isso significa que é possível utilizar o mesmo código para desenvolver aplicativos para ambos sistemas operacionais Android e iOS.

2.2.6 Arquitetura de Software com Model-View-ViewModel (MVVM)

A arquitetura Model-View-ViewModel (MVVM) foi adotada como o padrão de design para a aplicação, visando uma clara separação de responsabilidades e uma estrutura de código mais organizada e sustentável. Neste padrão, a aplicação é dividida em três componentes principais: o Model, que representa os dados e a lógica de negócio; a View, responsável pela interface do utilizador (UI) e pela captura das suas interações; e o ViewModel, que atua como intermediário, expondo os dados do Model para a View e tratando a lógica de apresentação. Essa separação desacopla a UI da lógica de negócio, o que melhora significativamente a manutenibilidade e a testabilidade do código[25].

2.2.7 Framework HTTP Ktor

Ktor é um *framework* de cliente HTTP multiplataforma desenvolvido pela *JetBrains*. Sua função é atuar como a camada de comunicação com um servidor, como uma *API*

REST. Construído com foco primário em Kotlin (*Kotlin-first*), o *Ktor* utiliza as *Coroutines* da linguagem para o gerenciamento de operações de rede assíncronas. A sua *API* é projetada para a criação de clientes HTTP e a estruturação de requisições e respostas, abstraindo detalhes da implementação da rede[26].

2.2.8 Interface de usuário com Jetpack Compose

Jetpack Compose é o moderno *toolkit* do *Android* para a construção de interfaces de usuário (UI) nativas. Sua abordagem é fundamentada em um paradigma declarativo, o que significa que o desenvolvedor descreve como a UI deve se apresentar em um determinado estado de dados. A interface é construída a partir de funções escritas em *Kotlin*, anotadas com `@Composable`, que definem as diferentes partes da tela. Quando o estado da aplicação muda, o *framework* do *Compose* se encarrega de atualizar a UI para refletir essas mudanças, um processo conhecido como recomposição[27]

2.2.9 Firebase

O *Firebase* é uma plataforma de desenvolvimento de aplicações mantida pelo *Google*, que opera no modelo de *Backend-as-a-Service (BaaS)*. Seu objetivo é fornecer um conjunto de ferramentas e serviços gerenciados que auxiliam os desenvolvedores em diferentes estágios do ciclo de vida de uma aplicação, desde a construção até o monitoramento e o engajamento de usuários. A plataforma é composta por um conjunto de serviços independentes, mas que podem ser integrados entre si[28].

O serviço pensando para a aplicação móvel é o *Firebase Authentication* que é dedicado especificamente à gestão de identidade e autenticação de usuários. Sua função é fornecer uma solução completa para o processo de login, registro e gerenciamento de contas de usuários em uma aplicação[29]. As principais funcionalidades do serviço incluem:

- **Múltiplos Provedores de Autenticação:** O serviço suporta diversos métodos para que o usuário possa se autenticar:
  - **Email e Senha:** O sistema tradicional de registro com um endereço de email e uma senha.
  - **Provedores Federados (Login Social):** Integração com provedores de identidade de terceiros, como Google, Facebook, Apple, GitHub, Twitter, entre outros.
  - **Login Anônimo:** Permite criar contas temporárias para usuários que ainda não se registraram, possibilitando que eles utilizem a aplicação e convertam a conta para uma permanente posteriormente.
  - **Autenticação por Telefone:** Validação de usuários através de um código enviado por SMS.
  - **Login por Link de Email:** Permite que o usuário faça login clicando em um link seguro enviado para seu email, sem a necessidade de uma senha.

- **Gerenciamento de Sessão:** Após a autenticação, o Firebase Authentication gerencia a sessão do usuário, fornecendo à aplicação cliente um token de identificação (ID Token). Este token é utilizado para verificar a identidade do usuário em requisições subsequentes, tanto no cliente quanto em um backend seguro.

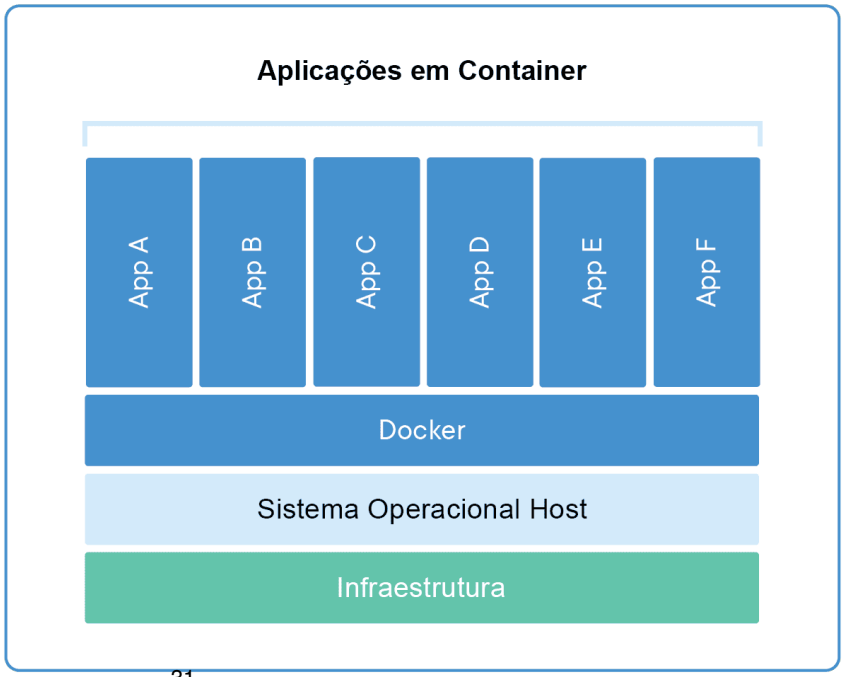
2.2.10 Docker/Containers

O Docker é uma plataforma de *software* aberta que facilita o empacotamento, a distribuição e a execução de aplicações em *containers*, proporcionando isolamento e consistência entre ambientes de desenvolvimento, teste e produção. Ele foi projetado para agilizar o ciclo de vida de serviços, aproveitando recursos do sistema operacional do *host*, sem depender diretamente de configurações de *hardware* ou de acesso privilegiado à infraestrutura física.

Um dos principais benefícios do Docker é a sua portabilidade. As aplicações empacotadas em *containers* Docker podem ser executadas em qualquer sistema que suporte o *runtime* do Docker, sem necessidade de alterações no código ou no ambiente. Isso se deve ao isolamento fornecido por *namespaces*(sistema de arquivos, processos, rede, usuários) e *cgroups*(controle de consumo de CPU, memória e I/O), que garante comportamento previsível em diferentes hosts.

Outra vantagem do Docker é a sua agilidade. A criação e inicialização de *containers* normalmente ocorre em poucos segundos, pois eles compartilham o *kernel* do *host* e não exigem a emulação completa de *hardware*, ao contrário de máquinas virtuais. Essa leveza e rapidez de *boot* tornam o Docker ideal para fluxos de integração contínua, testes automatizados e entrega contínua de aplicações[30].

Figura 9 – Visão geral de aplicações em containers com Docker



Fonte: Docker[31].

3 METODOLOGIA

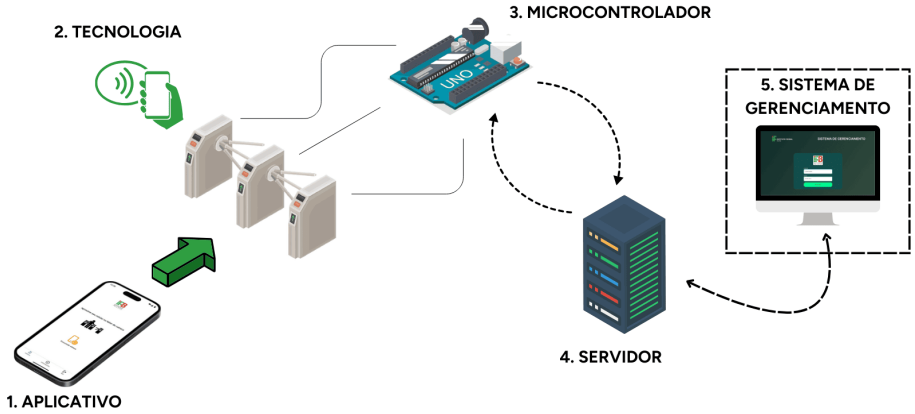
Este capítulo expõe as metodologias utilizadas na elaboração do sistema para controle de acesso. Nesse cenário, esta seção se propõe a explicar de modo técnico como as tecnologias foram aplicadas na construção do sistema e quais foram os obstáculos e objeções durante as etapas do desenvolvimento.

3.1 Visão geral do projeto

Antes de desenvolvermos qualquer tipo de protótipo ou implementação, é necessário abstrair todo o sistema, considerando desde o aplicativo e o leitor, até as catracas e a comunicação com o servidor. Isso é fundamental para definirmos quais ferramentas e tecnologias serão utilizadas para o desenvolvimento do sistema.

A Figura 10 exemplifica a visão geral desta arquitetura, detalhando seus componentes principais. Dentre eles, o Sistema de Gerenciamento (item 5), responsável pela administração do sistema e permissões dos usuários, corresponde a um trabalho derivado desenvolvido por Campos[32]. Com essa estrutura macro definida, podemos realizar o levantamento dos requisitos do sistema, prototipar, implementar e realizar os testes.

Figura 10 – Visão geral do sistema de controle de acesso IFB ACCESS



Fonte: elaborado pelos autores.

O funcionamento do sistema de controle de acesso utilizando NFC descrito abaixo:

1. **Aplicativo:** O processo começa com o aplicativo instalado em um *smartphone* que possui NFC, que se comunica com o leitor NFC integrado à catraca.
2. **Leitor NFC:** O leitor NFC na catraca verifica a identificação do usuário. Quando o *smartphone* se aproxima, o leitor lê os dados do NFC.
3. **Microcontrolador:** Os dados lidos pelo leitor são enviados para o microcontrolador que fará comunicação com o servidor.
4. **Servidor:** O microcontrolador se comunica o servidor central. O servidor é responsável pela autenticação do usuário. Ele verifica se o usuário tem permissão para acessar o

local.

Em resumo, o aplicativo no *smartphone* inicia a comunicação via NFC com o leitor na catraca. O microcontrolador se comunica com o servidor para autenticar o usuário.

3.2 Projeto do sistema

O levantamento dos requisitos do sistema foi inicialmente feito por meio da análise de sistemas já existentes que utilizam a tecnologia NFC, além de observações, formulação de hipóteses e testes. Posteriormente, os requisitos foram refinados por uma comissão criada especificamente para o projeto, conforme a Portaria nº 120/2024 - DGBR/RIFB/IFBRASILIA. Nessa comissão, foram realizadas reuniões para analisar, revisar e incrementar os requisitos do sistema.

Dessa forma, foram definidos os seguintes requisitos funcionais e não funcionais:

- Requisitos funcionais:
  - RF01 - O sistema deve realizar o cadastro e login do usuário.
  - RF03 - O sistema deve emitir a credencial para acesso.
  - RF04 - O sistema deve registrar as interações como data e hora da entrada e saída de cada usuário.
  - RF05 - O sistema deve enviar notificações para os responsáveis dos estudantes ao entrarem e saírem da instituição.
  - RF06 - O sistema deve restringir o acesso de entrada e saída.
  - RF07 - O sistema deve se comunicar com o módulo de NFC da catraca.
- Requisitos não funcionais:
  - RNF01 - O sistema deve ser executado em dispositivos móveis.
  - RNF02 - O sistema deve passar em testes de usabilidade pelos usuários.
  - RNF03 - O sistema deve restringir o cadastro a apenas uma credencial.
  - RNF04 - O sistema deve proteger as informações pessoais dos usuários de acordo com as regras da Instituição e pela Lei Geral de Proteção de Dados Pessoais (LGPD).

3.3 Software

Nesta seção, são apresentados os softwares utilizados neste trabalho, detalhando suas funcionalidades e a importância de cada um no desenvolvimento do projeto. Iniciaremos com o aplicativo desenvolvido em *Kotlin*, uma linguagem moderna e eficiente para a criação de aplicações *Android*. Discutiremos o processo de desenvolvimento, incluindo as etapas de design e prototipagem, que foram fundamentais para garantir uma interface intuitiva e uma experiência de usuário otimizada.

Em seguida, será abordado o servidor *conteinerizado utilizando Docker*, que permite a criação de ambientes isolados e consistentes para a execução de aplicações,

facilitando a escalabilidade e a portabilidade do sistema. Serão apresentados diagramas que ilustram a arquitetura do servidor, bem como o fluxo de dados entre os componentes. Também discutiremos o banco de dados MySQL, escolhido por sua robustez e confiabilidade no gerenciamento de dados, explicando como sua estrutura foi projetada para atender às necessidades específicas do projeto, garantindo eficiência e segurança no armazenamento das informações.

Por fim, será abordada a API desenvolvida em Flask, uma microestrutura em Python que permite a criação de aplicações web de forma rápida e simples. Será detalhado como a API se integra ao aplicativo e ao banco de dados, facilitando a comunicação entre os diferentes componentes do sistema. Essa seção fornecerá uma visão abrangente dos softwares utilizados, destacando como cada um contribui para a implementação e o sucesso do projeto.

3.3.1 Aplicativo Móvel

3.3.1.1 Mockup

Esta seção apresenta o *mockup* desenvolvido com a ferramenta de prototipação Figma, destacando suas funcionalidades e *design*. O *mockup* foi projetado para oferecer uma experiência intuitiva ao usuário, incorporando elementos de interface que facilitam a navegação e a interação.

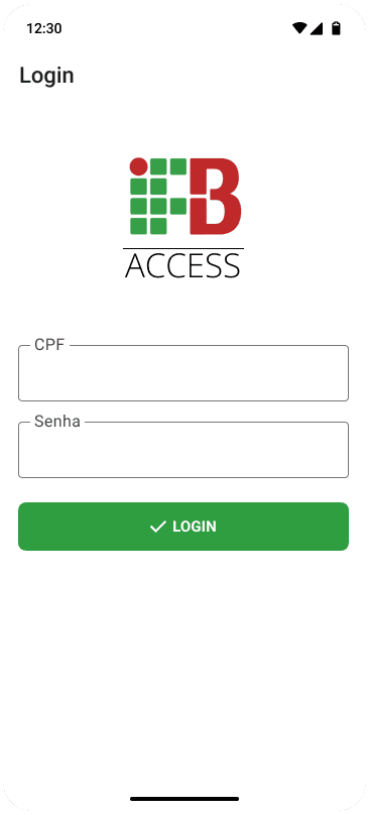
As principais funcionalidades incluem se autenticar ao realizar *login*, utilizar o NFC do dispositivo para comunicação com o leitor NFC da catraca, tela com histórico dos acessos do usuário em questão e possibilidade de sair da conta específica, que foram cuidadosamente planejadas para atender às necessidades dos usuários.

O *design* do *mockup* foi pensado em ser minimalista, acessível, além de conter as cores que remetem à paleta utilizada no próprio Instituto Federal[33]. Abaixo na Figura 11 é possível ver os *mockup*s de telas propostos para o aplicativo.

Figura 11 – Imagens do protótipo das telas do aplicativo móvel

(a) Tela de inicialização

(b) Tela de boas-vindas



(c) Tela de *login*

(d) Tela principal

(e) Histórico de acessos

(f) Tela de *logout*

Fonte: elaborado pelos autores.

3.3.1.2 Desenvolvimento

O processo de desenvolvimento do aplicativo móvel para emulação de credencial via NFC passou por diversas etapas e desafios tecnológicos. Inicialmente, o desenvolvimento começou com o uso da tecnologia *React Native*, um *framework* de *JavaScript* para desenvolvimento móvel[34]. A escolha foi baseada na familiaridade da equipe com *JavaScript* e *React*, o que teoricamente facilitaria a transição. Com o *React Native*, foi possível implementar com sucesso funcionalidades básicas, como a leitura e escrita em *tags* NFC. Contudo, o projeto exigia a emulação de credenciais de usuário no dispositivo usando o *Host-based Card Emulation (HCE)*, um requisito fundamental do sistema.

Diante de um obstáculo significativo, notou-se que o *React Native* apresentava limitações para implementar o HCE, o que forçou uma reavaliação da abordagem tecnológica. Como alternativa, considerou-se o uso do *Google Wallet* para gerar cartões NFC, mas a solução se mostrou inviável, pois seu protocolo está disponível apenas sob um Acordo de Não Divulgação (NDA), extrapolando o escopo do projeto[35].

Após uma pesquisa sobre aplicações que utilizam HCE, decidiu-se migrar o desenvolvimento para *Kotlin*, focando especificamente na plataforma *Android*, pois a maioria dos projetos que desenvolveram a funcionalidade eram nativos. Testes com um código de amostra em *Kotlin* demonstraram uma comunicação eficaz com o leitor NFC e a capacidade de implementar o HCE, oferecendo acesso direto às APIs do *Android* e garantindo maior controle.

