UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FERNANDO TETSUYA DAFLON SHINOHARA

DESENVOLVIMENTO DE SISTEMA BASEADO EM IOT PARA CONTROLE DE ACESSO COM FECHADURAS ELETROMAGNÉTICAS

PONTA GROSSA

2022

FERNANDO TETSUYA DAFLON SHINOHARA

DESENVOLVIMENTO DE SISTEMA BASEADO EM IOT PARA CONTROLE DE ACESSO COM FECHADURAS ELETROMAGNÉTICAS

Development of system based on IoT to access control with electromagnetic locks

Trabalho de conclusão de curso de graduação apresentada como requisito para obtenção do título de Bacharel em Ciência da Computação da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Prof. Me. Rogério Ranthum.

PONTA GROSSA

2022

FERNANDO TETSUYA DAFLON SHINOHARA

DESENVOLVIMENTO DE SISTEMA BASEADO EM IOT PARA CONTROLE DE ACESSO COM FECHADURAS ELETROMAGNÉTICAS

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Bacharel em Ciência da Computação da Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 01 de novembro de 2022

_____

Rogério Ranthum
Mestrado
Universidade Tecnológica Federal do Paraná - Campus Ponta Grossa

_____

Geraldo Ranthum
Mestrado
Universidade Tecnológica Federal do Paraná - Campus Ponta Grossa

_____

Augusto Foronda
Doutorado
Universidade Tecnológica Federal do Paraná - Campus Ponta Grossa

PONTA GROSSA

2022

AGRADECIMENTOS

Inicialmente, agradeço a Deus por me dar forças para enfrentar todos os obstáculos encontrados ao longo da realização deste trabalho e da minha vida.

Aos meus pais, minha eterna gratidão por todo apoio na conquista dos meus sonhos e pelo esforço e dedicação para me proporcionar uma educação digna.

A minha querida esposa que me acompanhou e apoiou em todos os momentos de dificuldade enfrentados na realização do curso.

Ao meu orientador, professor e amigo, Rogério Ranthum, por todas as oportunidades de aprendizado e pelo acompanhamento no desenvolvimento deste trabalho.

E a todos os envolvidos, diretamente ou indiretamente, na minha formação, o meu muito obrigado.

RESUMO

A segurança pode ser interpretada como proteção de algo. Garantir segurança previne o manuseio de algo por uma pessoa não autorizada. Em um ambiente como, por exemplo, um espaço comercial, podem existir portas com fechaduras mecânicas tradicionais, porém, podem ser facilmente violadas. Com o intuito de maximizar a segurança e minimizar custos e impactos físicos negativos ao ambiente ou porta, foi desenvolvido um sistema completo (hardware e software) de controle de acesso com fechaduras eletromagnéticas que não interferem no funcionamento das fechaduras mecânicas comuns e utiliza conceitos de IoT (Internet of Things). Uma fechadura pode ser aberta ou fechada sem a necessidade, obrigatoriamente, de uma chave física e, além disso, devido a aplicação de conceitos IoT, foi integrado o uso de câmeras de segurança IP e toda ação realizada a partir do sistema é registrado no histórico para consulta. Para realização do trabalho foi feito um estudo de trabalhos correlatos para análise de aprimoramento do produto, planejamento e desenvolvimento da estrutura física e lógica das tecnologias utilizadas e implantação do produto a um ambiente real. O sistema pode se comportar de maneiras distintas de acordo com o ambiente aplicado, porém os resultados obtidos nos testes foram positivos, pois com o sistema em funcionamento foi possível controlar o acesso a um ambiente por meio de agendamento semanal para diversos usuários e as aplicações desenvolvidas possibilitaram a interação com a fechadura de maneira prática e segura. Devido a aplicação de conceitos IoT, é possível planejar possíveis aprimoramentos ao sistema.

Palavras-chave: sistemas de segurança; internet das coisas; fechaduras e chaves;

ABSTRACT

Security can be interpreted as protecting something. Ensuring security prevents the handling of something by an unauthorized person. In an environment such as, for example, a commercial space, there may be doors with traditional mechanical locks, but they can be easily breached. In order to maximize security and minimize costs and negative physical impacts to the environment or door, a complete access control system (hardware and software) was developed with electromagnetic locks that do not interfere with the operation of common mechanical locks and uses IoT concepts. (Internet of Things). A lock can be opened or closed without necessarily needing a physical key and, in addition, due to the application of IoT concepts, the use of IP security cameras was integrated and every action performed from the system is recorded in the history for consult. To carry out the work, a study of related works was carried out for the analysis of product improvement, planning and development of the physical and logical structure of the technologies used and implementation of the product in a real environment. The system can behave in different ways according to the applied environment, but the results obtained in the tests were positive, because with the system in operation, it was possible to control access to an environment through weekly scheduling for several users and the applications developed enabled interaction with the lock in a practical and safe way. Due to the application of IoT concepts, it is possible to plan possible improvements to the system.

Keywords: security systems; internet of things; locks and keys;

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

IoT	*Internet of Things*
LDAP	*Lightweight Directory Access Protocol*
UTFPR	Universidade Tecnológica Federal do Paraná
SGBD	Servidor e Gerenciador de Banco de Dados
Java EE	*Java Platform Enterprise Edition*
REST	*Representational State Transfer*
JSON	*JavaScript Object Notation*
SQL	*Structured Query Language*
HTTP	*Hypertext Transport Protocol*
HTML	*Hypertext Markup Language*
CSS	*Cascading Style Sheets*
API	*Application Programming Interface*
LAN	*Local Area Networks*
IP	*Internet Protocol*
Wi-Fi	*Wireless Fidelity*
UTP	*Unshielded Twisted Pair*
GPIO	*General Purpose Input/Output*
QRCode	*Quick Register Code*
COTED	Coordenação de Tecnologia na Educação

SUMÁRIO

1 INTRODUÇÃO

Internet das Coisas, ou mais conhecido do inglês, *Internet of Things* (IoT), é um termo utilizado para se referir a interconexão de vários objetos de diversas naturezas, como dispositivos eletrônicos, sensores, ou até mesmo seres não físicos, como dados e ambientes virtuais (KOSMATOS; TSELIKAS; BOUCOUVALAS, 2011).

As diversas aplicações em IoT podem ser categorizadas e uma destas categorias seria descrito como “Controle e Monitoramento”, onde o foco é o monitoramento e controle de dados relacionados aos estados dos objetos interconectados (LEE I.; LEE K., 2015). Neste contexto, uma possível aplicação é o controle de acesso a um ambiente a partir de abertura e fechamento de portas.

A segurança pode ser interpretada como proteção de algo. Garantir segurança previne o manuseio de algo por uma pessoa não autorizada. Em um ambiente como, por exemplo, um espaço comercial, podem existir portas com fechaduras mecânicas tradicionais, porém, podem ser facilmente violadas. Com o intuito de aprimorar estas fechaduras e maximizar a segurança, diversos autores apresentaram diferentes tipos de fechaduras, como fechaduras automáticas digitais com senha, com software, entre outros. (NEHETE et al., 2016). Estas fechaduras substituem a fechadura mecânica normalmente utilizada, consequentemente, podem gerar mais custos e inviabilizar a instalação dependendo do tipo de porta.

Este projeto propõe o desenvolvimento de um sistema de controle de acesso a fechaduras eletromagnéticas utilizando conceitos de IoT. As fechaduras eletromagnéticas podem ser instaladas em portas com fechaduras mecânicas sem danifica-las, ou seja, possibilita o uso de ambas fechaduras e em qualquer tipo de porta.

1.1 Objetivos

Os objetivos deste trabalho são descritos a seguir. A seção 1.1.1 descreve o objetivo geral do trabalho e a seção 1.1.2 descreve os objetivos específicos do trabalho.

1.1.1 Objetivo geral

Desenvolver um sistema completo (*hardware* e *software*) de controle de acesso aos ambientes com fechaduras eletromagnéticas utilizando conceitos de IoT.

1.1.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

- Analisar projetos correlatos.
- Planejar e desenvolver estrutura física do sistema.
- Desenvolver aplicação web para gerenciamento de informações e controle de acesso.
- Desenvolver aplicação para dispositivos móveis que permite acesso aos ambientes.
- Aplicar o sistema em um ambiente real para análise de funcionamento.

1.2 Justificativa

Uma porta é um dos primeiros recursos de defesa para manter a segurança física da casa. Se ela puder ser aberta facilmente, um ladrão poderá facilmente entrar e roubar o conteúdo da casa. A princípio, uma porta incorpora apenas uma chave física para tranca-la ou destranca-la, mas, com o avanço da tecnologia, este modelo foi inovado, a porta digital que pode trancar ou destrancar sem a necessidade de uma chave física (ANDREAS *et al*., 2019, p. 674).

Diante disso, não somente em casas, mas em qualquer local com necessidade de controle de acesso, o motivo de aprimorar os meios de segurança em torno de um ambiente por meio deste trabalho. Uma fechadura poderá ser aberta ou fechada sem a necessidade, obrigatoriamente, de uma chave física e, além disso, devido a aplicação de conceitos IoT, a possibilidade de integração com outros sistemas de segurança como câmeras, sensores, entre outros dispositivos eletrônicos, e também gerar registros de possíveis acontecimentos indesejados, como por exemplo, o furto de objetos contidos em um ambiente.

Norman (2017, p. 21) afirma:

> Os sistemas de controle de acesso são uma parte importante de um programa de segurança geral projetado para impedir e reduzir o comportamento criminoso e as violações das políticas de segurança de uma organização. Mas é importante lembrar que é apenas uma parte (Norman, 2017, p. 21).