Com a tecnologia definida, o desenvolvimento do aplicativo IFB ACCESS em *Kotlin* foi iniciado no *Android Studio*, com o código-fonte disponibilizado no Github[1]. Desde o início, a equipe adotou padrões de engenharia de *software* para aumentar a manutenibilidade, eficiência e segurança. A escolha fundamental da arquitetura foi o padrão *Model-View-ViewModel (MVVM)*, por ser uma abordagem recomendada oficialmente para o desenvolvimento moderno de aplicações *Android*.

Na construção das interfaces, o *Jetpack Compose* foi escolhido em vez do tradicional *Extensible Markup Language (XML)*, aproveitando seu paradigma declarativo e a criação de componentes reutilizáveis para reduzir redundâncias e a complexidade geral do desenvolvimento. Para a comunicação com a *API REST*, foi implementada a biblioteca *Ktor*, escolhida por ser uma solução moderna e nativa de *Kotlin* para requisições HTTP. As operações assíncronas foram gerenciadas com as *coroutines* do *Kotlin*, que simplificaram o código e o tratamento de exceções ao substituir os tradicionais *callbacks* por fluxos sequenciais.

A autenticação de usuários foi integrada ao *Firebase*, solução que forneceu uma infraestrutura segura e escalável, dispensando a necessidade de um serviço de *login* customizado. Apesar da conveniência, os dados sensíveis não foram armazenados nos servidores em nuvem do *Firebase*, mas sim em um servidor local nas dependências do IFB,

[1] O código-fonte está disponível em: https://github.com/infocbra/ifb-access-frontend

reforçando o controle e atendendo aos requisitos de confidencialidade e integridade.

3.3.2 Servidor

O servidor foi desenvolvido utilizando o *framework Flask* em *Python*, que atua tanto como servidor HTTP — escutando uma porta e recebendo requisições — quanto como aplicação de *back-end*, processando essas requisições, realizando a autenticação NFC, gerenciamento de permissões e registro das interações no banco de dados.

Para facilitar o *deploy* e a gestão do servidor, o Docker foi utilizado, permitindo criar, implantar e executar a aplicação em *containers*. A estrutura de pastas e arquivos do projeto Docker está organizada da seguinte forma:

```
.
├── /database
│   ├── init.sql
│   ├── /mysql_data
│   └── /mysql_dump
├── /flask_api
│   ├── /dao
│   │   └── user_dao.py
│   ├── /service
│   │   └── user_service.py
│   ├── Dockerfile
│   ├── app.py
│   ├── config.py
│   └── requirements.txt
├── /proxy
│   ├── conf
│   └── Dockerfile
├── .env
├── .gitignore
└── docker-compose.yaml
```

O arquivo `docker-compose.yaml` define a aplicação com cinco serviços principais: `database_mysql`, `flask_api`, `proxy` e `ngrok`.

`database_mysql`: Este serviço inicializa o banco de dados com um script SQL (init.sql). Está configurado para realizar verificações de saúde e reiniciar automaticamente em caso de falha.

`flask_api`: Este serviço constrói a aplicação Flask a partir do Dockerfile localizado na pasta flask_api. Ele depende do serviço `database_mysql` para garantir que o banco de dados esteja disponível antes de iniciar a API.

`proxy`: Este serviço utiliza o Nginx como proxy reverso, mapeando a porta 80 do host para a porta 80 do container. O proxy depende do serviço `flask_api`.

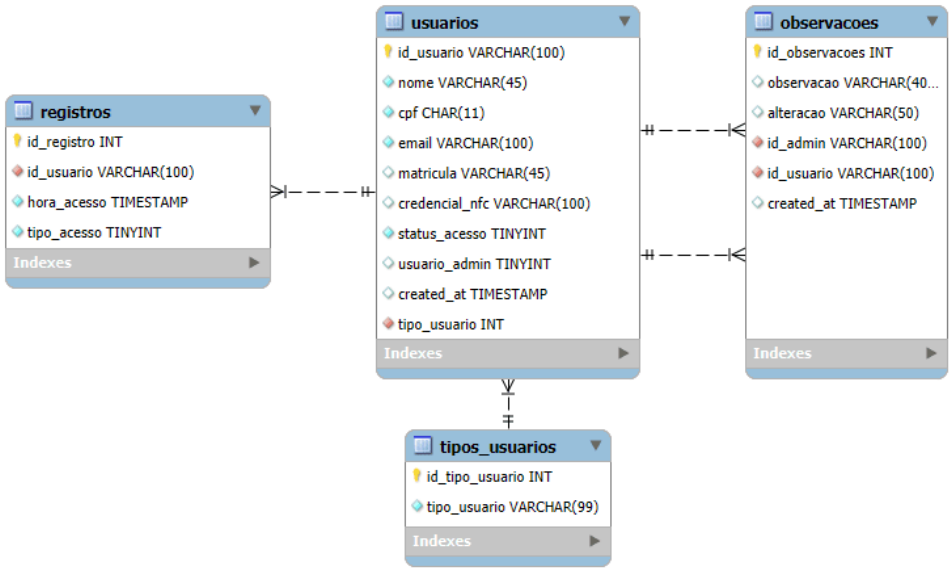
`ngrok`: Este serviço utiliza o Ngrok como ferramenta para expor o servidor local à internet. Sua configuração realiza o tunelamento de conexões, mapeando a porta 4040 do host para a porta 4040 do container. O ngrok depende do serviço `proxy`.

O código-fonte do projeto foi versionado e está disponivel no repositório do GitHub[2]. A configuração do ambiente de desenvolvimento exige a criação de um arquivo de variáveis de ambiente, denominado `.env`. Este arquivo é gerado a partir do modelo `.env.example` e deve ser preenchido com as credenciais específicas da aplicação, tais como as chaves de acesso ao banco de dados e as chaves de API necessárias para a correta operação do sistema. Concluída essa etapa de configuração, a aplicação está pronta para ser executada.

3.3.2.1 Banco de Dados

Neste projeto, decidimos utilizar o MySQL como SGBD. O MySQL é uma escolha popular e confiável, sendo um banco de dados relacional de código aberto. Ele se destaca por sua flexibilidade e por ser amigável com diversas linguagens de programação. A Figura 12 a seguir mostra o modelo físico para o sistema de controle de acesso, fornecendo os detalhes das tabelas e as entidades de dados.

Figura 12 – Modelo físico do banco de dados



Fonte: elaborado pelos autores.

Foram desenvolvidas as entidades para o banco de dados: *usuarios*, *observacoes*, *tipos-usuarios* e *registros*. Esses modelos fazem referência aos usuários, às observações dos administradores, ao tipo de usuário (se o usuário é docente, externo, aluno etc) e aos registros dos acessos dos usuários ao campus, respectivamente.

[2] O código-fonte está disponível em: https://github.com/infocbra/ifb-access-backend

Cada entidade possui uma série de atributos que fazem referência aos objetos que representam. A entidade registros, por exemplo, possui os atributos hora_acesso e tipo_acesso, que são, respectivamente, o horário que o usuário usou a catraca e se o acesso do usuário foi uma entrada ou saída. No Quadro 2 podemos observar as outras relações das entidades e os atributos e suas descrições.

Quadro 2 – Entidades do banco de dados e seus atributos

Entidade	Atributo	Descrição
usuarios	id_usuario	Identificador único para cada usuário
	nome	Nome do usuário
	cpf	Número de CPF do usuário
	email	Endereço de email do usuário
	matricula	Número de matrícula do usuário
	credencial_nfc	Credencial NFC do dispositivo do usuário
	status_acesso	Status do usuário (ativo/inativo)
	usuario_admin	Indica se o usuário é administrador ou não
	created_at	Data e hora de criação do usuário
	id_tipo_usuario	Chave estrangeira relacionada ao tipo do usuário
tipos_usuarios	id_tipo_usuario	Identificador único para o tipo de usuário
	tipo_usuario	Descrição do tipo de usuário (externo, docente, estudante, etc)
registros	id_registro	Identificador único para cada registro
	id_usuario	Referência ao usuário associado a esse registro
	hora_acesso	Data e hora em que o acesso foi registrado
	tipo_acesso	Registra se o acesso foi entrada ou saída pela catraca
observacoes	id_observacao	Identificador único para cada observação
	observacao	Observação escrita pelo administrador
	alteracao	Alteração realizada (Status de acesso, permissões de usuário, registros, etc)
	created_at	Data e hora da observação
	id_admin	Referência ao administrador responsável pela observação
	id_usuario	Referência ao usuário associado a essa observação

Fonte: elaborado pelos autores.

3.3.2.2 Application Programming Interface (API)

Uma *Application Programming Interface Representational State Transfer* (API REST) é um conjunto de definições e protocolos que permite a comunicação entre diferentes sistemas de software de forma padronizada e eficiente. Ela utiliza os métodos *Hypertext Transfer Protocol* (HTTP) para realizar operações CRUD (*Create, Read, Update, Delete*) em recursos, facilitando a integração entre sistemas distribuídos e a criação de aplicações web escaláveis[36].

A escolha do Python como linguagem base para a API foi motivada por dois fatores principais: primeiramente, o sistema do IFB já utiliza Python em seus servidores, o que facilita a integração e manutenção do novo sistema. Além disso, alguns integrantes da equipe de desenvolvimento possuíam menor curva de aprendizado em relação ao Python, o que contribuiu para uma implementação mais rápida e eficiente. O objetivo principal da

API REST desenvolvida é gerenciar a comunicação entre o Arduino/Microcontroladora e o Servidor, além de autenticar os usuários e realizar o processo de login.

3.3.2.3 Endpoints da API

A API desenvolvida conta com diversos endpoints para gerenciar as operações relacionadas aos usuários e autenticação. O endpoint `/usuarios` com o método *GET* permite obter todos os usuários cadastrados no sistema, retornando uma lista completa de usuários. Para obter dados de um usuário específico, foi implementado o *endpoint* `/usuarios/int:id` com o método *GET*, onde o parâmetro `id` representa o identificador único do usuário desejado.

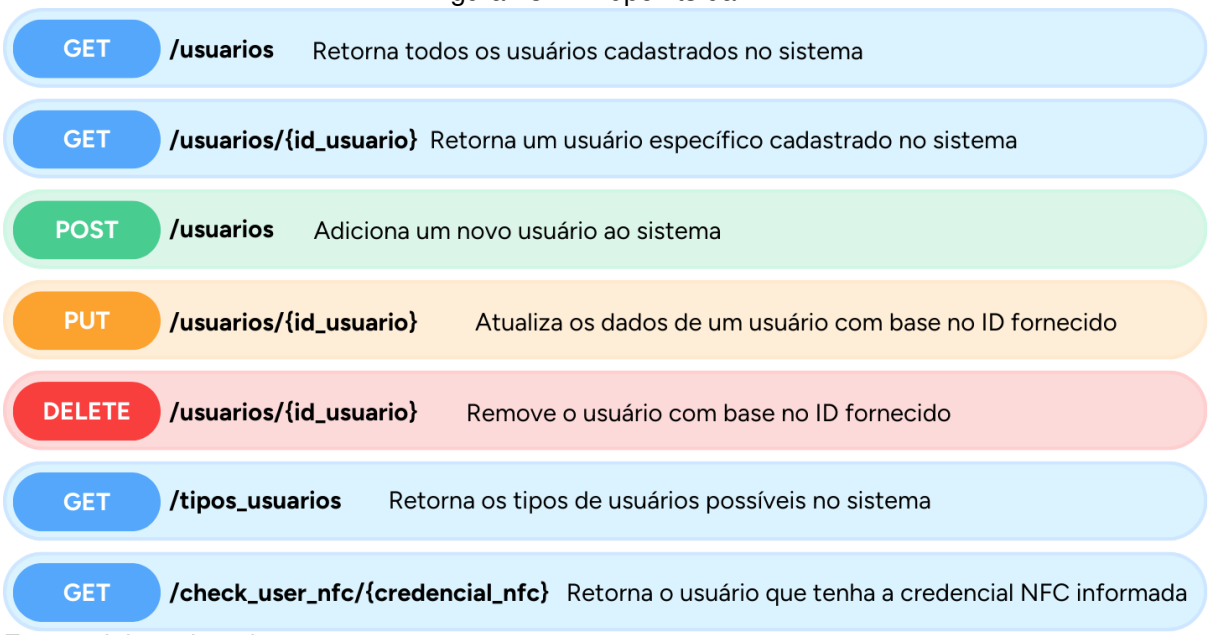
Para adicionar um novo usuário ao sistema, utiliza-se o *endpoint* `/usuarios` com o método *POST*. O corpo da requisição deve conter um JSON com as informações do novo usuário, incluindo `nome, email, matrícula ou CPF, e o id_tipo_usuário`. A atualização dos dados de um usuário existente é realizada através do *endpoint* `/usuarios/int:id` com o método *PUT*, onde o parâmetro `id` identifica o usuário a ser atualizado, e o corpo da requisição contém os dados atualizados em formato JSON.

A exclusão de um usuário é feita através do *endpoint* `/usuarios/int:id` com o método *DELETE*, onde o parâmetro `id` especifica o usuário a ser removido do sistema.

O *endpoint* `/tipos_usuarios` com o método *GET* foi criado para retornar os tipos de usuários possíveis no sistema, permitindo uma fácil categorização e gerenciamento de permissões dos usuários cadastrados.

Para verificar a existência de um usuário com base na credencial NFC, a API disponibiliza o *endpoint* `/check_user_nfc/string:credencial_nfc` com o método *GET*. Este *endpoint* recebe a credencial NFC como parâmetro na URL e retorna o usuário referente à credencial NFC informada.

Figura 13 – Endpoints da API



Fonte: elaborado pelos autores.

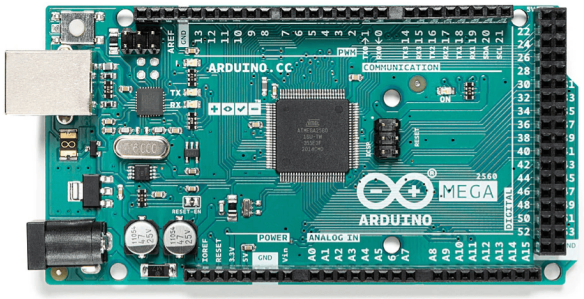
3.4 Hardware

Nesta seção, são apresentados todos os componentes utilizados na construção do leitor. Cada componente será descrito individualmente, destacando suas respectivas funções no sistema. Além disso, serão exibidos os componentes em conjunto, ilustrando como eles se interconectam para formar o dispositivo final.

3.4.1 Placa de desenvolvimento

Foi utilizada a placa de desenvolvimento Arduino Mega 2560 (ilustrada na Figura 14). Baseado no microcontrolador ATmega2560, este modelo se destaca por suas especificações robustas, oferecendo 54 pinos de entrada/saída digital — dos quais 15 podem ser usados como saídas PWM —, 16 entradas analógicas e uma capacidade de memória superior, com 256 KB de Flash, 8 KB de SRAM e 4 KB de EEPROM. Operando a uma frequência de 16 MHz, essas características tornam o Arduino Mega 2560 ideal para projetos complexos que demandam maior capacidade de processamento e conectividade, justificando sua escolha para esta aplicação [37].

Figura 14 – Placa de desenvolvimento Arduino Mega 2560



Fonte: Arduino Store[37].

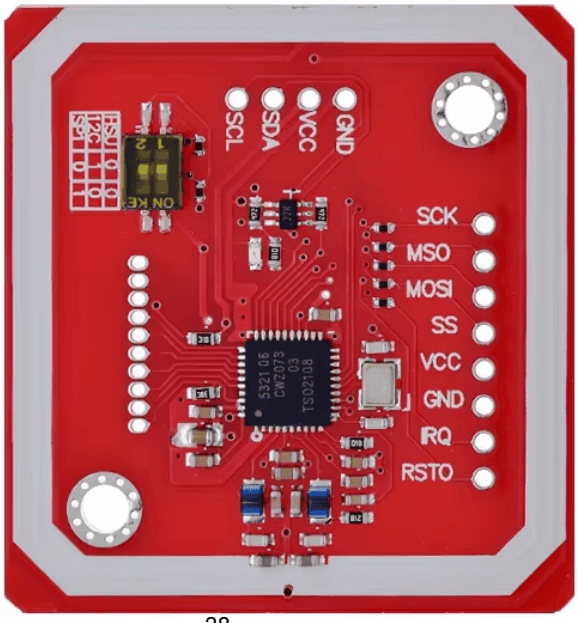
3.4.2 Módulo NFC

O módulo NFC RFID PN532 é um componente amplamente utilizado em projetos de comunicação sem fio de curto alcance. Ele é especialmente popular devido ao seu suporte a múltiplos tipos de comunicação. A seguir, discutimos em detalhes por que este módulo foi escolhido, os tipos de comunicação suportados e a escolha específica do *High Speed Uart* (HSU) como método de comunicação.

A escolha desse módulo, em comparação com outros disponíveis no mercado, se deve à sua capacidade de comunicação com outros dispositivos que utilizam tecnologia NFC, além dos cartões normais. Vale destacar que o módulo PN532 suporta três modos de comunicação com microcontroladores: **I2C**, **SPI** e **UART**.

A escolha pela comunicação via HSU se deve à maior confiabilidade em distâncias maiores, permitindo que o módulo se conecte ao Arduino sem interferências no sinal. Essa escolha também possibilita, posteriormente, a separação do controlador e do módulo NFC em ambientes distintos, com distâncias de até 1,5 km, utilizando o protocolo RS485 como intermediário para garantir a comunicação estável e eficiente. Na Figura 15 é possível observar o módulo PN532, os pinos de comunicação e a chave seletora do tipo de comunicação.

Figura 15 – Módulo NFC PN532

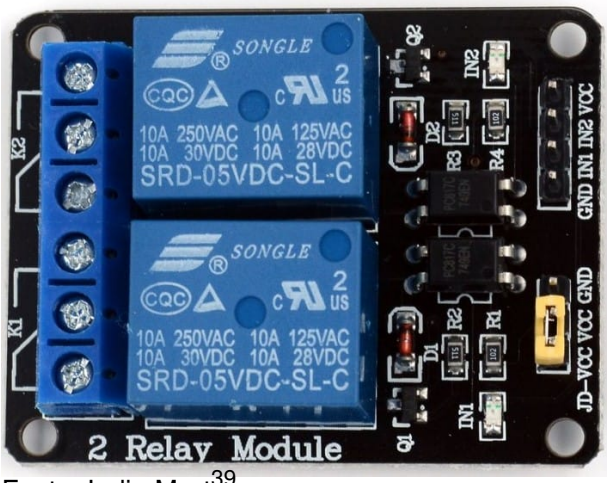


Fonte: Elechouse[38].

3.4.3 Relé e catraca

Outro componente importante desse sistema são os relés (Figura 16), que atuam diretamente no controle das catracas (Figura 17). Nesse sistema, o relé é usado para liberar a catraca. Normalmente, a catraca permanece desbloqueado e, caso um usuário não autorizado tente passar, um dispositivo eletromecânico da catraca, chamado solenoide, é acionado para bloquear a passagem. Quando um sinal de liberação do leitor é recebido, o relé é desenergizado, permitindo a passagem do usuário sem acionar o solenoide.

Figura 16 – Módulo relé duplo



Fonte: India Mart[39]

Figura 17 – Catraca Wolstar III

Fonte: Wolpac[40].

3.4.4 Módulo Ethernet ENC28J60

Por fim o módulo Ethernet ENC28J60, uma solução para adicionar conectividade de rede ao sistema. Baseado no chip ENC28J60 da Microchip, ele é um controlador Ethernet independente que se comunica com o microcontrolador principal via SPI, oferecendo suporte a velocidades de até 10 Mbps. Suas características incluem baixo consumo de energia, buffer interno para gerenciamento de pacotes e suporte a várias camadas do protocolo TCP/IP. A Figura 18 ilustra o módulo ENC28J60.

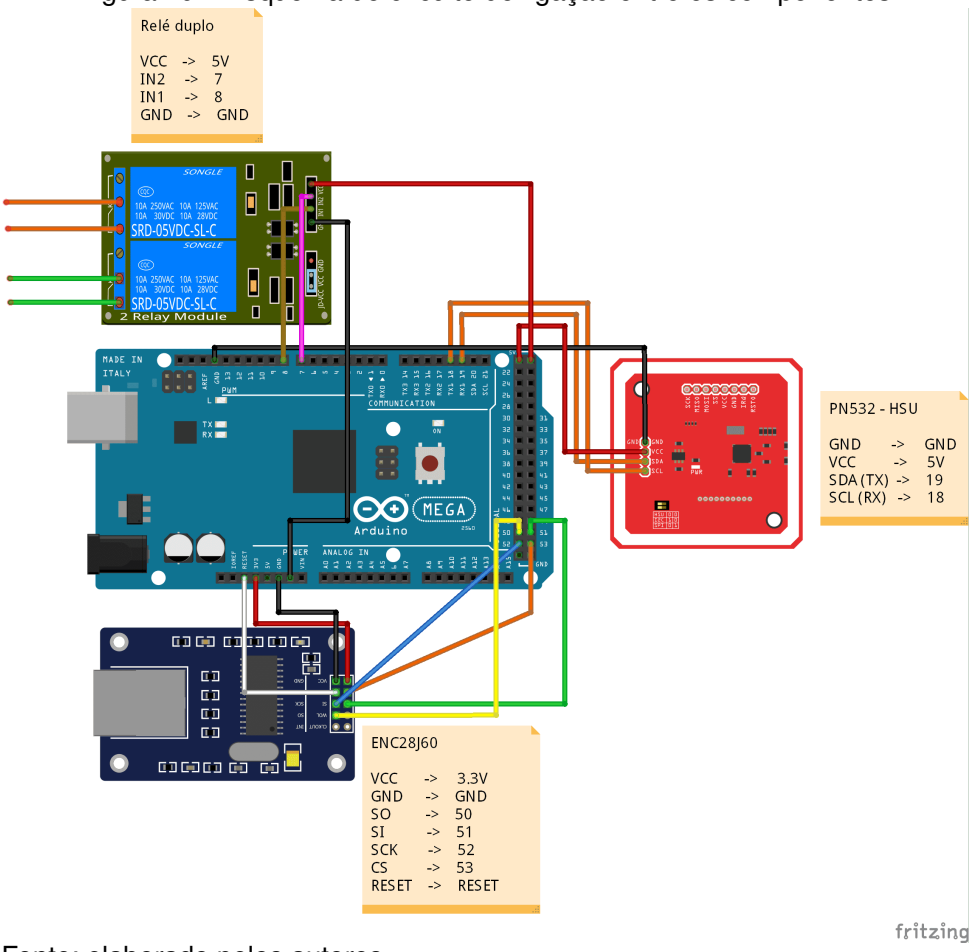
Figura 18 – Módulo Ethernet ENC28J60

Fonte: HU Infinito[41].

3.4.5 Leitor NFC

O protótipo do leitor foi desenvolvido combinando todos os elementos descritos nas subseções 3.4.1, 3.4.2, 3.4.3 e 3.4.4. Este protótipo serviu como uma plataforma de teste para validar a integração, o funcionamento dos componentes, a comunicação com o sensor NFC do celular e a implementação com a catraca. O esquema do circuito, apresentado Figura 19, ilustra detalhadamente todas as conexões realizadas entre os componentes utilizados, incluindo a disposição dos pinos e as interligações.

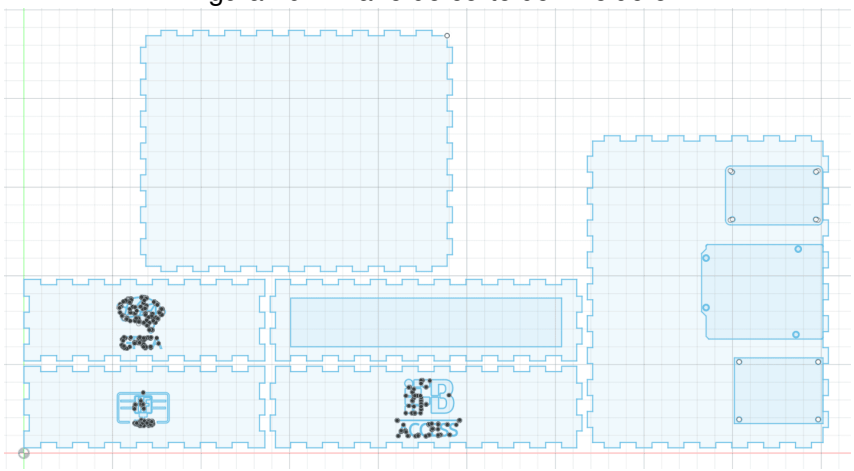
Figura 19 – Esquema do circuito de ligação entre os componentes



Fonte: elaborado pelos autores.

Para a montagem do leitor, foi projetada uma caixa para abrigar o sistema dentro da catraca. A Figura 20 apresenta o desenho 2D da caixa, criado com o MakerCase para gerar junções do tipo dedo. O desenho foi posteriormente editado no AutoCAD para a inclusão de logos e a criação de furos para a placa de desenvolvimento, o módulo *Ethernet* e o relé duplo. Posteriormente no capitulo de resultados é apresentado a figura da caixa montada como parte de resultado do trabalho.

Figura 20 – Plano de corte do invólucro



Fonte: elaborado pelos autores.

3.4.6 Software embarcado

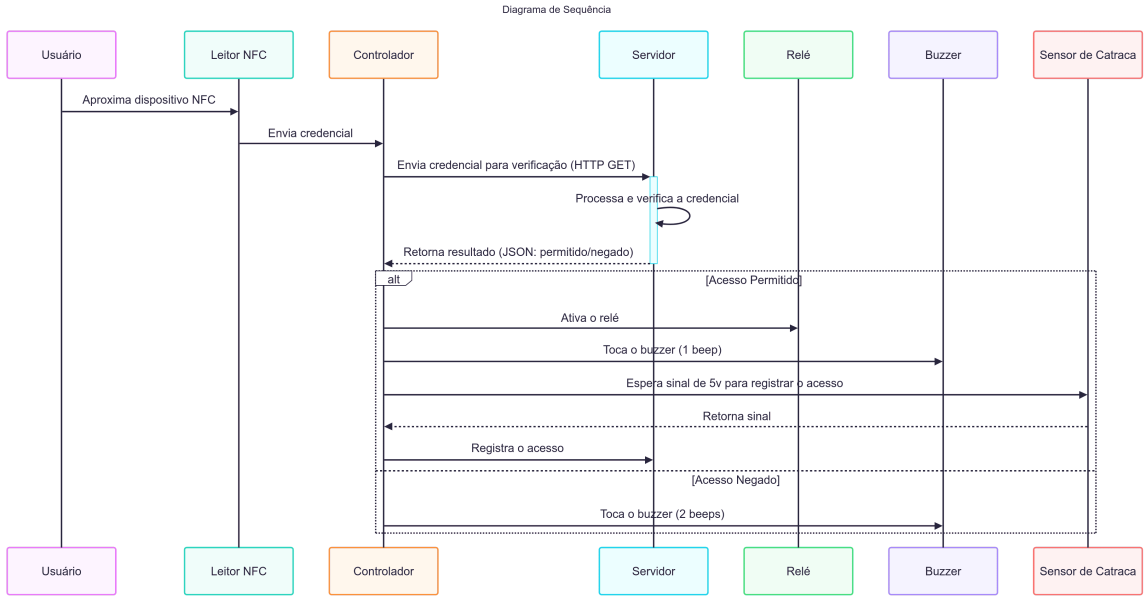
Utilizando a plataforma de prototipagem Arduino com a placa de desenvolvimento Mega 2560, cuja linguagem nativa é C/C++, foi desenvolvido o código embarcado no dispositivo que contém toda a rotina do leitor NFC.

O principal componente utilizado é o módulo PN532 NFC RFID, que opera com a biblioteca desenvolvida pela Seeed Studio[42]. Essa biblioteca permite a configuração e a comunicação com o microcontrolador por meio do protocolo HSU. Durante o desenvolvimento, é gerado o AID, um identificador único que desempenha a função essencial de determinar exatamente qual aplicativo o leitor deve acessar para estabelecer a comunicação. Esse identificador age como um ’endereço’ exclusivo, assegurando que o leitor interaja com o aplicativo correto, eliminando ambiguidades e garantindo uma comunicação eficiente e confiável.

Os relés são controlados utilizando funções padrão do Arduino, como *digitalWrite()* e *pinMode()*, que permitem configurar o estado dos pinos como ligado ou desligado. O diferencial está na lógica de programação: quando um dispositivo NFC válido é detectado, o sistema avalia o estado de acesso e o tempo decorrido desde o último registro para decidir se deve acionar o relé de entrada ou o de saída. Essa abordagem garante que o controle dos relés seja feito de forma precisa, com base no comportamento esperado do sistema.

Além disso, o módulo Ethernet é utilizado para permitir a comunicação do sistema com a rede local. Este módulo, que se comunica com o Arduino através do protocolo SPI, permite enviar e receber dados pela rede. Na figura Figura 21, encontra-se o diagrama de sequência com a rotina implementada no leitor.

Figura 21 – Diagrama de sequência do leitor



Fonte: elaborado pelos autores.

3.5 Testes de desenvolvimento

Antes de realizar os testes com os usuários finais, cada etapa do desenvolvimento do sistema foi testada. Foram avaliados o funcionamento do leitor, a comunicação com o aplicativo e a integração do sistema com a catraca.

A primeira parte foi compreender o funcionamento da catraca[40], foram estudados seu manual técnico e suas interfaces de comunicação para a liberação do acesso. O modelo Wolstar III é equipado com um mecanismo denominado Apache, que opera no regime de travamento e pode funcionar de forma unidirecional ou bidirecional. Normalmente, o equipamento permanece liberado, mas, em caso de tentativa de passagem por um usuário não autorizado, um solenóide é acionado para bloquear o acesso.

Quando um sinal de liberação é emitido, seja por meio de um leitor ou de um botão, o sistema permite a passagem do usuário sem necessidade de ativar o solenóide. Além disso, o módulo de controle do equipamento, ao operar no modo ’Pulso Momentâneo’, aguarda por um período pré-determinado após a liberação. Se o usuário não realizar a passagem dentro desse intervalo, o sistema cancela a liberação e volta a estar disponível para um próximo usuário[40].

Após identificar os sinais que seriam utilizados, foi implantado um protótipo inicial para verificar se a comunicação entre os componentes estava ocorrendo conforme o esperado, conforme ilustrado na Figura 23.

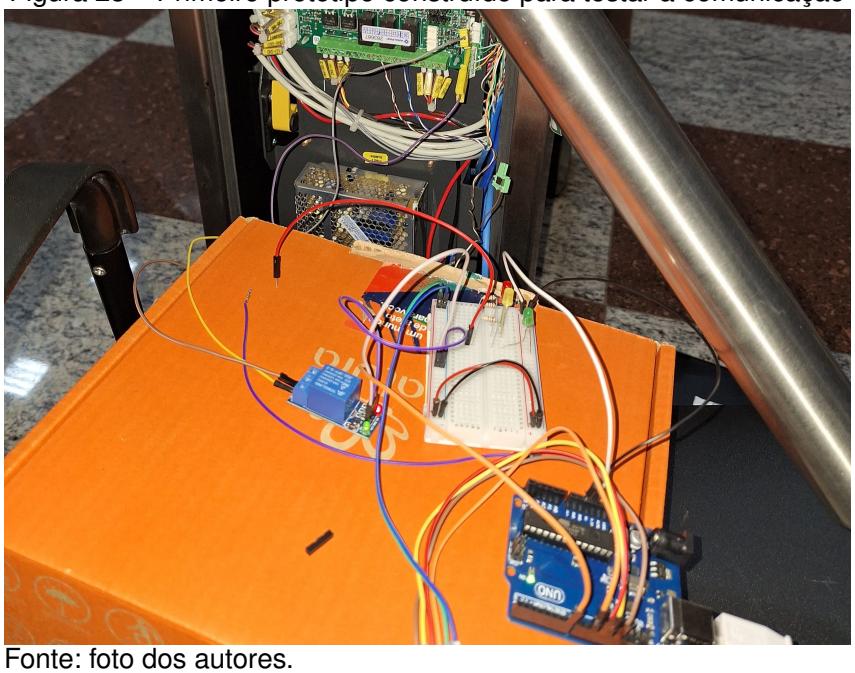
Figura 22 – Sinais de entrada e saída descritos no manual da catraca

Descrição dos sinais de entrada e saída

- **BOT –** Libera entrada e saída;
- **INFO1 –** Informação de passagem - entrada;
- **INFO2 -** Informação de passagem - saída;
- **LIB1 –** Libera entrada;
- **LIB2 –** Libera saída;
- **EMER –** Passagem livre.

Fonte: Manual Wolstar III[40].

Figura 23 – Primeiro protótipo construído para testar a comunicação



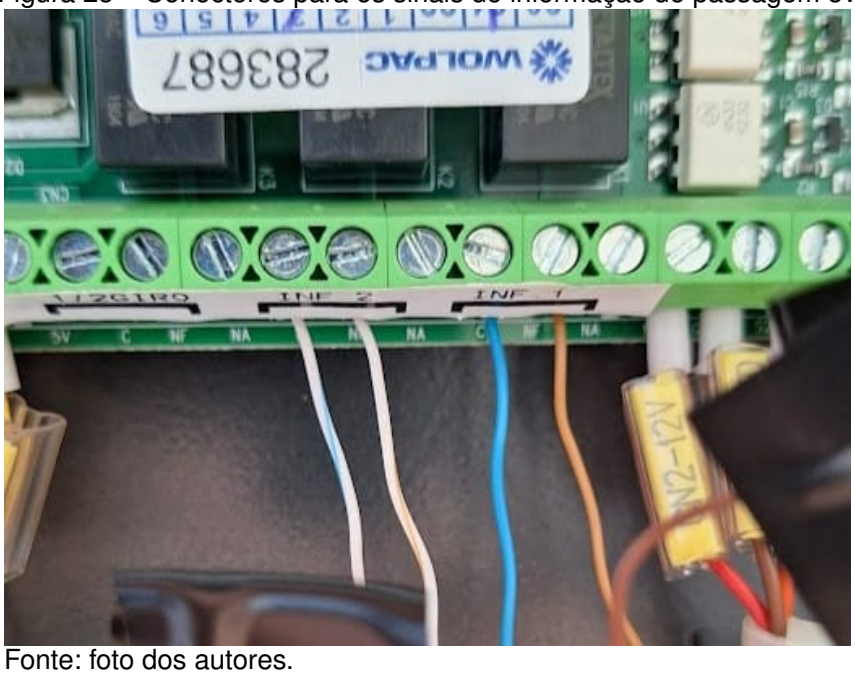
Fonte: foto dos autores.