Vale salientar que um sistema de fechadura magnética não é suficiente para obter segurança total de um ambiente, pois a entrada e saída de algo de um ambiente não depende apenas da abertura e fechamento de uma fechadura. Este projeto visa aprimorar e diminuir custos para se obter um sistema de controle de acesso a ambientes a partir das portas sem a necessidade de remover ou alterar as fechaduras mecânicas utilizadas comumente e possibilitar que novos sistemas baseados em IoT sejam utilizados simultaneamente ao trabalho proposto.

1.3 Organização do trabalho

Este trabalho está dividido em cinco capítulos. O Capítulo 2 apresenta a fundamentação teórica do trabalho. O Capítulo 3 descreve o desenvolvimento da aplicação web, aplicação de dispositivo móvel e a modelagem da estrutura física de todo o sistema. O Capítulo 4 exibe os resultados obtidos por este trabalho a partir de implantação em ambiente real. E, por fim, o Capítulo 5 apresenta as conclusões e propostas para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste trabalho é descrita a seguir. A seção 2.1 descreve os conceitos de Internet das Coisas, a seção 2.2 discorre sobre trabalhos correlatos a este, a seção 2.3 descreve e lista os componentes físicos (hardware) utilizados neste trabalho e a seção 2.4 as tecnologias de software.

2.1 Trabalhos correlatos

Sankar e Srinivasan (2018) propuseram um sistema de fechadura digital baseado na Internet das Coisas que contem teclado para entrada de senha de texto e um leitor biométrico. A arquitetura física proposta pelos autores utiliza um Microcontrolador Arduino Yun com uma webcam conectada em que as imagens obtidas são salvas em um armazenamento em nuvem ou local e podem ser acessadas através de um aplicativo de dispositivo móvel e e-mail.

Vongchumyen *et al.* (2017) desenvolveram um sistema em que uma fechadura convencional é modificada com hardware eletrônico e controlada por software, mantendo o uso das chaves físicas comuns. No sistema utiliza-se um dispositivo Raspberry Pi para interpretar os comandos enviados via rede WiFi pelo software web e a partir dele emitir comandos a um microcontrolador ATtiny2313 que aciona um motor de passo para travar ou destravar a fechadura. Também foi utilizado um alto-falante Piezo que funciona como um microfone para detectar batidas na porta e, com isso, enviar um e-mail que notifica a ação para o usuário.

Basha, Jilani e Arun (2016) realizaram o desenvolvimento de um sistema de portas inteligentes utilizando a Internet das Coisas em que o intuito é identificar e notificar intrusão a partir do movimento indesejado em uma porta. Foi utilizado um acelerômetro ADXL345 para detectar movimento da porta e um Raspberry Pi para ler e processar os dados. Os dados processados são enviados ao Amazon Web Services Internet of Things (AWS IoT) e com base neles é emitido um e-mail pelo AWS Simple Notification Service (SNS). Todos os registros são salvos em uma planilha da Google utilizando Application Program Interface (APIs).

2.2 Internet das Coisas

O termo Internet das Coisas (em inglês, *Internet of Things,* IoT*)* foi utilizado pela primeira vez pelo britânico Kevin Ashton para descrever um sistema no qual objetos físicos se conectavam à Internet por meio de sensores. Nos dias atuais, a IoT é muito utilizada para descrever cenários na qual envolve conectividade com a Internet e a capacidade de computação de uma vasta variedade de objetos, dispositivos, sensores e itens do cotidiano (ROSE; ELDRIDGE; CHAPIN, 2015).

Ela pode ser definida, também, como “Uma rede aberta e abrangente de objetos inteligentes com capacidade de auto-organização, compartilhamento de informações, dados e recursos, reagindo e agindo diante de situações e mudanças no ambiente” (MADAKAM; RAMASWAMY; TRIPATHI, 2015).

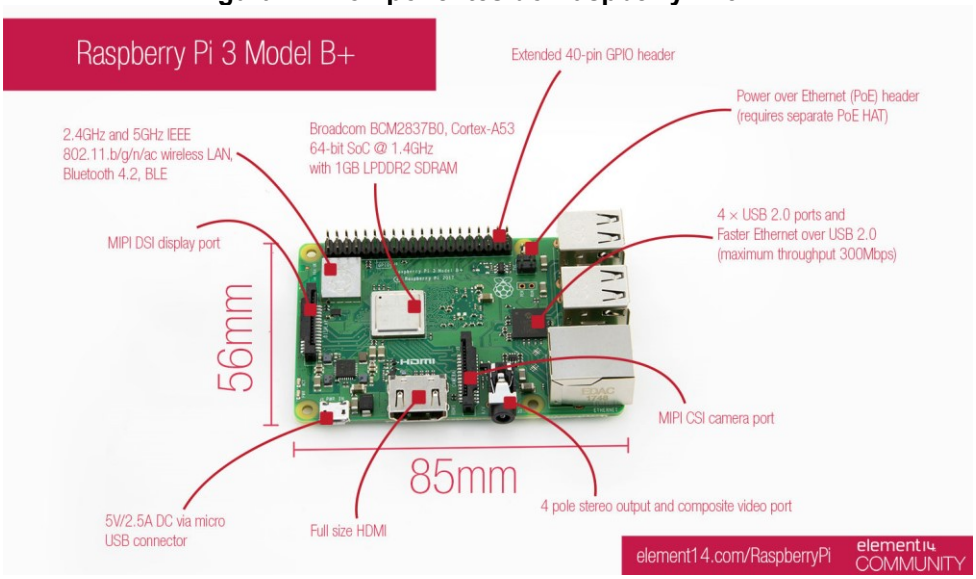
2.3 *Hardware*

Conforme proposto por este trabalho, foi desenvolvido uma solução utilizando componentes físicos (hardware) para controle de acesso. Foi utilizado um microcomputador Raspberry Pi 3 B+, sistemas de fechadura eletromagnética, dispositivos móveis (smartphone e tablet) e câmeras de segurança com conexão via rede (câmera IP). Também foi utilizado um componente eletrônico chamado relé para instalação da solução.

2.3.1 Microcomputador Raspberry Pi 3 B+

Raspberry Pi é um microcomputador de baixo custo, do tamanho de um cartão de crédito e que utiliza periféricos como teclado e mouse comuns. Este dispositivo é capaz de fazer qualquer coisa como um computador comum, desde navegar na internet, jogar jogos, etc. (RASPBERRY PI FOUNDATION, 2022).

Figura 1 – Componentes do Raspberry Pi 3 B+



Fonte: Stanton (2018)

A escolha de utilizar o Raspberry Pi 3 B+ se deve ao baixo custo, disponibilidade de entradas e saídas digitais para gerenciamento de múltiplas fechaduras simultaneamente, acesso à internet, facilidade de instalação e, principalmente, pelo seu tamanho, autonomia e capacidade de processamento de informações.

2.3.2 Fechadura eletromagnética

A fechadura eletromagnética foi patenteada em maio de 1989 por Arthur, Richard e David Geringer da empresa *Security Door Controls*. O objeto descrito em seus projetos seria, a princípio, é o mesmo das fechaduras eletromagnéticas atuais onde consiste em um eletroímã e uma placa metálica robusta. A patente expirou em 2006 (ACADEMIC, 2022).

Existem diversos sistemas de fechadura magnética disponíveis no mercado e, independente da marca ou modelo, são fáceis de serem adaptadas a este trabalho. É um sistema relativamente de baixo custo e de grande escalabilidade devido a sua fácil instalação.

Figura 2 – Eletroímã e placa metálica de uma fechadura eletromagnética

Fonte: V-Guard (2019)

Em relação a sua escalabilidade, a facilidade de instalação em qualquer tipo de superfície, tipos de porta horizontal ou vertical e até mesmo em objetos que contenha uma forma de abertura e fechamento, por exemplo um baú. Também o fato de que pode ser instalada sem obstruir o sistema de segurança utilizado na situação em questão, como em uma porta com fechadura mecânica comum, a fechadura eletromagnética não irá interferir no funcionamento desta.

2.3.3 Dispositivo móvel *smartphone*

De acordo com Barmpatsalou *et al.* (2019), os dispositivos móveis são um resultado de um processo de evolução de um período o qual os recursos computacionais e rede foram impulsionados para acompanhar a carga de trabalho em constante crescimento. Este fato permitiu que dispositivos como smartphones e tablets realizassem tarefas cada vez mais complexas a ponto de substituir dispositivos tradicionais como computadores desktop e notebooks.

A utilização de dispositivo móvel justifica-se pelo fato de que um pouco mais de 80% da população mundial possui um smartphone (BANKMYCELL, 2021) e a vasta possibilidade de funcionalidades que podem ser implementadas nestes dispositivos devidos suas capacidades físicas (hardware) e lógicas (software).

2.3.4 Câmera de Segurança IP

O investimento em câmeras de monitoramento tem sido cada vez mais frequentes em qualquer local, seja residencial, empresarial ou até mesmo em ambientes públicos. Esse objeto de monitoramento traz benefícios ao usuário como visualização de diversos ambientes de maneira simultânea, proteção, controle de entrada e saída de pessoas em um espaço, entre outros (GLOBALTECHBRASIL, 2019).

Em projetos em que a câmera necessita interação com a internet ou outros eletrônicos que suportam a tecnologia IP (*Internet Protocol)*, as câmeras IP apresentam recursos muito úteis, como inteligência embarcada, por exemplo (INTELBRAS, 2020)

O maior benefício do uso desse tipo de câmera é a instalação que é facilitada pelo sistema IP, que seria conexão via rede com o mesmo cabo usado na conexão do computador a internet, conhecido como UTP (do inglês, *Unshielded Twisted Pair*) (INTELBRAS, 2020). Alguns modelos trazem a possibilidade de conexão Wireless também.

2.4 *Software*

Conforme os objetivos deste trabalho, foi desenvolvido também uma aplicação web para gerenciamento de dados e uma aplicação de dispositivos móveis para ser utilizado por usuários no acesso à fechadura magnética.

2.4.1 Banco de dados MySQL

O MySQL é um servidor e gerenciador de banco de dados (SGBD) relacional com dois tipos de licença, sendo uma delas de software livre (gratuito) tanto para fins acadêmicos como para realização de negócios. Desenvolvido por David Axmark, Allan Larsson e Michael “Monty” Widenius na década de 90, este banco de dados é completo, robusto e extremamente rápido, com todas as características existentes nos principais bancos de dados pagos existentes no mercado (MILANI, 2006).

2.4.2 Servidor LDAP

Lightweight Directory Access Protocol (LDAP) é um protocolo de rede que permite organizar informações de maneira hierárquica e como principais características são a facilidade de localizar dados, grande escalabilidade e ser de código aberto (MORIMOTO, 2004).

Um servidor LDAP pode ser responsável pela autenticação do usuário em uma rede e as informações deste usuário ficam armazenadas na base de dados do servidor. O mesmo permite ou não que o cliente realize consultas e modificações (MACHADO; JUNIOR, 2006).

2.4.3 API RESTFul em Java

Uma *Application Programming Interface* (API) é o nome utilizado para se referir a um conjunto de rotinas e padrões definidos para aplicação onde que outras aplicações possam utilizar as funcionalidades implementadas de forma simples e sem conhecer os detalhes da implementação. Sendo assim, pode-se afirmar que as APIs permitem uma interoperabilidade entre aplicações (PIRES, 2017).

O termo *REpresentational State Transfer* (REST), anunciado por Roy Fielding em 2000, não é um protocolo ou padrão, mas sim um conjunto de restrições que aplicado a um sistema cria-se um estilo de arquitetura (SANDOVAL, 2009).

De acordo com a Red Hat (2020), para que uma API seja considerada do tipo RESTFul, ela precisa estar em conformidade com os seguintes critérios:

- Possuir arquitetura cliente/servidor formada por clientes, servidores e recursos, com solicitações gerenciadas por HTTP.
- Comunicação *stateless* (em português, sem estado) entre cliente e servidor, ou seja, nenhuma informação do cliente é armazenada entre as solicitações ao servidor, são separadas e desconectadas ao fim.
- Armazenar dados em cache.
- Ter uma interface uniforme entre os componentes para transferência de informações de maneira padronizada.
- Possuir sistema em camadas que organiza o servidor.

Java é uma linguagem de programação desenvolvida pela Sun Microsystems em 1995 (adquirida pela empresa Oracle em 2009) e possui características que o diferencia de outras linguagens de programação, entre elas ser orientada a objetos, independente de plataforma e concorrente, possuir mecanismos de segurança embutidos, não incluir ponteiros e oferecer ótima performance (JUNIOR, 2021).

2.4.4 Servidor Wild Fly

Wild Fly é um servidor de aplicações de código aberto, gratuito, escrito linguagem de programação Java, baseado nos padrões definidos pela Java EE (*Java Platform Enterprise Edition)* e mantido pela comunidade e a empresa Red Hat™. A Java EE oferece uma solução robusta, portável, escalável e que atende demandas de acesso, transações, segurança, entre outras necessidades. (DEVMEDIA, 2022).

2.4.5 Ionic *Framework*

A Ionic foi fundada em 2012 por Max Lynch e Bem Sperry com o objetivo de facilitar criação de aplicativos móveis nativos com o uso de tecnologias web. Sendo de código aberto, a Ionic é uma das plataformas de criação de aplicativos móveis multiplataforma com Javascript mais utilizadas no mundo (IONIC, 2022).

O desenvolvimento com Ionic Framework é baseado nas linguagens HTML, CSS e Javascript. A partir de outros *frameworks*, como Angular e Cordova, é possível apresentar informações de forma dinâmica e acessar recursos nativos de um aparelho (GRIFFITH, 2017).

Cordova foi desenvolvido, originalmente, pela Nitobi Software em 2009 com o intuito de ser uma solução de código aberto para construir aplicativos móveis nativos usando tecnologias web. Em 2011 foi comprada pela Adobe Systems e assim renomeada para Apache Cordova (GRIFFITH, 2017).

O Apache Cordova fornece uma biblioteca de APIs escritas em Javascript que interage com recursos nativos de um dispositivo móvel como acesso à câmera, tirar fotos, enviar e-mail, entre outras funcionalidades (RAVULAVARU, 2017).

2.4.6 Angular

O Angular é um projeto de código aberto mantido pela Google. Foi anunciado, inicialmente, em 2009 como AngularJS e desde então vem sendo uma das ferramentas mais populares no desenvolvimento de aplicativos web. O objetivo do Angular é prover uma ferramenta MVW (*model-view-whatever*), ou seja, uma ferramenta que construa aplicativos web complexos e de página única (GRIFFITH, 2017).

Em 2014, o Angular passa por uma atualização significante onde as novas características são, principalmente, a melhora de performance e velocidade de processamento dos dados. Esta versão foi chamada de Angular 2, que utilizando a linguagem Typescript, “um superconjunto tipado de Javascript que compila para Javascript simples” (RAVULAVARU, 2017).

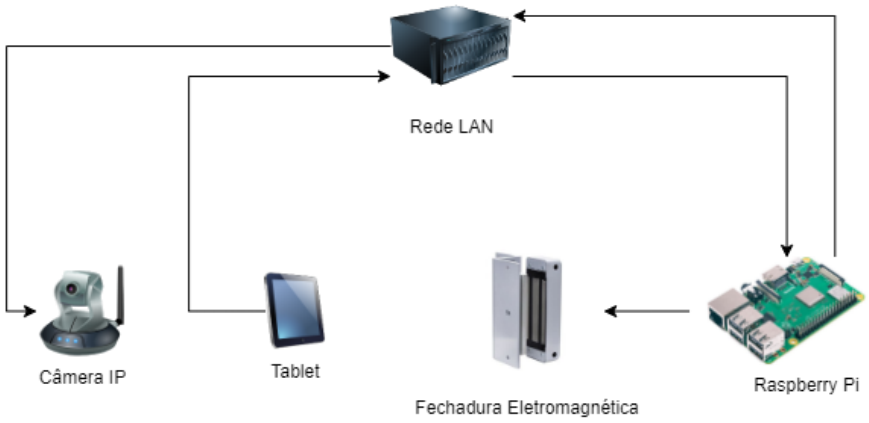
3 DESENVOLVIMENTO

Este capítulo tem como objetivo descrever as etapas de desenvolvimento do projeto. A seção 3.1 descreve o estudo e implementação da estrutura física e a seção 3.2 descreve a do software.

O projeto foi desenvolvido para ser implementado, inicialmente, em ambientes da UTFPR campus Ponta Grossa e, devido a este fato, muitos dos dispositivos tecnológicos utilizados foram por motivos de disponibilidade, baixo custo ou que já são utilizados no âmbito da universidade.

3.1 Estrutura física (*Hardware*)

Figura 3 – Representação em diagrama da estrutura física do trabalho



Fonte: Autoria própria (2022)

Considerando os conceitos de IoT, como proposto pelo trabalho, é indispensável o uso de dispositivos que possuem capacidade de se comunicar entre si. Portanto, foi utilizado uma rede LAN para que os dispositivos se comuniquem via protocolo IP.

A primeira ação em relação ao desenvolvimento da estrutura física do projeto, foi a realização de um estudo sobre a disposição dos dispositivos na instalação em um ambiente real e, com isso, implementa-los visando menor impacto negativo financeiro e físico do local. Sendo assim, o aproveitamento de espaço e diminuição da quantidade de instalação elétrica foram aderidas.

Na Fotografia 1 ilustra-se um protótipo de central de fechadura eletromagnética. Aproveitando-se do espaço na caixa de proteção do sistema de fechadura, pode-se observar que é possível manter o microcomputador seguro e de maneira discreta. O sistema de fechadura é alimentado por uma bateria 12V capaz de manter o eletroímã magnetizado por dias mesmo diante a uma queda energética local, e para aproveitar esta fonte de energia, ao invés de conectar o microcomputador à rede elétrica local, foi utilizado um regulador de tensão para 5V, que é suficiente para manter o Raspberry Pi em funcionamento em conjunto com o sistema da fechadura.

Fotografia 1 – Central de fechadura eletromagnética com microcomputador conectado

Fonte: Autoria própria (2022)

O microcomputador Raspberry Pi 3 B+ possui 28 pinos GPIO configuráveis (PI4J, 2019) e, com isso, possibilita gerenciar mais de uma fechadura simultaneamente. Porém, alguns modelos de sistema de fechadura eletromagnética não são compatíveis diretamente com os sinais lógicos emitidos pelo GPIO. Para solucionar esta questão, foi utilizado um relé eletrônico (Fotografia 3) que é capaz de filtrar a comunicação entre o microcomputador e o sistema da fechadura.