Na Figura 24, são apresentados os pinos responsáveis pelo sinal de liberação, enquanto na Figura 25 estão os pinos que enviam o sinal indicando a passagem do usuário pela catraca, permitindo o registro efetivo no sistema.

Figura 24 – Conectores para os sinais de liberação

Fonte: foto dos autores.

Figura 25 – Conectores para os sinais de informação de passagem 5v



Fonte: foto dos autores.

3.6 Avaliação do sistema

Para os testes com os usuários do sistema, foi elaborado um formulário para recrutar participantes interessados em testar o sistema de controle de acesso, que foi divulgado por meio de mensagens, e-mail e pelo perfil da instituição no Instagram. O formulário continha perguntas específicas sobre o sistema operacional do smartphone (Android ou iOS) e a presença da funcionalidade NFC (Near Field Communication) no

dispositivo. Além disso, no formulário, foram disponibilizados os "Termos de Uso e Política de Privacidade", cujo detalhamento está disponível no Apêndice B.

Para a coleta de *feedback* dos usuários após os testes, foi elaborado um formulário com o objetivo de avaliar tanto a usabilidade quanto a eficiência da solução proposta. A metodologia de avaliação de usabilidade aplicada foi a *System Usability Scale* (SUS), um questionário desenvolvido por John Brooke em 1986 para medir a satisfação do usuário com sistemas[43]. O SUS coleta as respostas por meio de uma escala de cinco pontos, um método proposto originalmente por Likert para medir atitudes[44]. Nessa escala, os participantes classificam seu nível de concordância com cada afirmativa, variando de 1 (Discordo Totalmente) a 5 (Concordo Totalmente).

Além das 10 questões padrão do SUS, o formulário foi complementado com quatro perguntas específicas, elaboradas para obter uma análise mais aprofundada sobre a performance do sistema. Essas questões adicionais investigaram a velocidade de reconhecimento da credencial, a praticidade da autenticação via NFC em comparação a outros métodos, e a necessidade de múltiplas tentativas para obter o acesso. A aplicação deste questionário foi direcionada aos participantes do teste-piloto para coletar dados quantitativos e qualitativos sobre sua experiência de uso.

4 RESULTADOS E DISCUSSÃO

Este capítulo se dedica a apresentar e analisar os resultados do projeto. Serão expostos os desafios superados, as soluções e os dados coletados, oferecendo uma análise sobre a viabilidade, a usabilidade e o impacto do sistema de controle de acesso proposto.

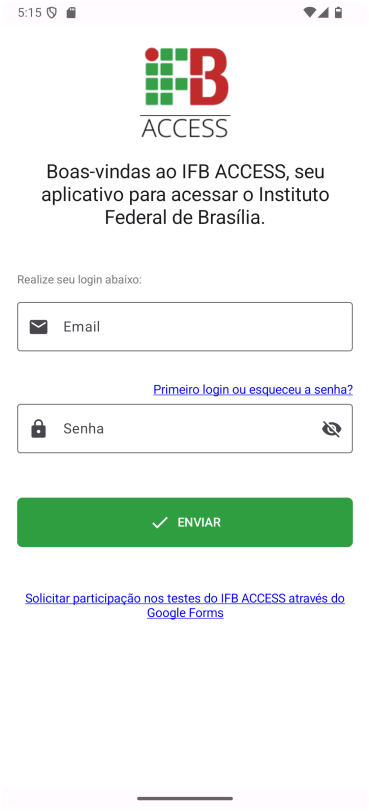
Como reconhecimento formal da inovação e do trabalho desenvolvido, o sistema teve seu software registrado junto ao Instituto Nacional da Propriedade Industrial (INPI) sob o número BR512025001602-6, um marco que assegura a propriedade intelectual da solução. Adicionalmente, o projeto foi apresentado no Simpósio de Integração, Inovação e Tecnologia (SIIT)[45], onde recebeu menção honrosa de melhor pôster na edição de 2024, reforçando a relevância pesquisa[46].

4.1 Aplicativo móvel

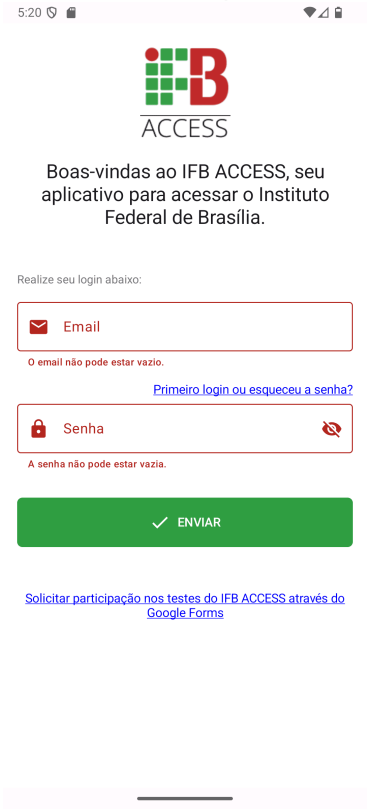
4.1.1 Implementação das funcionalidades

A fase inicial de desenvolvimento do aplicativo móvel IFB ACCESS foi concluída com a implementação bem-sucedida de suas funcionalidades essenciais, que foram estruturadas em sete telas principais: Tela de *login*, Tela de completar cadastro, Tela de recuperação de senha, Tela principal, Tela de registros de acessos, Tela de informações e Tela de sair da conta. Dentre as funcionalidades implementadas, destacam-se o processo de *login* via *Firebase*, a comunicação com a *API* utilizando *Ktor* e, a emulação de cartões por meio da tecnologia HCE. As Figuras 26, 27 e 28 a seguir ilustram as telas desenvolvidas e, após cada figura é apresentada uma descrição que detalha as telas em questão.

Figura 26 – Imagens das telas do aplicativo móvel (Parte 1 de 3)



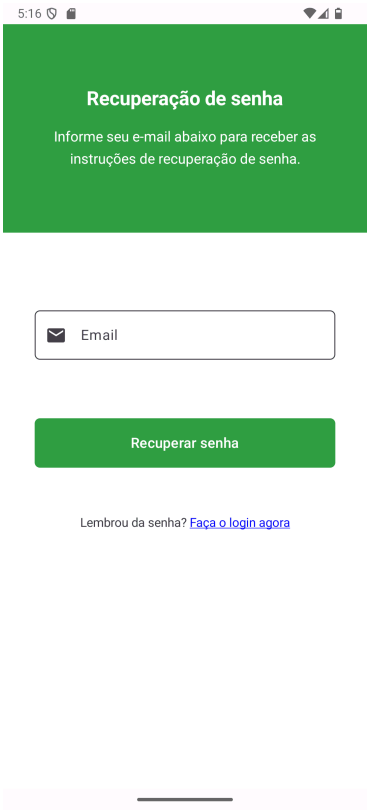
(a) Tela de *login*



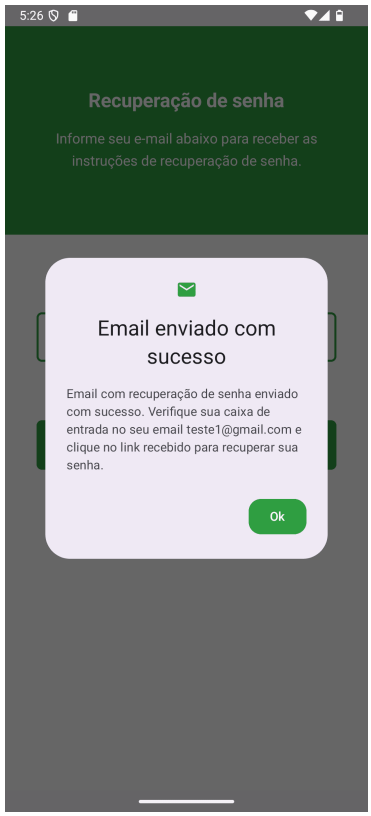
(b) Tela de *login* com erro

(c) Tela para completar cadastro

(d) Tela de cadastro com *drop-down menu* aberto



(e) Tela de recuperação de senha



(f) Caixa de diálogo aberta após recuperação de senha enviada

Fonte: elaborado pelos autores.

O aplicativo foi projetado com uma foco em construir uma interface intuitiva, iniciando o fluxo do usuário diretamente na tela de *login*, ilustrada na Figura 26a. Essa abordagem representa uma melhoria em relação ao protótipo, pois diminui o número de cliques necessários. Outra modificação fundamental foi a substituição do campo de CPF por *e-mail*, uma alteração necessária para garantir a compatibilidade com o sistema de autenticação do *Firebase*. Por fim, a tela foi aprimorada com duas funcionalidades: um link para recuperação de senha e outro para que novos usuários solicitem acesso ao sistema.

Visando uma melhor experiência do usuário, implementou-se um *feedback* visual para situações de erro durante o *login*. Nesses casos, os campos de texto recebem bordas e um texto de apoio em vermelho para notificar o usuário sobre a falha na autenticação, como demonstra a Figura 26b.

Outra funcionalidade implementada foi a tela para finalização de cadastro (Figura 26c), cuja adição foi motivada pela necessidade de aumentar a segurança. Os dados solicitados nesta etapa são utilizados para confirmar a identidade de quem utiliza o sistema e para o levantamento de estatísticas de uso. Entre os dados coletados está o tipo de vínculo com a instituição, que o usuário pode selecionar por meio de um *menu dropdown*, como mostra a Figura 26d.

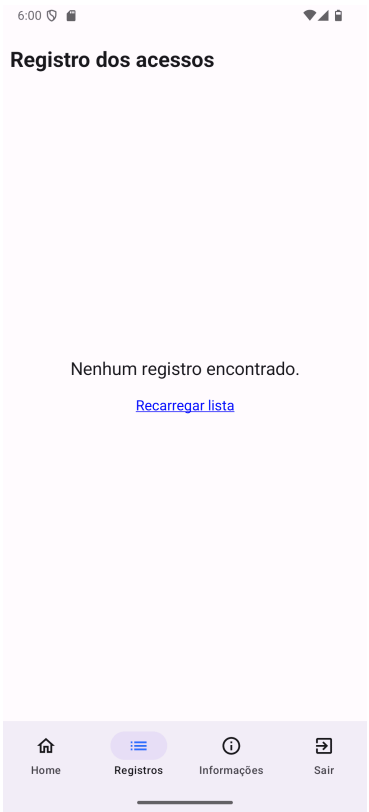
A tela de recuperação de senha (Figura 26e) atende aos usuários que esqueceram sua credencial ou que estão acessando o sistema pela primeira vez. O fluxo exige que o usuário insira seu *e-mail* institucional. Caso o endereço seja válido, ao acionar o botão de recuperação, o sistema exibe uma caixa de diálogo informando que o *e-mail* foi enviado com sucesso e instruindo o usuário a verificar sua caixa de entrada para clicar no link recebido e redefinir sua senha.

Figura 27 – Imagens das telas do aplicativo móvel (Parte 2 de 3)

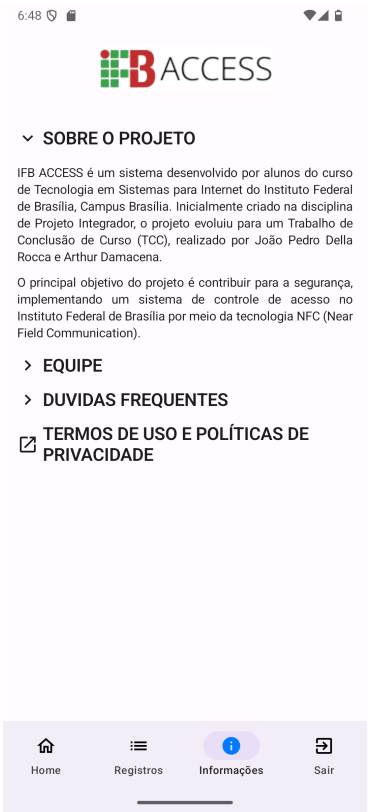
(a) Tela principal

(b) Tela principal quando NFC está desligado

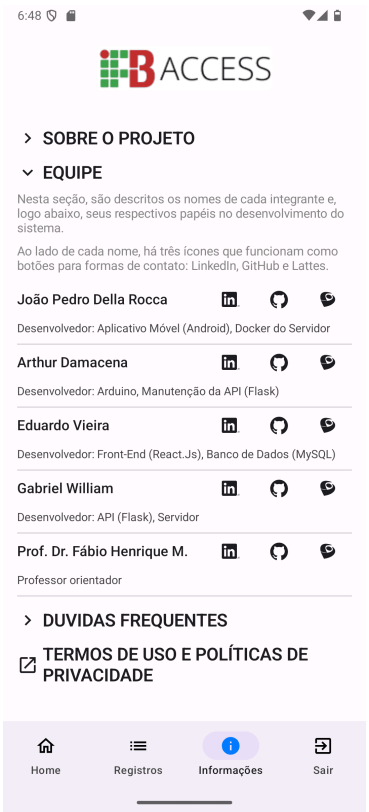
(c) Tela de registros de acessos com dados



(d) Tela de registros de acessos sem dados



(e) Tela de informações sobre o projeto



(f) Tela de informações sobre a equipe.

Fonte: elaborado pelos autores.

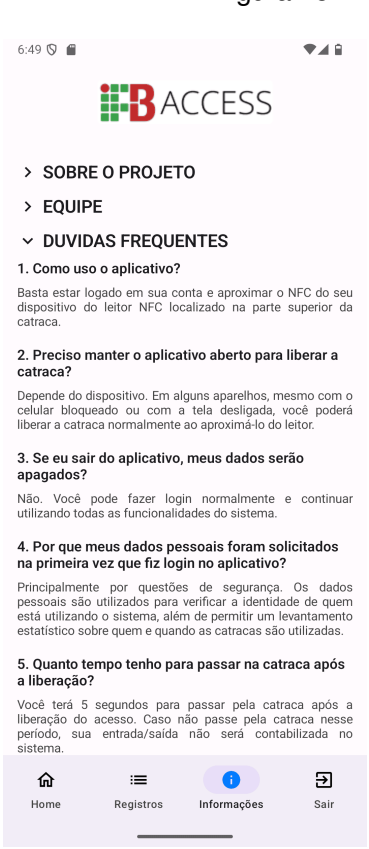
Após o *login*, a interface principal do aplicativo utiliza uma barra de navegação inferior (*bottom tab navigation*), projetada para facilitar a orientação e o acesso às diferentes seções do sistema.

A tela inicial, apresentada ao usuário após a autenticação (Figura 27a), exibe um breve tutorial visual. Este guia instrui o usuário a aproximar o celular do leitor da catraca e aguardar o sinal de liberação (luz verde), sendo acompanhado por um ícone ilustrativo. Caso a funcionalidade NFC do dispositivo esteja desativada, o aplicativo exibe um alerta, conforme a Figura 27b, com um ícone específico e a mensagem “NFC desligado. Ative para usar o IFB ACCESS”, orientando o usuário a habilitar o recurso para prosseguir.

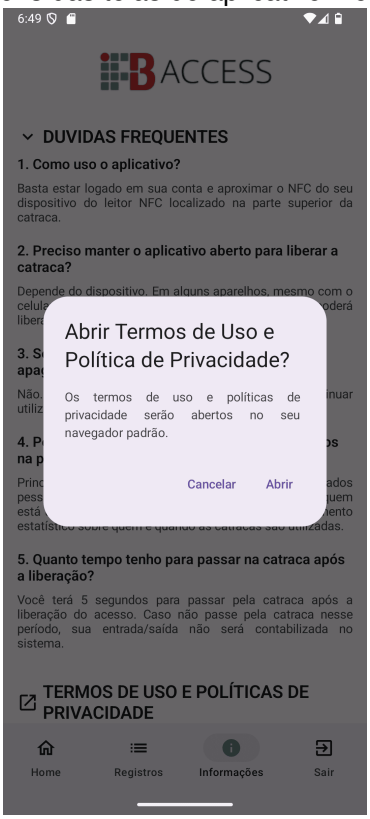
A seção de “Registros de Acesso”, ilustrada nas Figura 27c e Figura 27d, exibe o histórico de utilização do sistema. Cada entrada detalha a data, a hora e o tipo de acesso (entrada ou saída da instituição). Na ausência de registros, o sistema informa ao usuário com a mensagem “Nenhum registro encontrado.”.

A tela de Informações foi projetada para esclarecer dúvidas e promover a transparência sobre o projeto. Suas seções iniciais incluem “Sobre o projeto” (Figura 27e), que resume a motivação e os objetivos do trabalho, e “Equipe” (Figura 27f), que apresenta os integrantes com links para seus perfis profissionais.