Fotografia 2 – Relé eletrônico

Fonte: Autoria própria (2022)

O sistema de fechadura pode ser instalado em qualquer local, pois são simples fios conectores que ligam o eletroímã com o sistema. Igualmente a conexão do sistema da fechadura com o microcomputador.

Para a interação com a fechadura, foi pensado no uso de um dispositivo móvel que pode ser acoplado próximo à porta controlada. Este dispositivo móvel, que pode ser um tablet ou smartphone, deve estar conectada na rede LAN via Wi-Fi para que possa se comunicar com o serviço WEB hospedado no microcomputador (detalhado na seção 3.2.1). Essa solução possibilita ao usuário acessar a fechadura por qualquer dispositivo móvel desde que esteja conectada à rede, ou seja, pode ser um dispositivo pessoal.

Fotografia 3 – Câmera IP de segurança utilizado na UTFPR Ponta Grossa

Fonte: Autoria própria (2022)

Assim como o dispositivo móvel, a câmera de segurança IP também deve ser instalada estrategicamente próximo à porta e conectada na rede.

Considerando um possível grande fluxo de entrada e saída de um ambiente, um botão pode ser instalado na parte interna do local (ilustrado na Fotografia 4), que desmagnetiza os eletroímãs por um tempo limitado (configurado diretamente no sistema da fechadura). Este pode ser instalado a qualquer distância da porta ou da

central da fechadura, desde que possa ser conectada por fios elétricos diretamente à fechadura. O objetivo é minimizar a dificuldade de saída do ambiente, caso necessário.

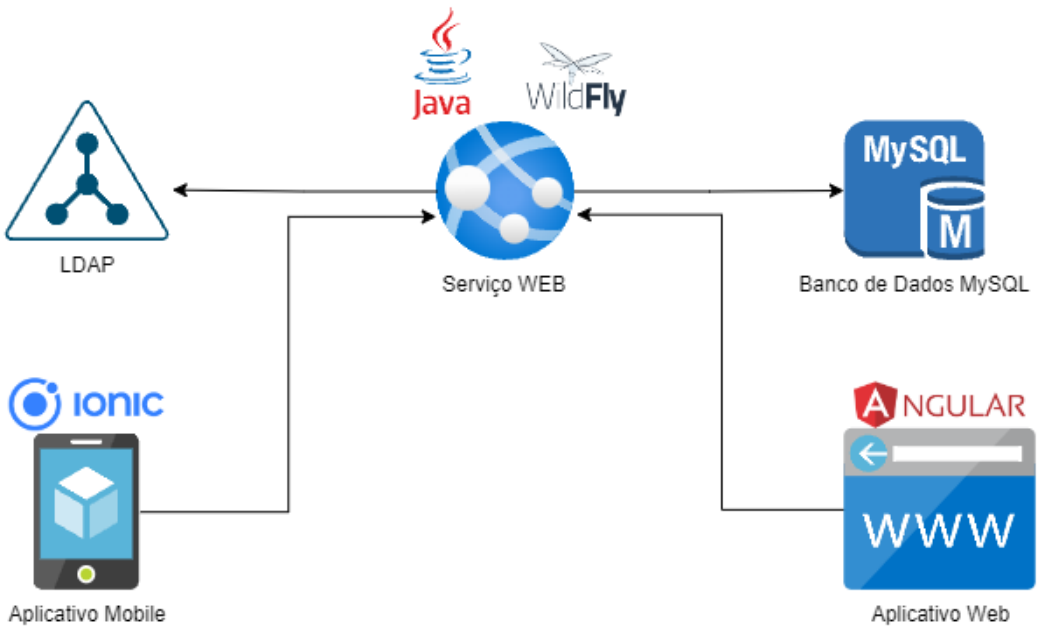
Fotografia 4 – Sistema de fechadura com botão de acionamento

Fonte: Autoria própria (2022)

3.2 Aplicação (*Software*)

Para o funcionamento da estrutura física proposta, foi desenvolvido um serviço web que é executado no Raspberry Pi. Este serviço se comunica com o LDAP a partir da rede LAN, e mantém conexão com o banco de dados MySQL que, também, se encontra no Raspberry Pi. Com isso, os dispositivos móveis como smartphones e tablets são capazes de interagir com as fechaduras a partir da troca de informações com este serviço web. O fluxo de comunicação dentre as tecnologias pode ser visualizado na Figura 4.

Figura 4 – Representação em diagrama da estrutura lógica do trabalho



Fonte: Autoria própria (2022)

O servidor LDAP possui informações para autenticação dos usuários internos da organização em que o sistema se encontra instalado. No banco de dados MySQL são armazenados informações sobre as os ambientes com Raspberry Pi, as fechaduras, câmeras, histórico de acessos e mudanças de estado das fechaduras, informações para autenticação de usuários externos (que não fazem parte da organização) e agendamento para controle de acesso aos ambientes por meio de data e horário.

Para o desenvolvimento do sistema foi necessário utilizar um contexto de alguma organização real, pois algumas informações podem se divergir de acordo com o ambiente de instalação, como nome dado ao local onde o sistema vai gerenciar. Com isso, o sistema foi implementado no contexto da UTFPR, campus de Ponta Grossa, onde que o sistema controla o acesso de vários ambientes que possuem salas de aula ou departamentos. Estes são contidos nos blocos, que são a divisão dos setores do campus da universidade (ilustrada na figura 5).

Figura 5 – Representação do ambiente na UTFPR Campus Ponta Grossa

Fonte: Autoria própria (2022)

3.2.1 Serviço WEB

De acordo com a W3C *(World Wide Web Consortium)*, um serviço WEB é um sistema de software projetado para fornecer suporte à interação entre máquinas interoperáveis em uma rede (BOOTH *et al*., 2004), ou seja, facilitar a interação para troca de informações.

O serviço web disponibiliza uma API que foi desenvolvido com padrões RESTFul na linguagem de programação Java. Este é hospedado no servidor Wild Fly, que também hospeda a aplicação WEB (descrito na seção 3.2.2) e envia informações para a aplicação móvel (descrito na seção 3.2.3). Este serviço tem a função de gerenciar os dados armazenados no banco de dados MySQL, consultar informações no servidor LDAP e gerenciar os estados das fechaduras e imagens das câmeras IP.

A aplicação WEB utiliza a API para gerenciar todas as informações e configurações necessárias para o funcionamento do sistema. A aplicação para

dispositivos móveis, também por meio da API, troca informações com o serviço web a fim de autenticar um usuário e permiti-lo interagir com as fechaduras.

3.2.2 Aplicação WEB - Administração

Para o desenvolvimento da aplicação web, foi utilizado o *framework* Angular. Esta aplicação se comunica diretamente com o serviço web e torna o gerenciamento do controle de acesso às fechaduras mais simples e fácil.

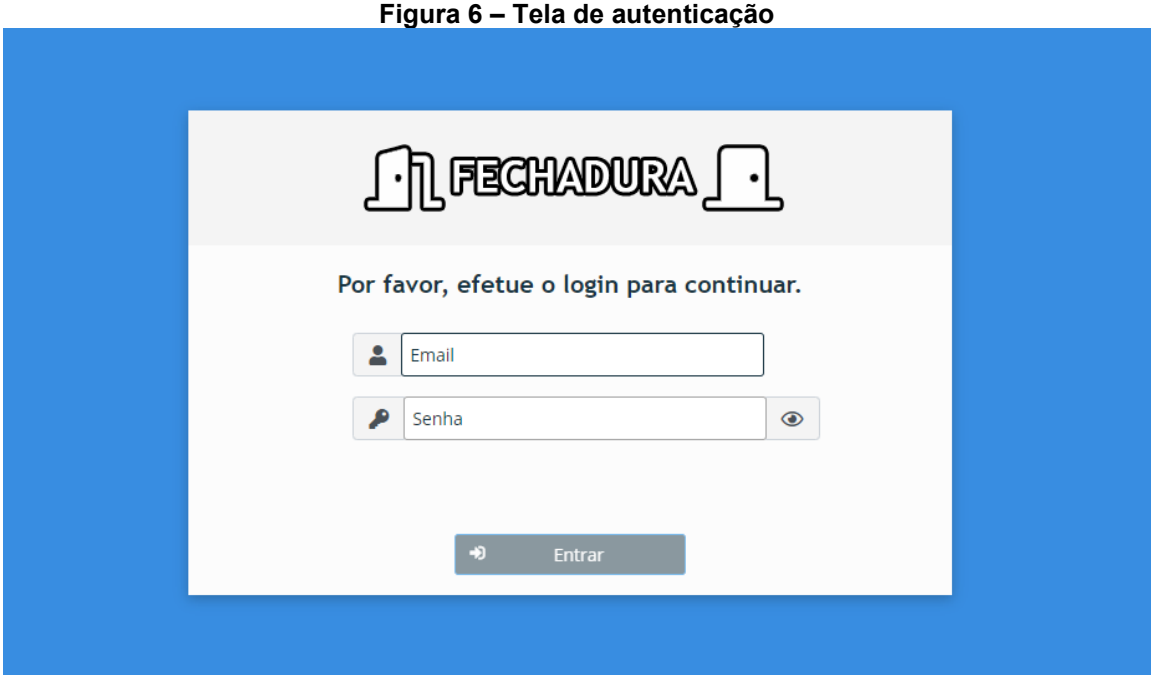
Esta aplicação é dividida em oito módulos:

- Autenticação.
- Gerenciamento de Usuários Administrativos.
- Gerenciamento de Raspberry.
- Gerenciamento de Blocos.
- Gerenciamento de Ambientes.
- Gerenciamento de Empresas e Funcionários Terceirizados.
- Gerenciamento de Agendas.
- Visualização de Histórico.

O acesso ao sistema é feito por meio de autenticação com e-mail e senha cadastrados no servidor LDAP ou no próprio banco de dados do sistema, gerenciado por um administrador no módulo de gerenciamento de usuários, descrito mais adiante.

A Figura 6 apresenta a tela de autenticação do sistema e a Figura 7 a tela de verificação de segurança em que o serviço web envia uma sequência numérica ao e-mail do usuário e o mesmo deve ser inserido no campo solicitado para que a autenticação seja efetuada com sucesso. O envio deste e-mail pode ser configurado com qualquer servidor de e-mail disponível à organização.

Figura 6 – Tela de autenticação



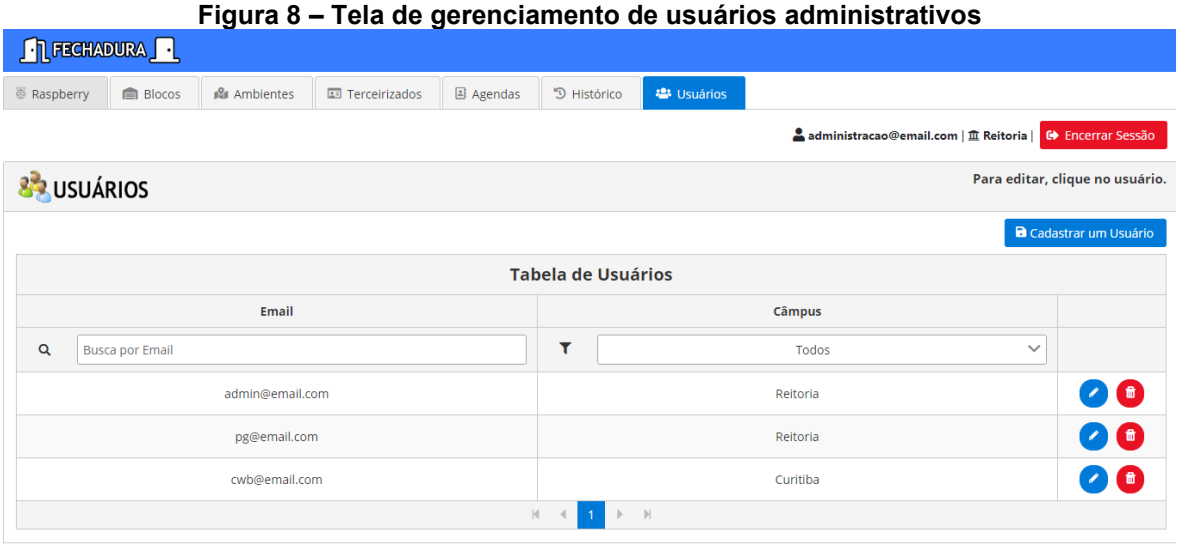
Fonte: Autoria própria (2022)

Figura 7 – Tela de verificação de e-mail

Fonte: Autoria própria (2022)

A Figura 8 apresenta a tela de gerenciamento de usuários, onde é possível criar acessos administrativos ao sistema com limitações por campus.

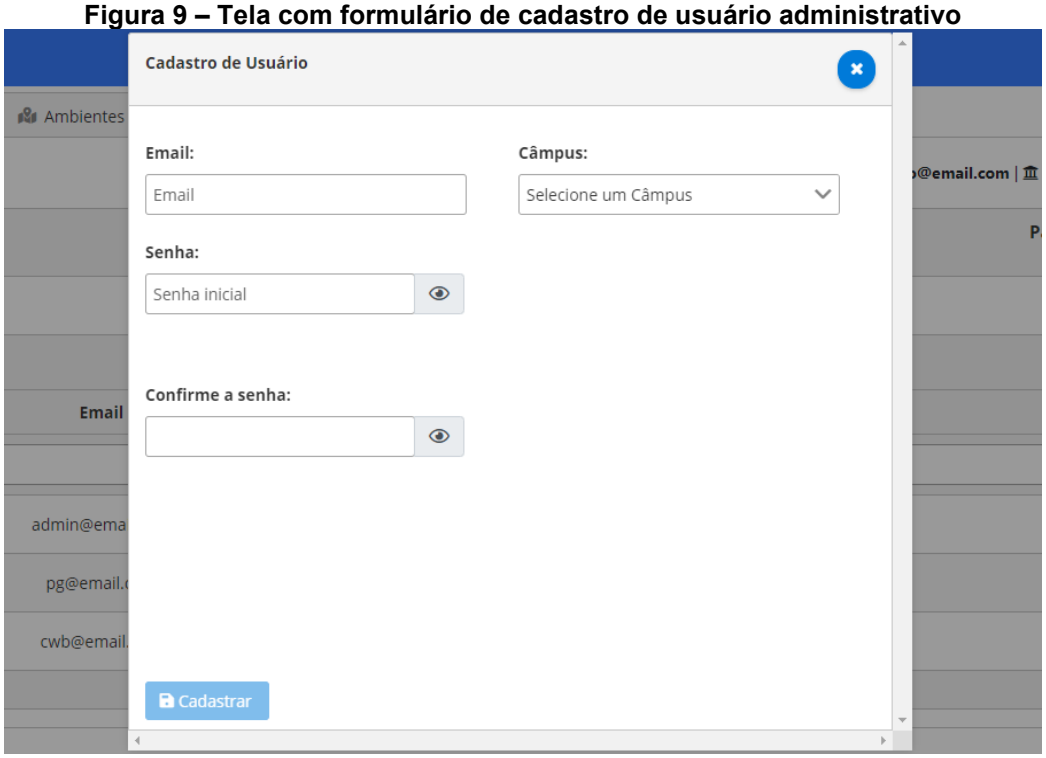
Figura 8 – Tela de gerenciamento de usuários administrativos



Fonte: Autoria própria (2022)

A Figura 9 apresenta o formulário de cadastro de um usuário administrativo. O formulário de edição é semelhante.

Figura 9 – Tela com formulário de cadastro de usuário administrativo

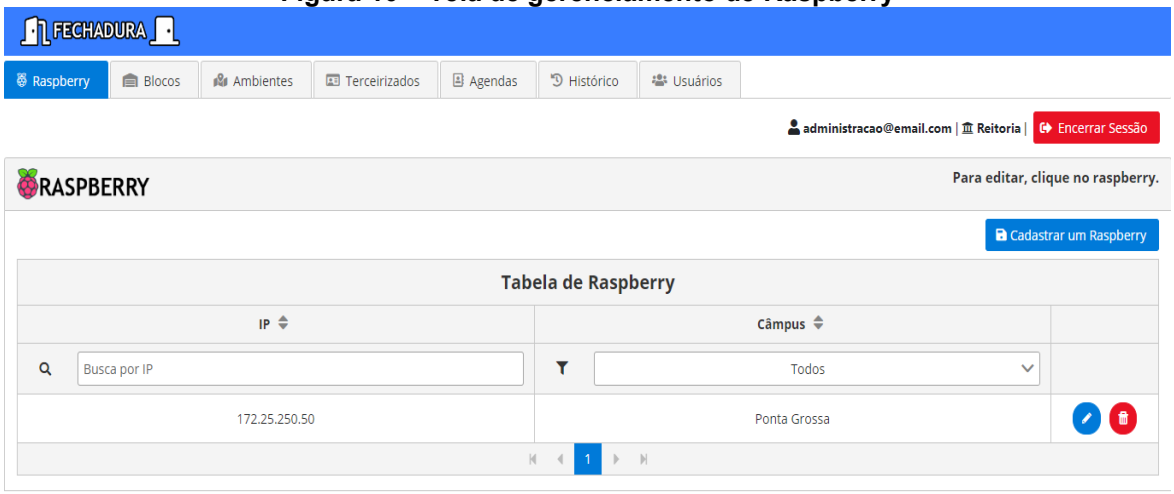


Fonte: Autoria própria (2022)

Assim como descrito anteriormente, no contexto da UTFPR, o usuário autenticado pode gerenciar Raspberry de acordo com o campus vinculado ou, se o

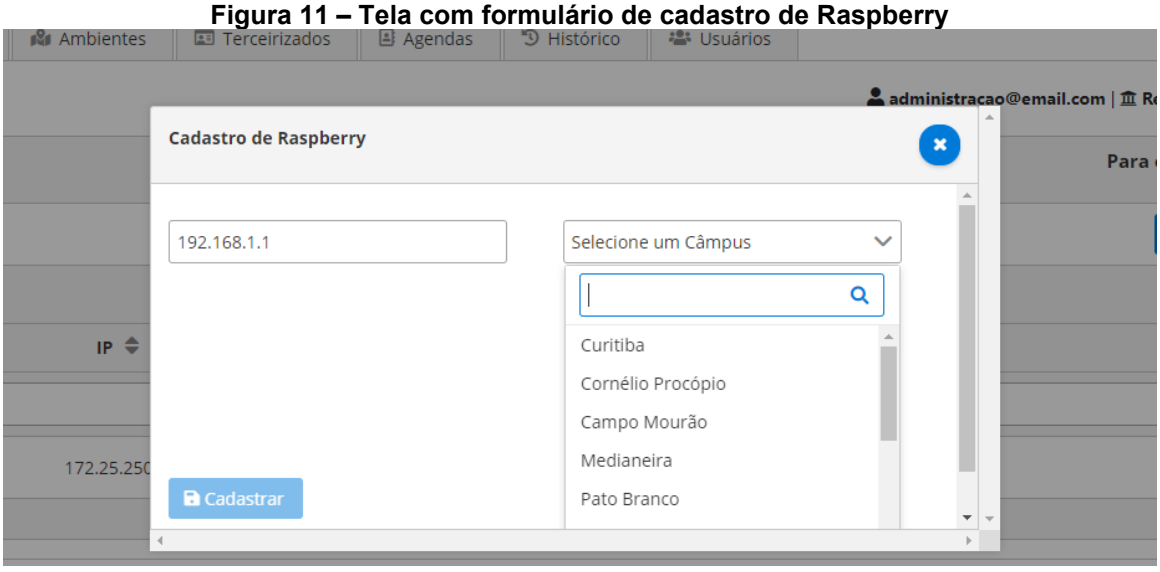
usuário for administrador geral, de todos os campus, como ilustrado na Figura 10 e Figura 11.