Figura 28 – Imagens das telas do aplicativo móvel (Parte 3 de 3)



(a) Tela de informações com dúvidas frequentes



(b) Caixa de diálogo aberta ao clicar no "termos de uso e políticas de privacidade"

(c) Tela sair da conta

Fonte: elaborado pelos autores.

Ainda na “Tela de Informações”, o usuário encontra uma seção de “Dúvidas Frequentes” (Figura 28a) para sanar os questionamentos mais comuns sobre a utilização do sistema. Adicionalmente, um link permite visualizar os “Termos de Uso e Política de Privacidade” (Figura 28b), cujo conteúdo completo está disponível no Apêndice B.

Finalmente, a “Tela de sair da conta” (Figura 28c) apresenta uma mensagem de confirmação para evitar saídas acidentais, alertando que será necessário realizar uma nova autenticação para continuar utilizando o aplicativo. Para prosseguir, o usuário deve marcar uma caixa de seleção (*checkbox*), confirmando sua decisão de encerrar a sessão.

4.1.2 Publicação e testes na Google Play Store

Finalizada a primeira versão do aplicativo, o passo seguinte foi iniciar o processo de publicação e validação em um ambiente real. Com o auxílio do Grupo de Pesquisa em Computação Aplicada (GPCA), o aplicativo foi inserido em uma organização para ser publicado na *Google Play Store*, o que permitiu o acesso às ferramentas de teste e distribuição da plataforma.

O processo de publicação na *Google Play Store* segue um modelo de testes em faixas, conforme detalhado no Quadro 3. Inicialmente, o aplicativo passou por uma breve fase de **teste interno**, cuja finalidade é distribuir versões preliminares a um pequeno grupo de testadores confiáveis para obter *feedback* antecipado. Em seguida, avançou para a faixa de **teste fechado**, que visa compartilhar o aplicativo com um grupo maior e controlado para garantir a conformidade com as políticas do *Google Play* antes do lançamento. A etapa final é a **produção**, que torna o aplicativo disponível publicamente após o cumprimento dos requisitos de teste, como a validação com no mínimo 12 testadores por 14 dias.

Quadro 3 – Requisitos de teste de aplicativos no *Google Play* por faixa

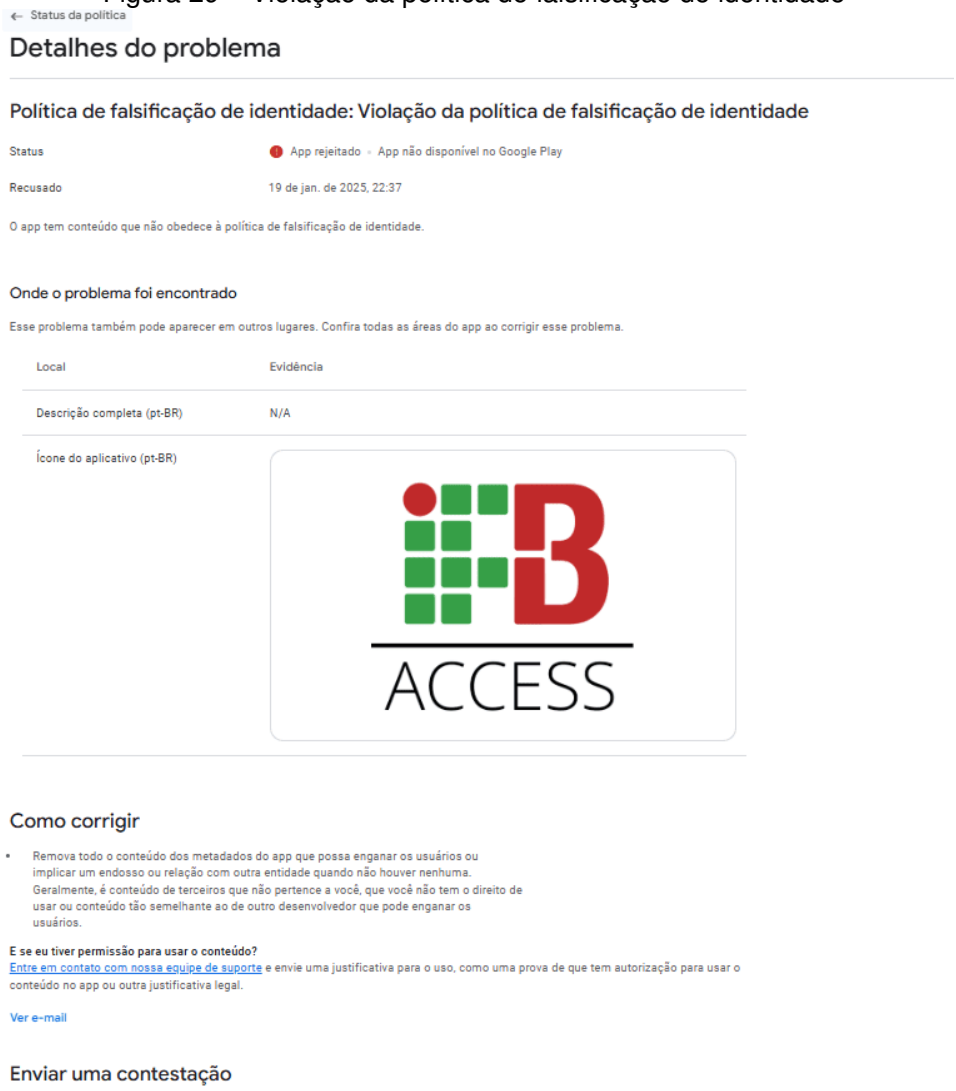
Tipo de faixa	**Propósito**	**Requisitos para acessar esta faixa**
Teste interno	Distribuir rapidamente versões para um pequeno grupo de testadores confiáveis, a fim de identificar problemas e obter *feedback* antecipado (antes ou depois de você terminar de configurar seu aplicativo).	Nenhum.
Teste fechado	Compartilhar seu aplicativo com um amplo grupo de usuários que você controla, para poder corrigir problemas e garantir que seu aplicativo esteja em conformidade com as políticas do *Google Play* antes do lançamento.	Deve ter terminado de configurar seu aplicativo.
Teste aberto	Disponibilizar a versão de teste do seu aplicativo no *Google Play* — qualquer pessoa pode participar do seu teste e enviar *feedback* privado para você.	Deve ter obtido acesso à produção para acessar os testes abertos.
Produção	Tornar seu aplicativo disponível para bilhões de usuários no *Google Play*.	Antes de solicitar o acesso à produção, você deve realizar um teste fechado com pelo menos 12 testadores inscritos por 14 dias. Após cumprir os critérios, você poderá solicitar o acesso à produção respondendo a algumas perguntas sobre seus testes, seu aplicativo e sua prontidão para produção no *Play Console*.

Fonte: Google Play[47]

A trajetória do IFB ACCESS por essas faixas, no entanto, enfrentou desafios iniciais. Em 19 de janeiro, a primeira submissão do aplicativo foi rejeitada pela *Google Play* sob a justificativa de "Violação da política de falsificação de identidade", conforme ilustrado na Figura 29. A rejeição ocorreu porque o logotipo desenvolvido para o aplicativo continha a identidade visual do Instituto Federal de Brasília (IFB), mas a equipe ainda não possuía

a autorização formal para seu uso. A situação foi regularizada em 12 de março, com a obtenção de uma declaração oficial da instituição autorizando o uso da marca. Após o envio de uma contestação anexando este documento, o aplicativo foi finalmente aceito na plataforma.

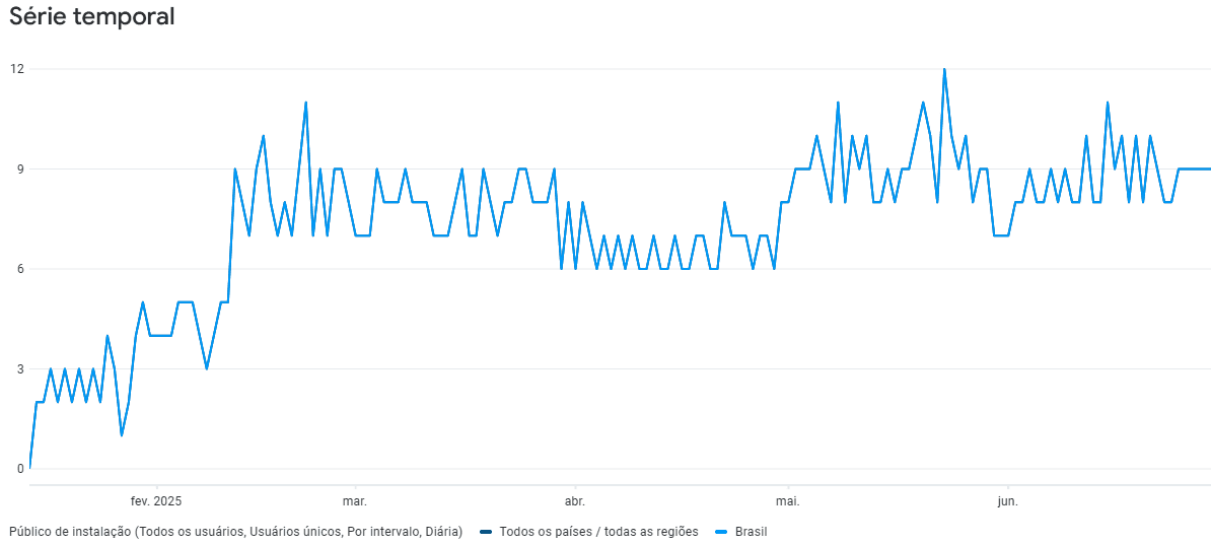
Figura 29 – Violação da política de falsificação de identidade



Fonte: Ferramenta de estatísticas do *Google Play Console*

Superados os impedimentos iniciais, em 10 de fevereiro, um *e-mail* (Apêndice D) foi enviado aos participantes selecionados, anunciando o início oficial dos testes e a disponibilidade do aplicativo para *download*. A comunicação fornecia um passo a passo detalhado sobre como instalar o aplicativo, iniciar os testes, enviar *feedback* e contatar a equipe em caso de dúvidas. O envio deste convite teve um impacto direto e positivo na adesão, o que pode ser observado no aumento do número de instalações, conforme ilustra a Figura 30, que saltou de 3 para 11 entre os dias 9 e 22 de fevereiro.

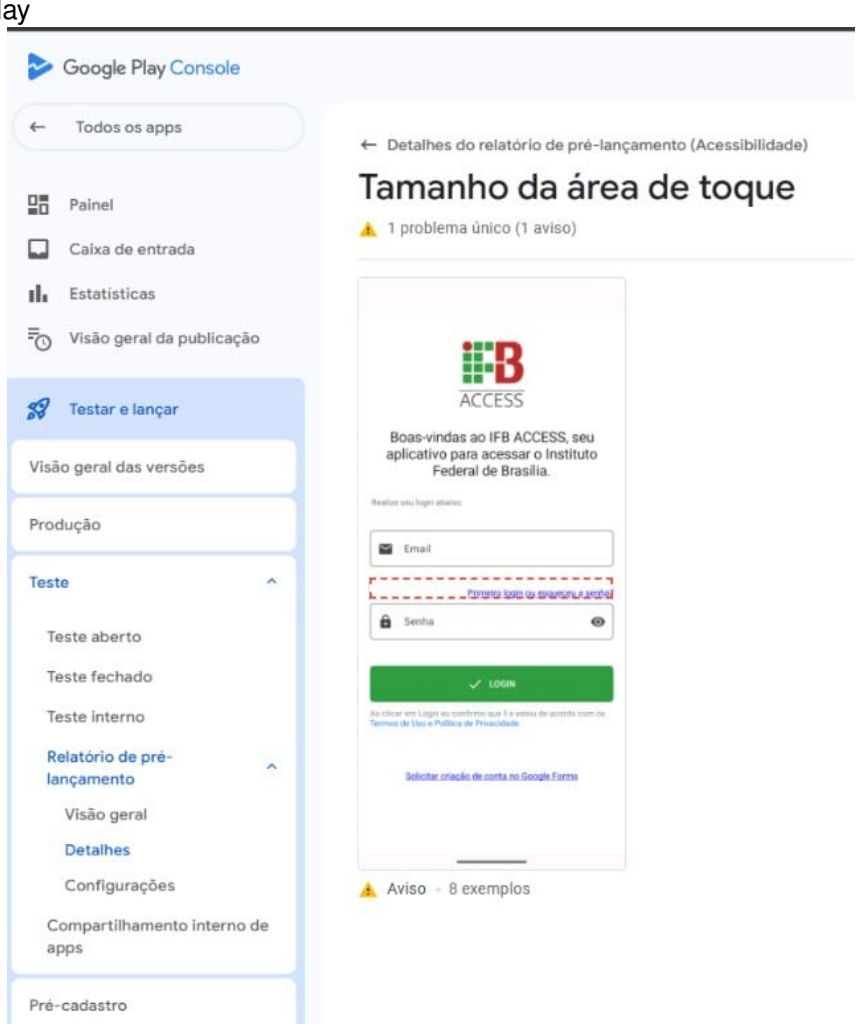
Figura 30 – Série temporal de instalações do aplicativo no Google Play (Jan-Jul 2025)



Fonte: Ferramenta de estatísticas do *Google Play Console*

Durante o período de testes, as ferramentas de análise da própria *Play Store* forneceram informações valiosas sobre a qualidade do aplicativo. Em uma análise automatizada de acessibilidade, por exemplo, a plataforma identificou uma inconsistência na interface, ilustrada na Figura 31: um texto clicável possuía a função de clique associada ao seu contêiner-pai em vez do próprio elemento de texto. Esse apontamento demonstra a eficácia das ferramentas do *Google* em identificar desvios de boas práticas de desenvolvimento que poderiam passar despercebidos.

Figura 31 – Problema de tamanho de toque reportado pela ferramenta de acessibilidade do Google Play



Fonte: Ferramenta de estatísticas do *Google Play Console*

Em contrapartida, a análise de estabilidade apresentou resultados extremamente positivos. O painel de falhas e erros não registrou nenhuma ocorrência durante todo o período de testes, indicando que o aplicativo se mostrou estável, sem erros críticos que afetassem o desempenho ou a experiência do usuário.

Outro indicador relevante foi o tamanho do aplicativo. A ferramenta de análise da *Play Store* demonstrou que a versão compilada para distribuição ocupa apenas 21.3 megabytes (MB) para *download* e 30.1 MB de armazenamento total após a instalação no dispositivo. Esses números confirmam que o aplicativo é leve e exige pouco espaço de armazenamento, um fator importante para garantir sua acessibilidade em uma ampla gama de dispositivos.

A fase de teste fechado foi concluída com sucesso. Com base nos dados coletados e no cumprimento dos pré-requisitos técnicos exigidos pela plataforma, o IFB ACCESS demonstrou estar pronto para o lançamento. Atualmente, o aplicativo encontra-se na fase de submissão para a faixa de produção, o último passo para sua disponibilização ao público na *Google Play Store*.

4.2 Hardware

O fomento para a aquisição do hardware essencial à prototipagem deste sistema foi obtido através da aprovação no Edital 15/2023, promovido pela Pró-Reitoria de Pesquisa e Inovação do Instituto Federal de Brasília (PRPI/RIFB/IFBRASILIA). A proposta, submetida sob o título "Arduino + NFC: Uma combinação mágica para projetos inovadores", alcançou a primeira colocação na seleção, com a expressiva nota de 98 pontos. O auxílio-pesquisa de R$ 700,00 concedido foi fundamental para viabilizar a construção do protótipo inicial, cujos componentes e custos estão detalhados na Tabela 1. O protótipo foi apresentado com sucesso durante a 3ª Semana Nacional da Educação Profissional e Tecnológica, conforme ilustrado na Figura 32.

Tabela 1 – Valores e fontes para os componentes de hardware do sistema IFB ACCESS

Componente	Valor Aproximado (R$)	Fonte/Loja
Módulo NFC PN532	R$ 50,00 – R$ 80,00	Mercado Livre, Amazon Brasil, MakerHero
Arduino Mega 2560	R$ 120,00 – R$ 200,00	Mercado Livre, Baú da Eletrônica
Módulo Ethernet ENC28J60	R$ 40,00 – R$ 75,00	Mercado Livre, FilipeFlop, MakerHero
Módulo Relé 2 Canais 5V	R$ 10,00 – R$ 25,00	Eletrogate, Mercado Livre, RoboCore
Buzzer Ativo 5V	R$ 2,00 – R$ 10,00	Eletrogate, Baú da Eletrônica, Mercado Livre
Total Estimado	**R$ 222,00 – R$ 390,00**	

Fonte: Pesquisa de mercado em diversas lojas online brasileiras (junho de 2025).

Figura 32 – Apresentação na 3ª Semana Nacional da Educação Profissional e Tecnológica

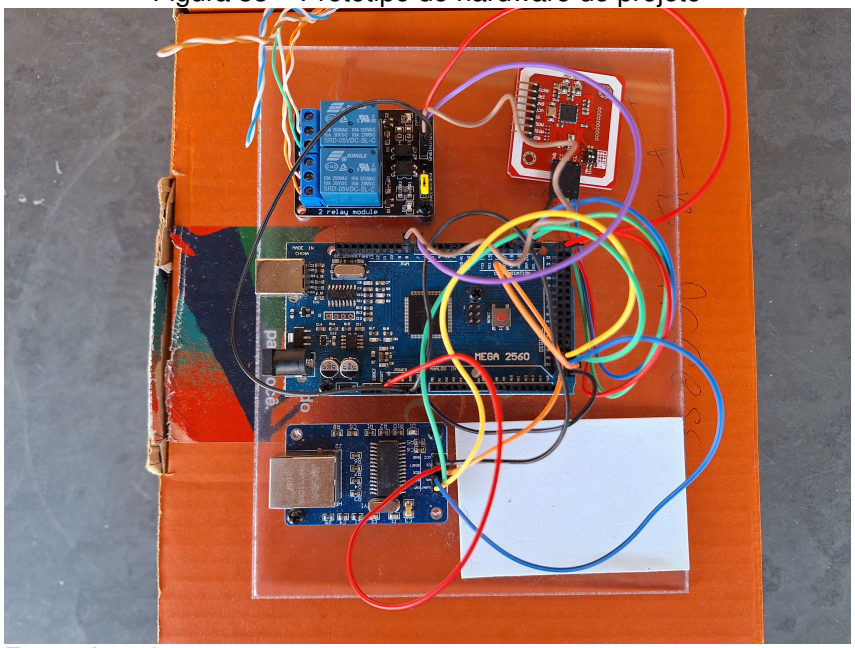
Fonte: foto dos autores.

4.2.1 Montagem do hardware

Com o sucesso das etapas de validação, que abrangeram os testes de comunicação do protótipo inicial com a catraca (Figura 23), o projeto avançou para a montagem final dos componentes definitivos do sistema embarcado IFB ACCESS. Esta fase de construção foi documentada em três resultados principais, detalhados a seguir.

O primeiro resultado é o hardware final do sistema. A Figura 33 exibe a montagem dos componentes eletrônicos, conectados diretamente ao Arduino Mega 2560, seguindo o circuito projetado na metodologia (Figura 19).

Figura 33 – Protótipo do hardware do projeto



Fonte: foto dos autores.

Para acondicionar este circuito, foi fabricado um invólucro, cujo resultado é apresentado na Figura 34. A imagem demonstra a caixa finalizada, produzida em MDF com corte a laser CNC e complementada por uma tampa de acrílico, conforme o plano de corte da Figura 20.

Figura 34 – Invólucro em MDF e tampa de acrílico

Fonte: foto dos autores.

Por fim, a etapa de montagem foi concluída com a integração do hardware ao invólucro e a instalação do conjunto na catraca. A Figura 35 ilustra a obra completada, com o dispositivo já implementado em seu ambiente de operação.

Figura 35 – Sistema embarcado IFB ACCESS implantado na catraca

Fonte: foto dos autores.

4.3 Resultados do teste-piloto

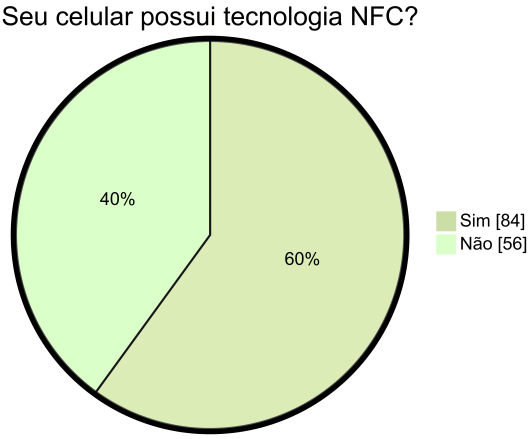
O formulário para recrutamento de participantes (Apêndice A) para o sistema obteve 168 respostas de usuários do ensino superior e médio, docentes e equipe administrativa do

Instituto. Dentre os respondentes, 77% utilizam Android, enquanto 23% possuem iPhone (iOS) (Figura 36). Em relação à tecnologia NFC, 60% dos usuários Android afirmaram que seus celulares possuem essa funcionalidade, enquanto 40% não a possuem (Figura 37).

Figura 36 – Distribuição de sistemas operacionais móveis

Fonte: elaborado pelos autores.

Figura 37 – Distribuição de celulares com tecnologia NFC



Fonte: elaborado pelos autores.

É importante ressaltar que, inicialmente, o sistema IFB ACCESS foi desenvolvido apenas para dispositivos Android com suporte a NFC, o que levou à exclusão de participantes com iOS ou sem a funcionalidade NFC durante o processo de seleção para os testes. No entanto, as informações coletadas sobre os sistemas operacionais mais utilizados pelos frequentadores do campus serão valiosas para futuras expansões ou melhorias do sistema.

O Quadro 4 sistematiza a avaliação feita pelos 15 participantes após o termino das coletas dos *feedbacks* no preenchimento do questionário SUS.

Quadro 4 – Respostas dos 15 participantes sobre cada afirmativa do questionário SUS

Afirmativas SUS	Escala (1 a 5)				
	1	2	3	4	5
1				3	12
2	11	4			
3	1				14
4	12		3		
5	1	1		2	11
6	10	1	2	2	
7				4	11
8	13	2			
9				1	14
10	10	2	2	1	

Fonte: elaborado pelos autores.

Para a avaliação da solução proposta, foi selecionado um grupo de 15 usuários que já haviam utilizado o sistema durante o período de testes. O perfil dos participantes era composto por 11 discentes do curso de Sistemas para Internet, 1 docente e 3 servidores técnico-administrativos.

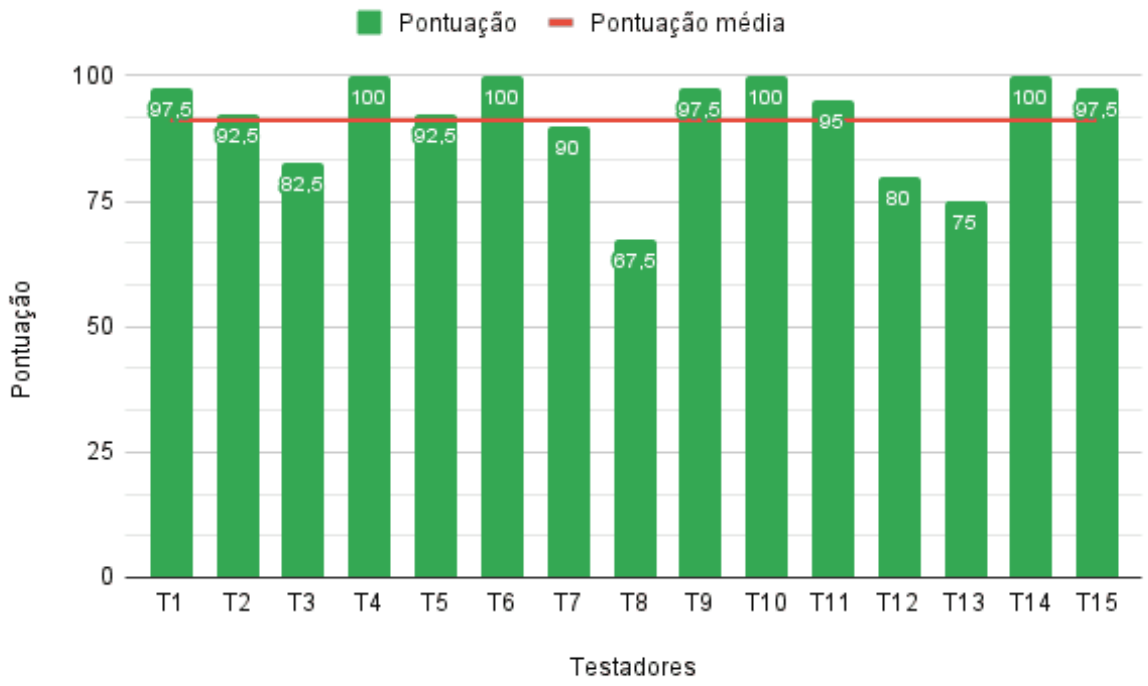
A análise dos dados coletados por meio do questionário SUS (Apêndice C)[1], demonstra uma avaliação favorável da solução proposta. O questionário foi estruturado de forma que as afirmativas ímpares são positivas e as pares, negativas. Conforme Brooke[43], essa formatação foi criada para evitar vieses, forçando os entrevistados a lerem atentamente cada item.

Verificou-se um consenso positivo em cinco das dez assertivas, o que evidencia pontos fortes do sistema: a totalidade dos respondentes manifestou o desejo de uso frequente, a confiança durante a operação e a percepção de uma rápida curva de aprendizado. De forma complementar, todos os participantes discordaram das afirmações sobre o sistema ser desnecessariamente complexo ou de difícil manipulação.

Em contrapartida, outros itens apresentaram divergência nas respostas. Embora 93,3% dos usuários tenham classificado o sistema como fácil de usar, um respondente (6,7%) discordou veementemente. As maiores divergências ocorreram nos itens sobre consistência e necessidade de aprendizado, em que uma minoria de 13,3% relatou uma experiência negativa, apontando a existência de pontos de atrito que justificam investigações futuras para o aprimoramento da solução.

[1] A planilha com os resultados completos está disponível no link encurtado do google planilhas em: https://is.gd/sbQUUj

Figura 38 – Pontuação final SUS de cada participante



Fonte: elaborado pelos autores.

Analisando a Figura 38, nota-se que a pontuação SUS mais baixa foi de 67,5 , obtida pelo participante T8. Já a maior pontuação, 100 , foi alcançada por quatro participantes: T4, T6, T10 e T14. A linha vermelha horizontal representa a média de todas as pontuações do estudo.

Considerando que a pontuação média de referência do SUS (*System Usability Scale*) é 68, onde valores acima são considerados positivos e abaixo são negativos, a grande maioria dos participantes avaliou a interface de forma positiva. Apenas um participante (T8) ficou ligeiramente abaixo desse marco, com 67,5 pontos. A média das pontuações de todos os 15 participantes neste estudo foi de 91,2 ± 10,2.

Ao classificar a pontuação média de 91,2 segundo o modelo proposto por Bangor *et al.*[48], observa-se o seguinte:

- **Faixas de Aceitabilidade:** A pontuação média se enquadra na faixa "Aceitável", a mais alta da escala.
- **Escala de Notas:** A média de 91,2 corresponde à nota "A", atribuída a pontuações entre 90 e 100.
- **Classificação com Adjetivos:** O resultado pode ser classificado como "Excelente"ou "Melhor Imaginável".

Dessa forma, a análise dos resultados obtidos demonstra que a pontuação média de 91,2 atingiu um desempenho de excelência. É possível concluir, com base na aplicação do questionário SUS, que a interface de usuário avaliada apresenta uma usabilidade de alta qualidade.

4.4 Discussão

A análise dos resultados do teste-piloto demonstra que o sistema IFB ACCESS não apenas atingiu seus objetivos técnicos, mas também obteve uma aceitação por parte dos usuários finais. A discussão a seguir contextualiza esses achados em relação aos trabalhos correlatos, destacando as contribuições e os diferenciais deste projeto.

A implementação da emulação de credenciais via HCE é um ponto central deste trabalho, uma abordagem técnica também explorada por Bispo[11] e Basyari *et al.*[9]. No entanto, um diferencial significativo do IFB ACCESS é a sua validação em um cenário prático e com usuários reais da instituição, superando o escopo de testes em ambientes de laboratório ou como provas de conceito, como os realizados por Bispo[11]. A aplicação do questionário SUS, que resultou em uma avaliação quantitativa, oferece uma evidência de usabilidade e aceitação que vai além das demonstrações funcionais apresentadas nos trabalhos anteriores.

O projeto também avança em relação a outras propostas da literatura. Enquanto Souza e Martins[10] concluíram seu trabalho com um protótipo que ainda necessitava do desenvolvimento de um aplicativo próprio, o IFB ACCESS entregou uma solução completa, com *software* cliente e servidor totalmente funcionais. Da mesma forma, o sistema concretiza a evolução sugerida por Silva[13], que propôs um sistema baseado em RFID com a possibilidade futura de migrar para NFC. Ao adotar diretamente a tecnologia NFC com HCE, o IFB ACCESS elimina a dependência de credenciais físicas (cartões ou tags), oferecendo uma conveniência superior e modernizando a interação do usuário com o sistema de controle de acesso.

Os dados coletados na fase de recrutamento (Figura 36 e 37) também forneceram informações importantes. A constatação de que 77% dos respondentes utilizam o sistema operacional *Android* valida a escolha da plataforma para o desenvolvimento inicial. Contudo, esses mesmos dados revelam os desafios para a universalização do sistema: 23% dos usuários possuem iOS e 40% dos usuários Android não dispõem de tecnologia NFC. Essa limitação de alcance aproxima a nossa discussão da solução proposta por Silva *et al.*[12], que implementaram um sistema híbrido com NFC e *QR Code* para ampliar a compatibilidade. Nossos resultados, portanto, reforçam empiricamente a necessidade de desenvolver métodos de acesso alternativos, como o *QR Code* ou *Bluetooth*, conforme sugerido na seção de trabalhos futuros, para garantir que toda a comunidade possa ser incluída.

5 CONSIDERAÇÕES FINAIS

Com base nos resultados obtidos, o projeto IFB ACCESS conclui com êxito o seu objetivo geral de contribuir para a melhoria da segurança no Instituto Federal de Brasília por meio do desenvolvimento de um sistema de controle de acesso via NFC. O trabalho superou o desafio inicial de um sistema de catracas inoperante e dependente de terceiros, desenvolvendo uma solução própria com hardware e software que reaproveita a infraestrutura existente.

A implementação de um protótipo funcional no campus, os testes-piloto e a comissão do projeto validaram a viabilidade e eficácia da abordagem. Os resultados dos testes de usabilidade foram majoritariamente positivos, com 100% dos participantes afirmando que gostariam de usar o sistema com frequência, considerando-o fácil de usar e sentindo-se confiantes durante a operação.

5.1 Trabalhos futuros

Como trabalhos futuros, sugere-se a expansão da compatibilidade do sistema para atender a um público maior. Nesse sentido, propõem-se as seguintes melhorias:

- **Expansão de funcionalidades:** Ativar recursos que foram planejados nos requisitos do sistema, como o envio de notificações de entrada e saída aos responsáveis dos estudantes, agregando mais valor e segurança para a comunidade escolar.
- **Versão para o sistema operacional iOS:** Desenvolver a versão para a plataforma iOS, que corresponde a 23% dos usuários no campus. Visto que a tecnologia de emulação de cartão (HCE) via NFC possui restrições neste sistema devido às politicas de controle da Apple, que restringem o acesso de desenvolvedores de terceiros à funcionalidade de emulação de cartão do chip NFC, priorizando seu uso para serviçes proprietários como o Apple Pay, propõe-se a utilização de tecnologias alternativas de comunicação por proximidade, como o *Bluetooth*, que já é explorado com sucesso por outras empresas e cujos testes preliminares já foram realizados pela equipe do projeto.
- **Métodos alternativos para dispositivos sem NFC:** Para incluir os 40% de usuários da plataforma *Android* que não possuem a tecnologia NFC, recomenda-se a implementação de métodos de acesso alternativos. Tecnologias como o *QR Code*, já explorado em trabalhos similares, ou o próprio *Bluetooth* poderiam ser adotadas, garantindo maior abrangência ao sistema.
- **Testes em larga escala e expansão:** Realizar testes de longa duração com um número maior de usuários comprometidos para monitorar a estabilidade, a performance e o consumo de recursos do sistema em um cenário de uso contínuo. Além disso,

planejar a expansão da solução para outras catracas do campus e, posteriormente, para outras unidades do Instituto Federal de Brasília (IFB).

- **Refinamento do *hardware*:** Evoluir o protótipo do *hardware*, atualmente montado com uma placa de desenvolvimento *Arduino*, para uma versão final com uma Placa de Circuito Impresso (PCB) dedicada. Isso resultaria em um dispositivo mais compacto, robusto, profissional e de manutenção simplificada para ser instalado nas catracas.

REFERÊNCIAS

1 SOUSA, G. C. **Ocorreram 36 ataques a escolas no Brasil entre 2002 e 2023**. 2024. Disponível em: <https://jornal.usp.br/atualidades/ocorreram-36-ataques-a-escolas-no-brasil-entre-2002-e-2023/>. Acesso em: 25 de abr. de 2024.

2 ESTADÃO. **Brasil registra 9 ataques em escolas neste ano e atinge patamar recorde; relembre casos**. 2023. Disponível em: <https://www.estadao.com.br/educacao/brasil-chega-a-nove-ataques-a-escolas-no-ano-patamar-recorde-relembre-casos-nprm/>. Acesso em: 29 de jul. de 2024.

3 EXAME. **Ataques em escolas no país mataram 35 alunos e professores até 2022, diz relatório**. 2023. Disponível em: <https://exame.com/brasil/ataques-em-escolas-no-pais-mataram-35-alunos-e-professores-ate-2022-diz-relatorio/>. Acesso em: 29 de jul. de 2024.