Figura 10 – Tela de gerenciamento de Raspberry



Fonte: Autoria própria (2022)

Figura 11 – Tela com formulário de cadastro de Raspberry



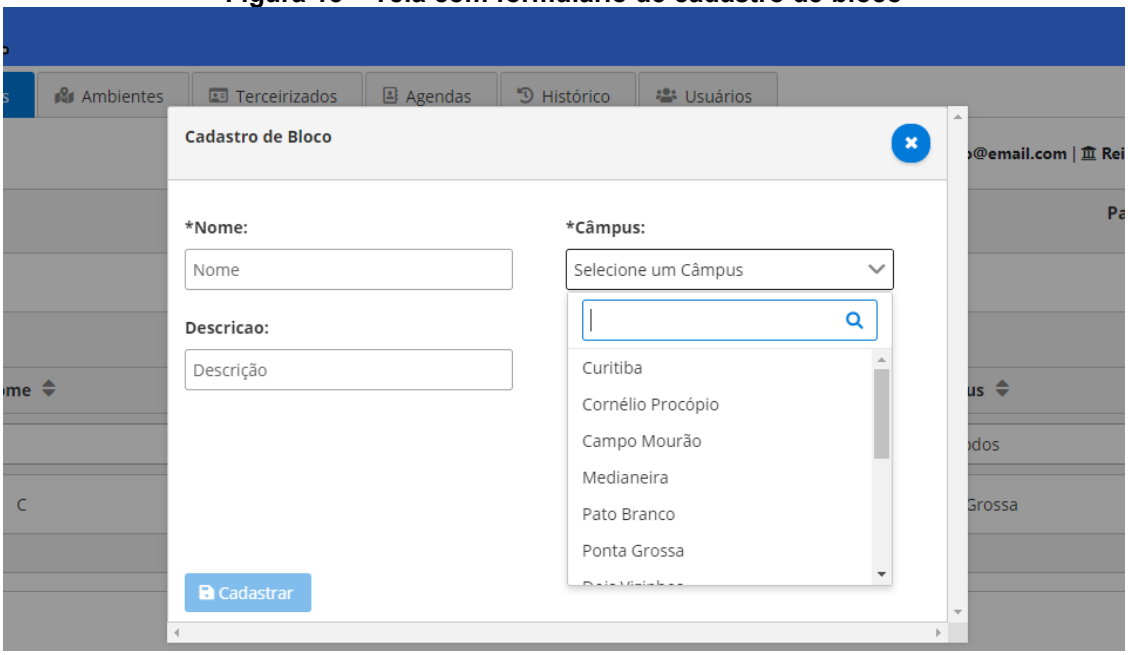
Fonte: Autoria própria (2022)

Para configurar as fechaduras é necessário cadastrar os blocos e ambientes que serão instalados toda estrutura física do sistema. Na Figura 12 e Figura 13 é apresentado as telas de gerenciamento de Blocos e seu formulário de cadastro, respectivamente.

Figura 12 – Tela de gerenciamento de blocos

Fonte: Autoria própria (2022)

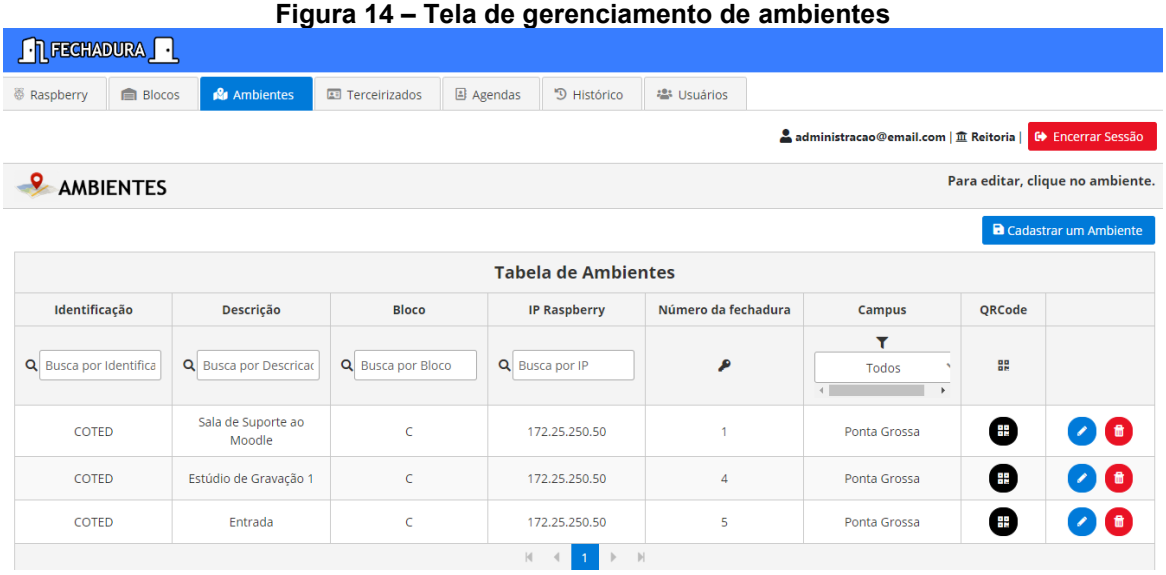
Figura 13 – Tela com formulário de cadastro de bloco



Fonte: Autoria própria (2022)

Os ambientes cadastrados no sistema equivalem a cada fechadura instalada. Na instalação física do sistema, uma fechadura eletromagnética é conectada a um pino GPIO do Raspberry. Este pino possui uma numeração que deve ser configurada no gerenciamento de ambientes juntamente com as configurações cadastradas para o Raspberry e o Bloco em que esse ambiente se encontra.

Figura 14 – Tela de gerenciamento de ambientes



Fonte: Autoria própria (2022)

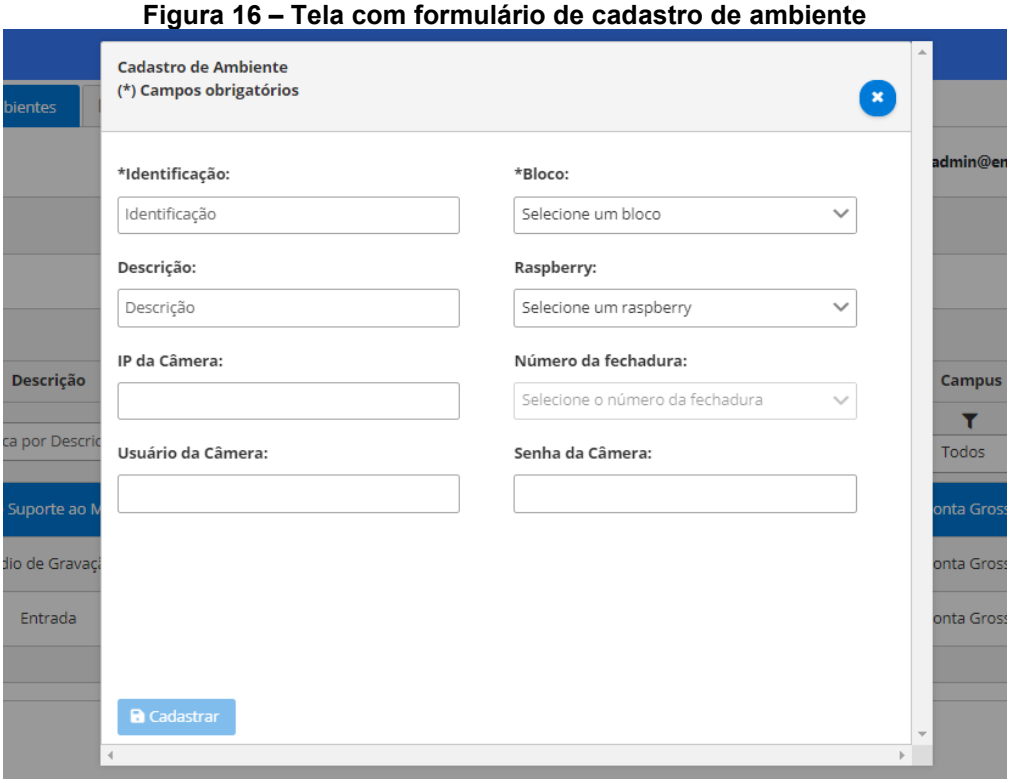
Para o uso da aplicação para dispositivos móveis (seção 3.2.3), pode-se gerar um QRCode *(Quick Response Code)* a partir da tela de gerenciamento de ambientes que contém os dados necessários para se conectar à fechadura (Figura 15). Este pode ser salvo e impresso, com isso, pode ser anexado em um local de fácil acesso e próximo à fechadura.

Figura 15 – Tela com QRCode gerado a partir de um ambiente

Fonte: Autoria própria (2022)

Além das configurações da fechadura, é possível inserir os dados de autenticação e IP da câmera que irá monitorar as ações aplicadas a fechadura em questão (ilustrado na Figura 16).

Figura 16 – Tela com formulário de cadastro de ambiente

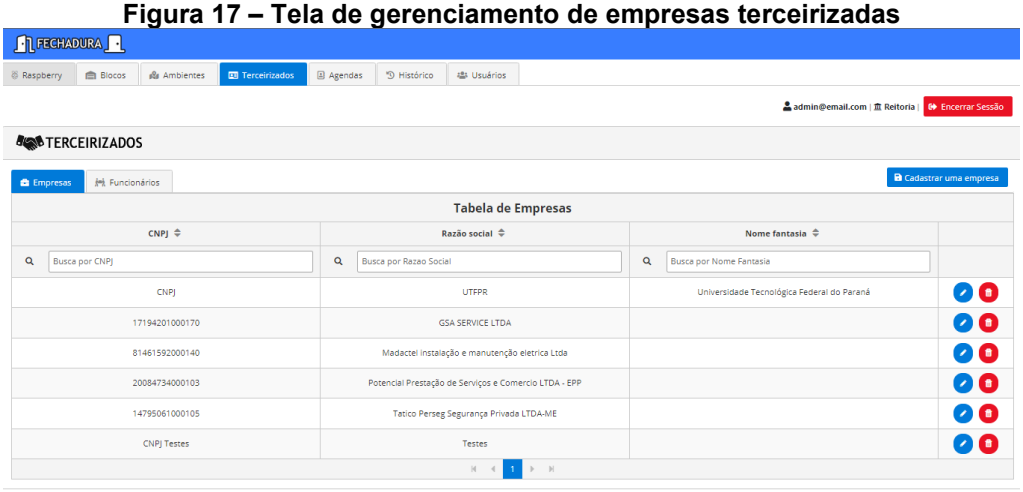


Fonte: Autoria própria (2022)

Com as informações de Raspberry, Bloco e Ambiente cadastradas no sistema e com a estrutura física instalada é possível acessar a fechadura com usuários cadastrados no servidor LDAP. Mas, é possível cadastrar outros usuários no sistema que precisem acessar um ambiente mesmo não possuindo registro no LDAP. Este pode ser cadastrado no gerenciamento de terceirizados.

O gerenciamento de terceirizados (Figura 17 à Figura 20) consiste em cadastro de empresas e seus funcionários. Esta funcionalidade foi implementada visando a possibilidade de cadastrar usuários aptos a acessarem um ambiente mesmo não possuindo relação direta com a organização mantenedora do sistema. No contexto da UTFPR, pode-se exemplificar uma empresa como de limpeza e seus respectivos funcionários.

Figura 17 – Tela de gerenciamento de empresas terceirizadas

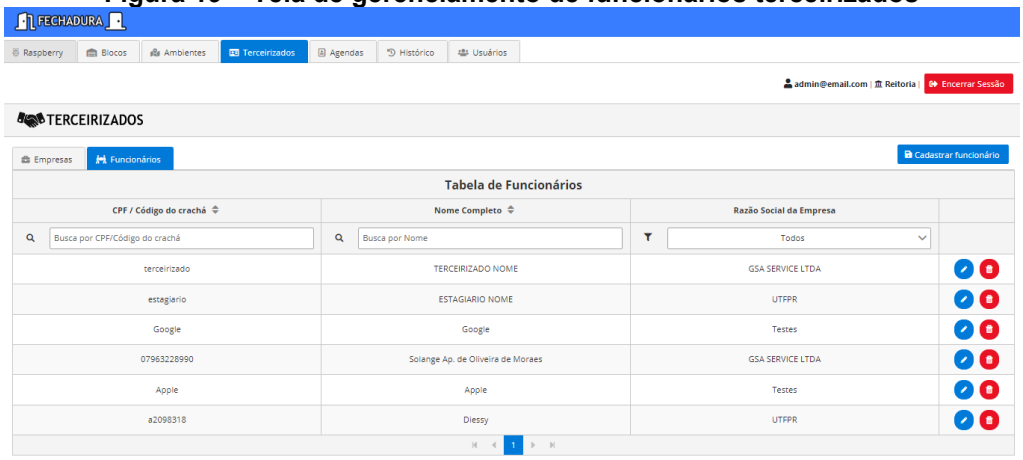


Fonte: Autoria própria (2022)

Figura 18 – Tela com formulário de cadastro de empresa

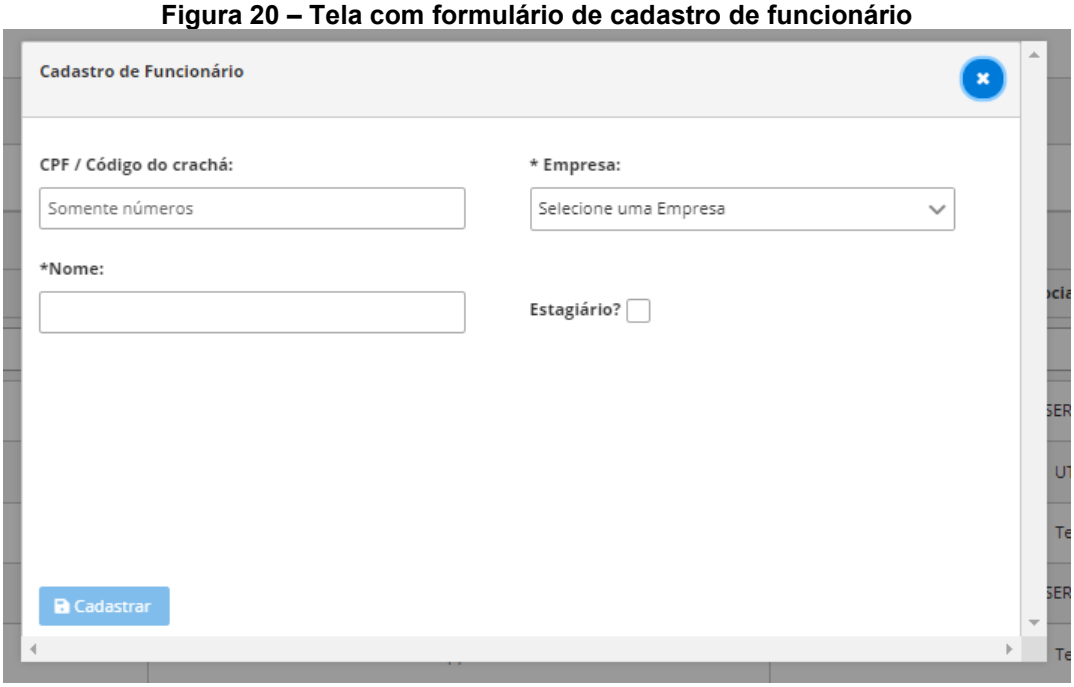
Fonte: Autoria própria (2022)

Figura 19 – Tela de gerenciamento de funcionários terceirizados



Fonte: Autoria própria (2022)

Figura 20 – Tela com formulário de cadastro de funcionário



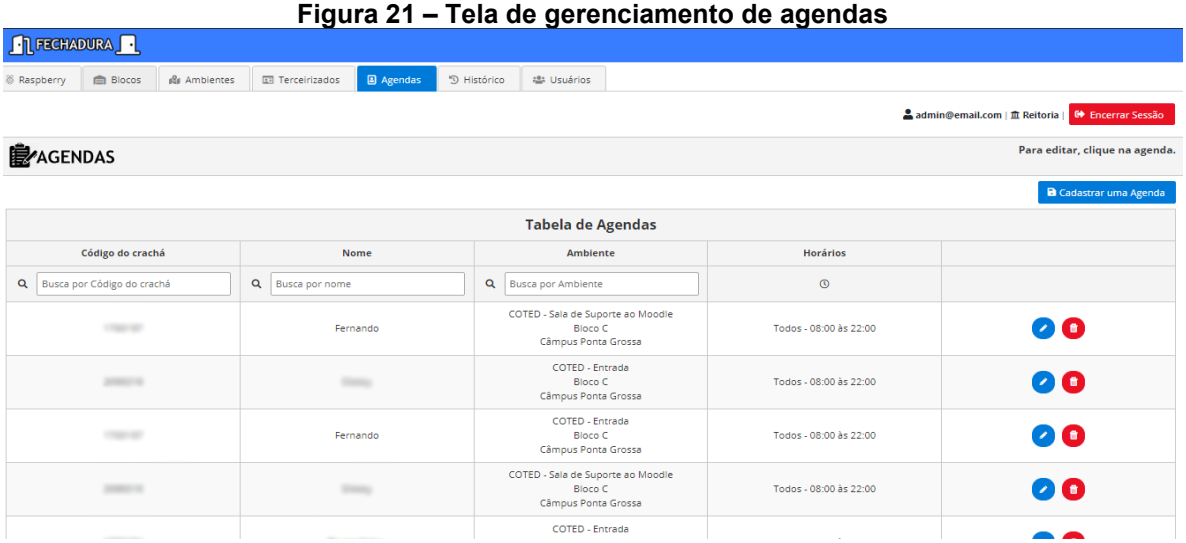
Fonte: Autoria própria (2022)

O usuário cadastrado no sistema pode utilizar a aplicação móvel se autenticando com seu código e senha que, inicialmente, são iguais. A senha poderá ser alterada em seu primeiro acesso via aplicação para dispositivos móveis (seção 3.2.3).