4 MARCONDES, J. S. **Controle de Acesso: O que é? Qual o Objetivo? Tipos e Funcionamento**. 2020. Disponível em: <https://gestaodesegurancaprivada.com.br/controle-de-acesso-o-que-e-objetivos-tipos-funcionamento>. Acesso em: 20 de abr. de 2024.

5 REMSDAQ. **Enhancing Security in Education with Access Control**. 2024. Disponível em: <https://www.remsdaq.com/latest-news/enhancing-security-in-education-with-access-control>. Acesso em: 18 de nov. de 2024.

6 STELZER, J. *et al.* Segurança nas instituições federais de ensino. In: **XVI COLOQUIO INTERNACIONAL DE GESTIÓN UNIVERSITARIOS - CIGU**. [S.l.: s.n.], 2016. p. 1–12. ISBN 978-85-68618-02-8.

7 SANTAELLA, L.; GALA, A.; POLICARPO, C.; GAZONI, R. **Desvelando a Internet das Coisas**. 2013. Disponível em: <https://www.researchgate.net/publication/327601891>.

8 PALMEIRA, E. J. S. de S.; FERNANDES, L. R. de A. **Controle de acesso para estádios de futebol utilizando tecnologia NFC**. 2013. 1-84 p.

9 BASYARI, R.; NASUTION, S.; DIRGANTARA, B. Implementation of host card emulation mode over android smartphone as alternative iso 14443a for arduino nfc shield. In: **ICCEREC 2015 - International Conference on Control, Electronics, Renewable Energy and Communications**. [S.l.: s.n.], 2015. p. 160–165. ISBN 9781479989751.

10 SOUZA, J. V. da S.; MARTINS, N. C. **Proposta de controle de acesso e rotina hospitalar baseado em NFC e banco de dados**. 2017. 1-65 p.

11 BISPO, B. **Sistema de controle de acesso via RFID/NFC**. 2019.

12 SILVA, D. S. *et al.* Sistema para controle de acesso à universidade utilizando nfc e qr code / university access control system using nfc and qr code. **Brazilian Journal of Development**, South Florida Publishing LLC, v. 8, p. 1–7, 5 2022.

13 SILVA, A. R. S. da. **IF ACCESS: Sistema de controle de acesso eletrônico utilizando tecnologia RFID e Microcontrolador**. 2022. 1-50 p.

14 EQUIPE TOTVS. **NFC: para que serve, vantagens e como aplicar a tecnologia em seu negócio**. 2021. Disponível em: <https://www.totvs.com/blog/inovacoes/nfc/>. Acesso em: 13 de mai. de 2025.

15 FONSECA, S. V. P.; AZEVEDO, W. G.; ALVES, G. B.; JULIO, J. C. P. Nfc (near field communication) entendimento e aceitação. **RCMOS - Revista Científica Multidisciplinar O Saber**, Editora Aluz, v. 2, p. 350–355, 1 2022.

16 SILVA, L. T. D. **Internet das coisas: RFID e NFC, conceitos e aplicações**. 2014. Disponível em: <https://www.academia.edu/36694832/INTERNET_DAS_COISAS_RFID_E_NFC_CONCEITOS_E_APLICA%C3%87%C3%94ES>.

17 NASSAR, V.; VIEIRA, M. L. H. **A internet das coisas com as tecnologias RFID e NFC**. 2014. 1-13 p. Disponível em: <https://pdf.blucher.com.br/designproceedings/11ped/00043.pdf>.

18 ANDROID. **Host-based card emulation overview**. 2023. Disponível em: <https://developer.android.com/develop/connectivity/nfc/hce>. Acesso em: 16 de nov. de 2023.

19 ZIGNANI, A.; SEALY, P. **NFC Forum Survey Results**. 2024. 1-12 p. Disponível em: <https://nfc-forum.org/learn/resources/2024-abi-usage-and-adoption-study/>.

20 ARDUINO. **What is Arduino?** 2018. Disponível em: <https://www.arduino.cc/en/Guide/Introduction>. Acesso em: 16 de mai. de 2024.

21 STACK OVERFLOW. **Most popular technologies language**. 2023. Disponível em: <https://survey.stackoverflow.co/2023/#most-popular-technologies-language>. Acesso em: 13 de jun. de 2024.

22 PYTHON. **What is Python? Executive Summary**. 2024. Disponível em: <https://www.python.org/doc/essays/blurb/>. Acesso em: 16 de mai. de 2024.

23 PALLETS. **Flask documentation**. 2025. Disponível em: <https://flask.palletsprojects.com/en/stable/>. Acesso em: 01 de jul. de 2025.

24 AVRAM, A. **Kotlin agora é uma linguagem oficial no Android**. 2017. Disponível em: <https://www.infoq.com/br/news/2017/06/android-kotlin/>. Acesso em: 05 de jun. de 2024.

25 ONGKO, A. S. **Getting Started With MVVM in Jetpack Compose**. 2022. Disponível em: <https://medium.com/better-programming/mvvm-in-jetpack-compose-part-4-fe757a1a1b84>. Acesso em: 29 de jun. de 2025.

26 KTOR. **Creating a cross-platform mobile application**. 2025. Disponível em: <https://ktor.io/docs/client-create-multiplatform-application.html>. Acesso em: 29 de jun. de 2025.

27 VORA, I. **Jetpack Compose vs XML: A comprehensive comparison for Android UI development**. 2024. Disponível em: <https://www.aubergine.co/insights/jetpack-compose-vs-xml-a-comprehensive-comparison-for-android-ui-development>. Acesso em: 29 de jun. de 2025.

28 RIBEIRO, A. L. S. **O que é Firebase? Para que serve, principais característica e um Guia dessa ferramenta Google**. 2023. Disponível em: <https://www.alura.com.br/artigos/firebase>. Acesso em: 01 de jul. de 2025.

29 SEIDOR. **O que é Firebase? Quais vantagens oferece em 2023 para nossos apps?** 2023. Disponível em: <https://www.seidor.com/pt-br/blog/o-que-e-firebase#firebase-authentication>. Acesso em: 01 de jul. de 2025.

30 GOMES, R. **Docker para Desenvolvedores**. Leanpub, 2019. 1-180 p. Disponível em: <http://leanpub.com/dockerparadesenvolvedores>.

31 DOCKER. **What is a container?** 2024. Disponível em: <https://www.docker.com/resources/what-container/>. Acesso em: 13 de jun. de 2024.

32 CAMPOS, E. V. **IFB ACCESS: Sistema de Gerenciamento**. Monografia (Trabalho de Conclusão de Curso (Tecnologia em Sistemas para Internet)) — Instituto Federal de Brasília – Campus Brasília, Brasília, 2025.

33 MINISTÉRIO DA EDUCAÇÃO. **Manual de Aplicação da Marca Instituto Federal**. [S.l.], 2015. 21 p. Disponível em: <https://redefederal.mec.gov.br/images/pdf/manual.pdf>. Acesso em: 16 de jan. de 2025.

34 ANDRADE, A. P. de. **O que é o React Native?** 2020. Disponível em: <https://www.treinaweb.com.br/blog/o-que-e-o-react-native>. Acesso em: 04 de ago. de 2024.

35 PASSKIT. **Custom NFC HCE with Google/Apple Wallet**. 2024. Disponível em: <https://stackoverflow.com/questions/77799645/custom-nfc-hce-with-google-apple-wallet>. Acesso em: 18 de mai. de 2024.

36 CEZAR, P. **API REST: Princípios e boas práticas para serviços RESTful**. 2018. Disponível em: <https://smarti.blog.br/api-rest-principios-boas-praticas-para-arquiteturas-restful/>. Acesso em: 04 de ago. de 2024.

37 ARDUINO STORE. **UNO Mega 2560**. 2024. Disponível em: <https://store.arduino.cc/products/arduino-mega-2560-rev3>. Acesso em: 13 de jun. de 2024.

38 ELECHOUSE. **PN532 V3**. 2008. Disponível em: <https://www.elechouse.com/elechouse/images/product/PN532_module_V3/PN532_%20Manual_V3.pdf>. Acesso em: 13 de jun. de 2024.

39 INDIA MART. **2 Channel Relay Module**. 2024. Disponível em: <https://www.indiamart.com/proddetail/2-channel-relay-module-19562460291.html>. Acesso em: 30 de jul. de 2024.

40 WOLPAC. **Wolstar III**. 2024. Disponível em: <https://www.wolpac.com.br/pt/product/wolstar-3>. Acesso em: 30 de jul. de 2024.

41 HU INFINITO. **Módulo Ethernet - ENC28J60**. Disponível em: <https://www.huinfinito.com.br/comunicacao-sem-fio-wireless/493-modulo-ethernet-enc28j60.html>. Acesso em: 13 de jan. de 2025.

42 ELECHOUSE. **PN532 - NFC library for Arduino using PN532**. Disponível em: <https://github.com/elechouse/PN532>. Acesso em: 13 de jan. de 2025.

43 BROOKE, J. SUS: A quick and dirty usability scale. In: JORDAN, P. W.; THOMAS, B.; WEERDMEESTER, B. A.; MCCLELLAND, I. L. (Ed.). **Usability Evaluation in Industry**. London: Taylor Francis, 1996. p. 189–194.

44 LIKERT, R. **A Technique for the Measurement of Attitudes**. New York: Columbia University Press, 1932. (Archives of Psychology, 140).

45 SILVA, A. D.; CAMARGOS, J. P. D. R. d.; OLIVEIRA, F. H. M. **IFB ACCESS: SISTEMA PARA CONTROLE DE ACESSO À INSTITUIÇÃO UTILIZANDO NFC**. Zenodo, 2024. Disponível em: <https://doi.org/10.5281/zenodo.14052906>.

46 SILVA, A. D.; CAMARGOS, J. P. D. R. d.; OLIVEIRA, F. H. M. IFB ACCESS: sistema para controle de acesso à instituição utilizando NFC. In: **Anais do Simpósio de Integração, Inovação e Tecnologia**. Brasília, DF: IFB Campus Brasília, 2024. Acesso em: 01 de julho de 2025. Disponível em: <https://is.gd/siitifbaccess>.

47 GOOGLE PLAY. **Requisitos de teste de aplicativos para novas contas de desenvolvedor pessoais**. 2025. Disponível em: <https://support.google.com/googleplay/android-developer/answer/14151465?hl=pt-BR&sjid=12194453875449379346-SA#zippy=%2Csummary-of-testing-requirements-per-track>. Acesso em: 15 de jun. de 2025.

48 BANGOR, A.; KORTUM, P. T.; MILLER, J. T. Determining what individual sus scores mean: Adding an adjective rating scale. **Journal of usability studies**, Usability Professionals' Association, v. 4, n. 3, p. 114–123, 2009.

APÊNDICE A – Formulário de convite para participação nos testes

Convite para participar dos testes do IFB ACCESS: Sistema para controle de acesso à instituição utilizando NFC

O IFB ACCESS se trata de um trabalho de conclusão de curso do curso superior de Tecnologia em Sistemas para Internet do Instituto Federal de Brasília Campus Brasília.

Este formulário tem como objetivo convidar a comunidade do IFB para testar o sistema e também reunir informações sobre os sistemas operacionais utilizados pelas pessoas que frequentam o campus e que tenham acesso à tecnologia NFC.

Os testes consistirão em os participantes baixarem o aplicativo desenvolvido e utilizarem o sistema de controle de acesso instalado na catraca designada sempre que entrarem ou saírem da instituição. O objetivo é avaliar a eficácia do sistema e coletar *feedback* dos participantes, identificando possíveis falhas, melhorias e benefícios do sistema.

Termos de Uso e Política de Privacidade

Estudantes envolvidos:

- Arthur Damacena Silva (arthur.silva7@estudante.ifb.edu.br)
- João Pedro Della Rocca de Camargos (joao.camargos@estudante.ifb.edu.br)
- Eduardo Vieira Campos (eduardo57082@estudante.ifb.edu.br)

Docentes orientadores:

- Dr. Fábio Henrique M. Oliveira (fabio.oliveira@ifb.edu.br)
- Dr. Caio Moura Daoud (caio.daoud@ifb.edu.br)

Além dos estudantes e orientadores, o projeto conta com o apoio da Comissão IFB ACCESS por meio da Portaria nº 120/2024 composta pelos servidores(as): Ana Roberta, Davi Lucas e Ramon Augusto. Também da CDTI, Plínio e Peterson.

IFB Campus Brasília

* Indica uma pergunta obrigatória

1. E-mail *

2. Qual seu sistema operacional? *

Marcar apenas uma oval.

- ◯ Android *Pular para a pergunta 3*
- ◯ iPhone (iOS) *Pular para a seção 4 ()*
- ◯ Outro: _____

3. O que é NFC: *

A tecnologia NFC permite a comunicação por aproximação entre dispositivos, como celulares e leitores.

Exemplos de uso do NFC:

- Pagamentos por aproximação, como no Google Pay ou Apple Pay;

- Transferência de arquivos ou contatos apenas encostando dois dispositivos;

- Uso de bilhetes eletrônicos ou cartões de transporte público aproximando o celular no leitor.

Verifique nas configurações do seu celular ou consulte o site do fabricante para confirmar se o seu modelo é compatível com a tecnologia NFC!

Seu celular possui tecnologia NFC (Near Field Communication)?

Marcar apenas uma oval.

- ◯ Sim *Pular para a pergunta 4*
- ◯ Não *Pular para a seção 5 ()*

4. **Você teria interesse em participar dos testes do sistema?** *

Independentemente da resposta, marque a opção correspondente e envie o formulário. Obrigado!

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

Nesta versão do sistema, ainda não é possível utilizar dispositivos iPhone para usufruir do sistema de controle de acesso.

No entanto, essa informação será essencial para nosso levantamento, ajudando a identificar a porcentagem de usuários de cada sistema operacional.

Clique no botão **"Enviar"** para registrar sua contribuição ao trabalho. Agradecemos sua ajuda!

Para participar dos testes desta versão do sistema, é necessário que seu smartphone seja compatível com a tecnologia NFC.

Mesmo assim, suas respostas às perguntas anteriores serão de grande valor para o nosso trabalho.

Clique no botão **"Enviar"** para registrar sua contribuição ao trabalho. Agradecemos sua ajuda!

Obrigado pelo interesse em participar! No momento, nosso sistema inicialmente é compatível apenas com dispositivos Android que possuem tecnologia NFC. Mas não se preocupe, continuamos trabalhando para expandir a compatibilidade no futuro. Fique de olho nas novidades!

Clique no botão **"Enviar"** para registrar sua contribuição ao trabalho. Agradecemos sua ajuda!

APÊNDICE B – Termos de Uso e Política de Privacidade

1. **Introdução**
   O aplicativo “IFB ACCESS” é desenvolvido com o objetivo de controlar o acesso às instalações do IFB Instituto Federal de Brasília Campus Brasília) - Via L2 Norte, SGAN 610 (610 Norte), Módulo D, E, F e G. Brasília/DF. CEP: 70830-450.

   Ao utilizar este aplicativo, o usuário concorda com os termos descritos nesta Política de Privacidade e Termos de Uso, além de consentir com o tratamento de seus dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).

2. **Coleta de Dados Pessoais**
   O “IFB ACCESS” pode coletar as seguintes informações pessoais durante o uso do aplicativo:
   - **Informações de Identificação Pessoal:** nome, e-mail, CPF e matrícula.
   - **Informações de Acesso:** histórico de acessos ao IFB.

3. **Finalidade da Coleta de Dados**
   Os dados pessoais coletados serão utilizados exclusivamente para os seguintes fins:
   - Garantir a identificação e segurança no acesso às instalações do IFB.
   - Prover funcionalidades relacionadas ao funcionamento do “IFB ACCESS”.
   - Cumprir com obrigações legais e regulatórias.

4. **Direitos dos Usuários**
   O usuário tem o direito de acessar, corrigir, atualizar ou excluir seus dados pessoais a qualquer momento. Para exercer esses direitos, o usuário deve entrar em contato com nossa equipe de suporte, através dos canais disponibilizados no aplicativo.

5. **Consentimento**
   Ao utilizar o “IFB ACCESS” e fornecer seus dados pessoais, o usuário consente com a coleta e o processamento de seus dados conforme descrito nesta Política de Privacidade.

6. **Segurança dos Dados**
   O “IFB ACCESS” adota medidas de segurança adequadas para proteger os dados pessoais dos usuários contra acessos não autorizados, perda, divulgação ou alteração. Contudo, nenhuma medida de segurança é infalível, e não podemos garantir a total segurança dos dados.

7. **Tecnologia NFC**
   O “IFB ACCESS” utiliza a tecnologia NFC (Near Field Communication) para controlar o

acesso às instalações do IFB. Para acessar as instalações, o usuário deve aproximar seu dispositivo habilitado ao leitor NFC na catraca. Essa tecnologia é rápida, segura e prática, permitindo um acesso eficiente às dependências do IFB.

8. **Alterações na Política de Privacidade**
   A presente Política de Privacidade pode ser atualizada periodicamente para refletir mudanças nas práticas de coleta e processamento de dados. Recomendamos que o usuário revise esta política regularmente. Caso haja alterações significativas, o usuário será informado por meio de notificações no aplicativo ou outro meio adequado.

9. **Contato**
   Para dúvidas, sugestões ou solicitações relacionadas a esta Política de Privacidade ou aos Termos de Uso, o usuário pode entrar em contato com a equipe de desenvolvedores do “IFB ACCESS” através dos e-mails listados no aplicativo.

Esses Termos de Uso e Política de Privacidade têm como objetivo garantir a transparência no tratamento dos dados pessoais e a conformidade com as exigências legais, promovendo a segurança e privacidade dos usuários do “IFB ACCESS”.

APÊNDICE C – Resultados do *feedback* do Sistema de Controle de Acesso

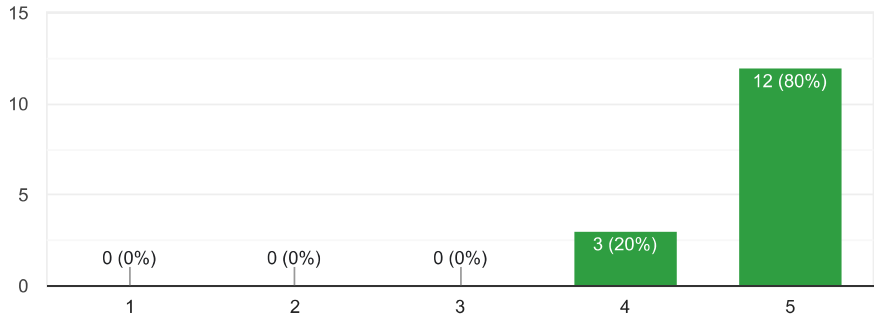
Feedback do Sistema de Controle de Acesso - IFB ACCESS

15 respostas

Publicar análise

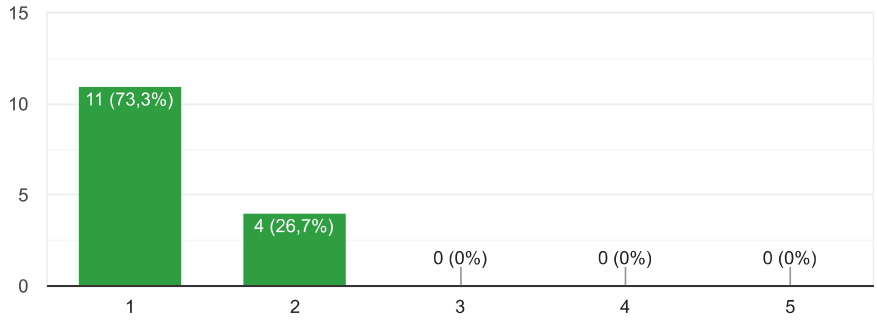
Eu acho que gostaria de usar esse sistema com frequência. Copiar

15 respostas



Eu acho o sistema desnecessariamente complexo. Copiar

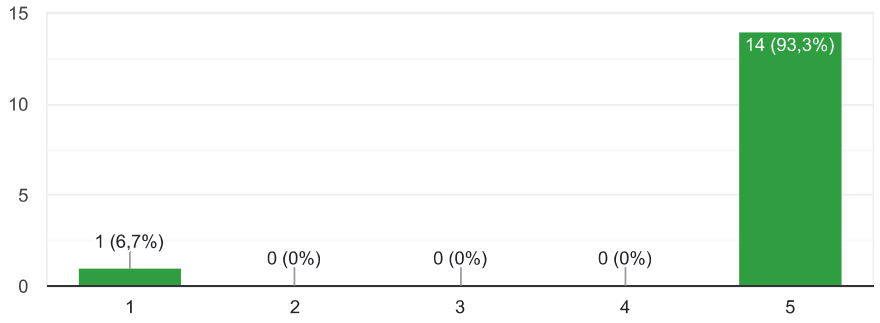
15 respostas



Eu achei o sistema fácil de usar.

Copiar

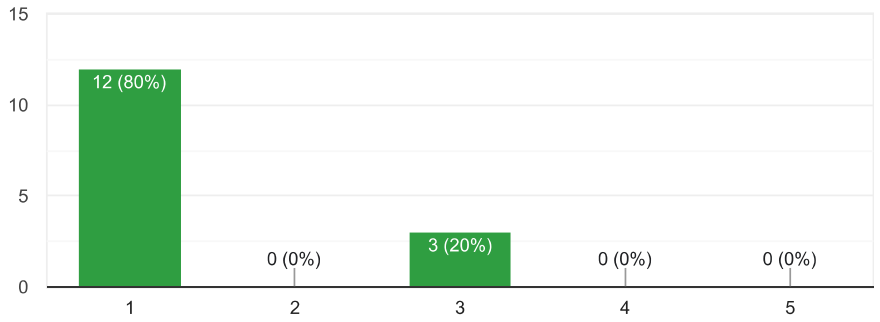
15 respostas



Eu acho que precisaria de ajuda de uma pessoa com conhecimentos técnicos para usar o sistema.

Copiar

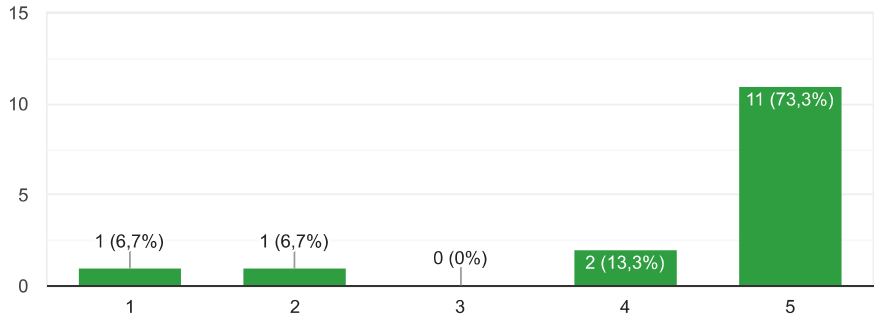
15 respostas



Eu acho que as várias funções do sistema estão muito bem integradas.

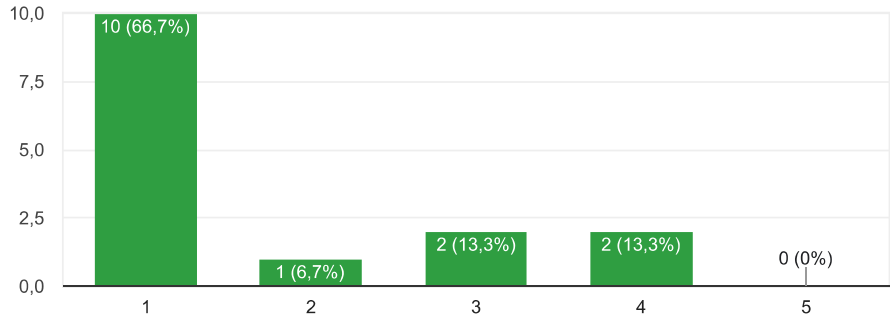
Copiar

15 respostas



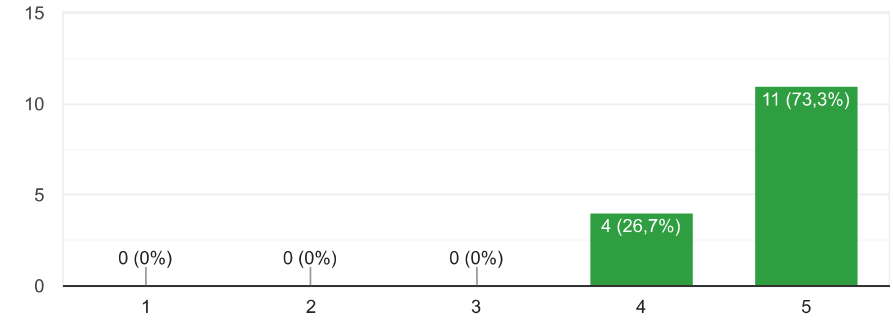
Eu acho que o sistema apresenta muita inconsistência. Copiar

15 respostas



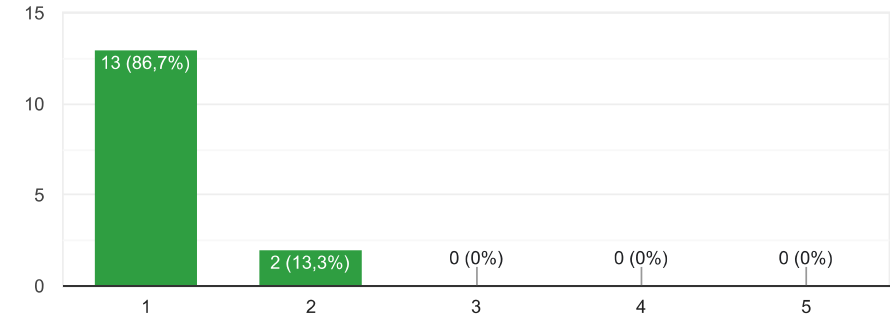
Eu imagino que as pessoas aprenderão como usar esse sistema rapidamente. Copiar

15 respostas



Eu achei o sistema atrapalhado de usar. Copiar

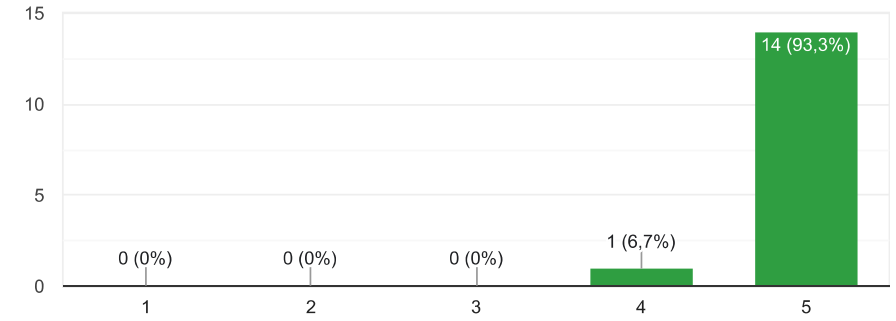
15 respostas



Eu me senti confiante ao usar o sistema.

Copiar

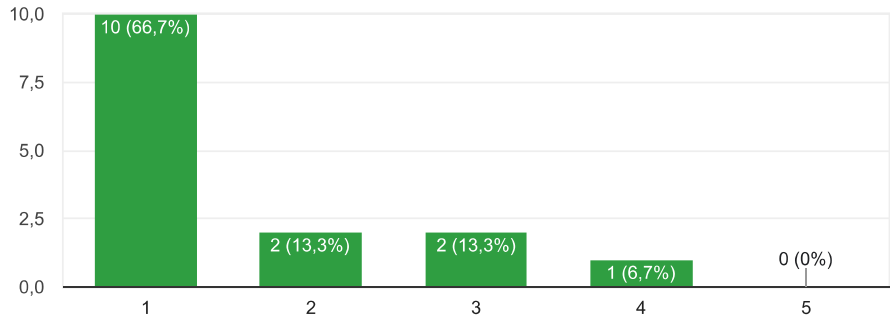
15 respostas



Eu precisei aprender várias coisas novas antes de conseguir usar o sistema.

Copiar

15 respostas

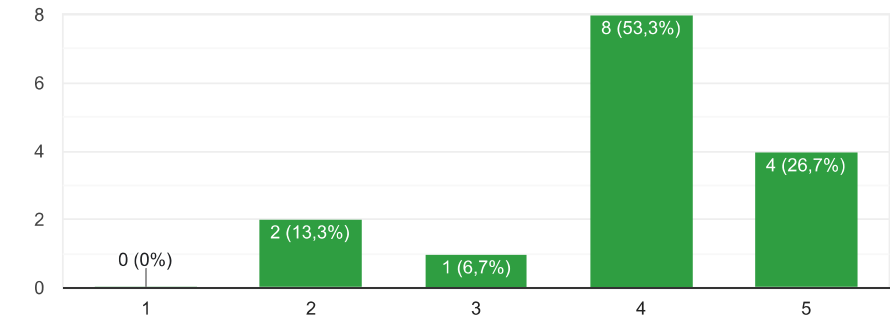


Seção 2: Sobre Eficiência

O sistema reconhece minha credencial de forma rápida.

Copiar

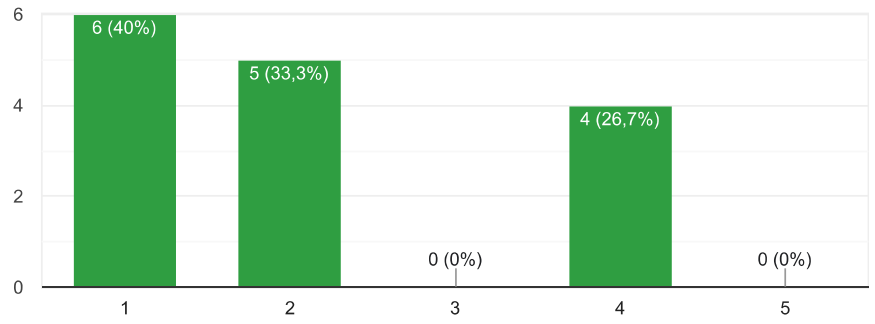
15 respostas



O sistema demora muito para processar meu acesso.

Copiar

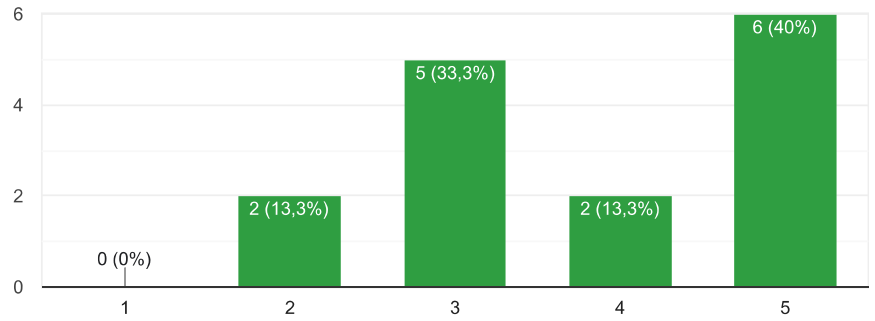
15 respostas



A autenticação via NFC foi mais prática que outros métodos que já usei.

Copiar

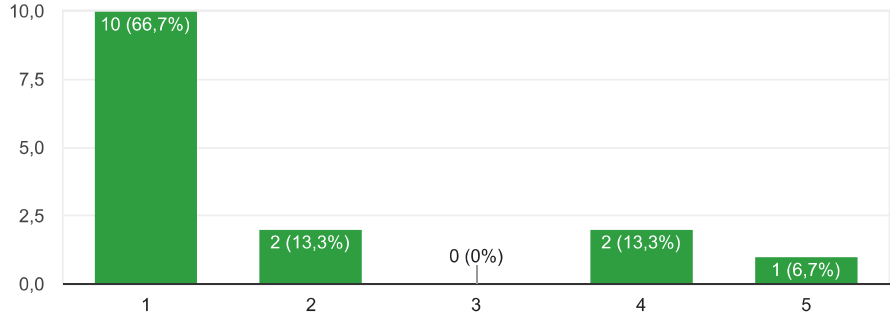
15 respostas



Precisei tentar várias vezes para conseguir acessar a instituição.

Copiar

15 respostas



APÊNDICE D – Email com informações e guia para iniciar os testes

INSTITUTO FEDERAL
BRASÍLIA

IFB ACCESS - Informações e guia para os testes

Arthur Silva <arthur.silva7@estudante.ifb.edu.br> 10 de fevereiro de 2025 às 15:13

Bem-vindo aos testes do IFB ACCESS

Agradecemos seu interesse na participação nos primeiros testes do nosso sistema. Estamos animados com esta fase e contamos com você para aprimorar a experiência.

Logo abaixo o conteúdo está dividido em:

- Download do Aplicativo IFB ACCESS e Primeiros Passos
- Realizando os Testes
- Feedback
- Dúvidas

‼️ Download do Aplicativo IFB ACCESS e Primeiros Passos

Todo o guia para realizar o download e realizar os primeiros passos no aplicativo está no link a seguir:

Clique aqui para acessar o link!

💡 Realizando os Testes:

Os testes consistem principalmente em utilizar o aplicativo IFB ACCESS, realizando login e explorando suas funcionalidades, como o uso do NFC e o registro de acessos.

As principais funcionalidades que você deve testar são:

- Realizar login na sua conta do aplicativo.
- Garantir a comunicação entre o celular (com o app logado) e o leitor da catraca para liberar o acesso.

Quaisquer erros, problemas ou dúvidas poderão ser registrados por meio de um formulário. Sua contribuição será de extrema importância para o crescimento do projeto IFB ACCESS."

🗣️ Feedback:

A sua opinião é essencial! Após os testes, pediremos que compartilhe suas impressões, sugestões e possíveis problemas encontrados. Enviaremos um formulário após alguns dias da realização dos testes através do seu email.

❓ Dúvidas?

Se tiver qualquer dúvida, entre em contato respondendo a este e-mail ou pelo endereço: arthur.silva7@estudante.ifb.edu.br

Atenciosamente,

Arthur Damacena Silva
Graduando em Tecnologia em Sistemas para Internet