O sistema permite ter três tipos de usuários que podem acessar os ambientes com as fechaduras. No contexto deste trabalho, tem-se o funcionário terceirizado, o estagiário e o professor. A diferença dentre estes usuários é que o funcionário e o professor podem mudar o estado da fechadura, aberto ou fechado, e mantê-lo até que seja acionado uma nova ação. O estagiário apenas poderá abrir a fechadura e com alguns segundos a mesma fecha automaticamente, ou seja, não poderá manter o estado de aberto continuamente.

O controle de acesso aos ambientes é feito no gerenciamento de agendas (ilustrado na Figura 21). Esta funcionalidade permite cadastrar intervalos de data e horário em que um usuário pode acessar um certo ambiente.

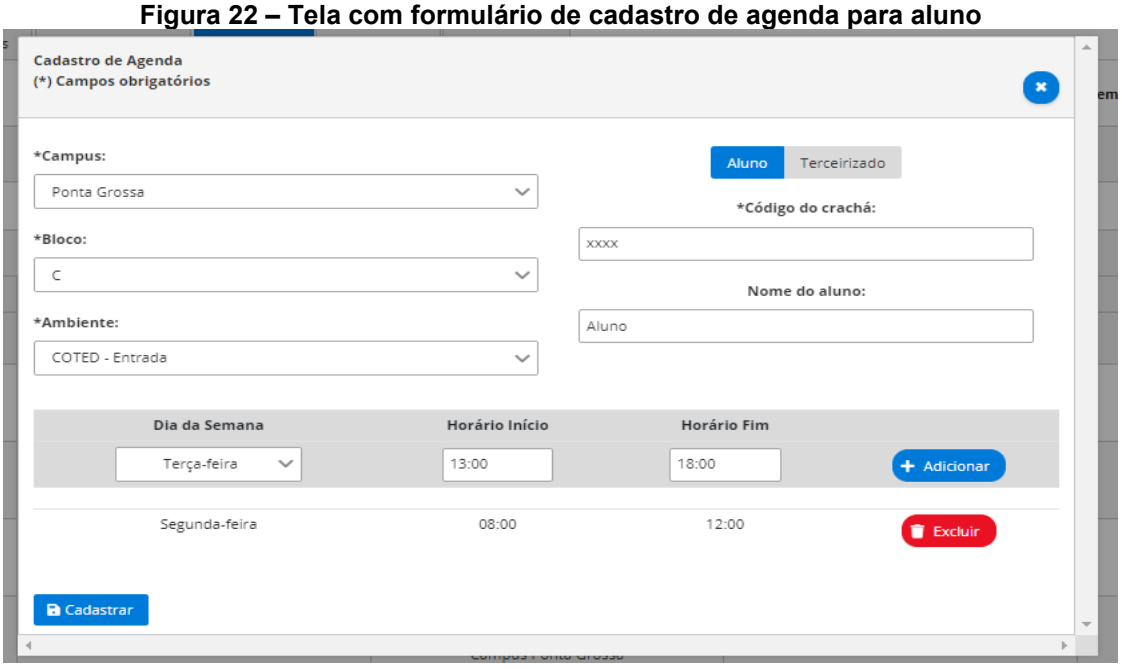
Figura 21 – Tela de gerenciamento de agendas



Fonte: Autoria própria (2022)

No cadastro da agenda é possível inserir regras por dia da semana em que o usuário tem permissão de acesso. O código informado na agenda deve ser de acordo com o identificador cadastrado no LDAP ou no sistema para que o mesmo possa ser identificado no momento da tentativa de acesso ao ambiente (ilustrado na Figura 22 e Figura 23).

Figura 22 – Tela com formulário de cadastro de agenda para aluno



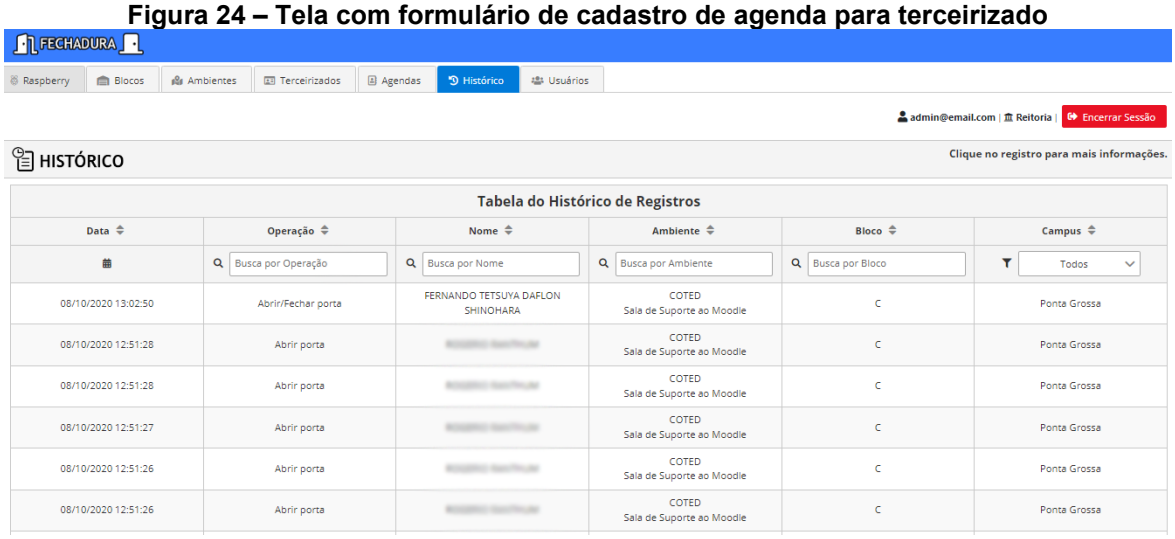
Fonte: Autoria própria (2022)

Figura 23 – Tela com formulário de cadastro de agenda para terceirizado

Fonte: Autoria própria (2022)

Ainda na aplicação web é possível verificar toda mudança de estado das fechaduras cadastradas e acionadas pelo sistema. No histórico de registros pode-se visualizar a data, horário, ambiente, qual ação foi efetuada como “abrir” ou “fechar” e o usuário responsável pela ação.

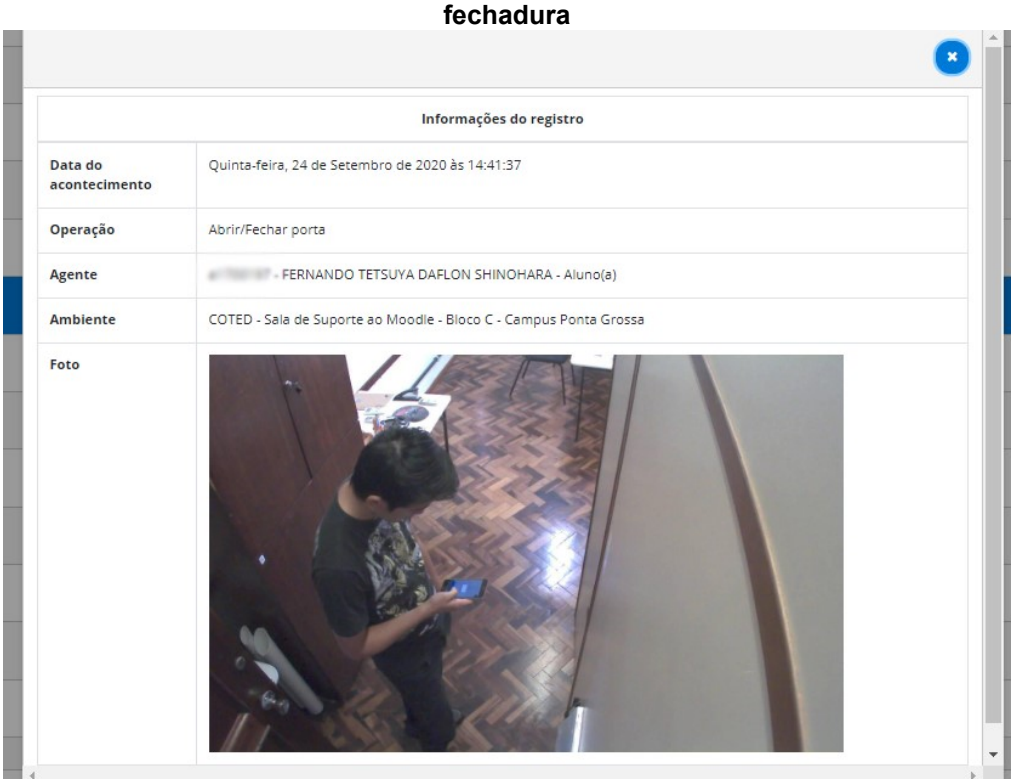
Figura 24 – Tela com formulário de cadastro de agenda para terceirizado



Fonte: Autoria própria (2022)

Para registros onde que a câmera IP foi configurada corretamente, pode-se visualizar a foto capturada no momento em que a ação com a fechadura foi registrada (ilustrada na Figura 25).

Figura 25 – Tela com visualização de informações geradas a partir de uma ação com a fechadura



Fonte: Autoria própria (2022)

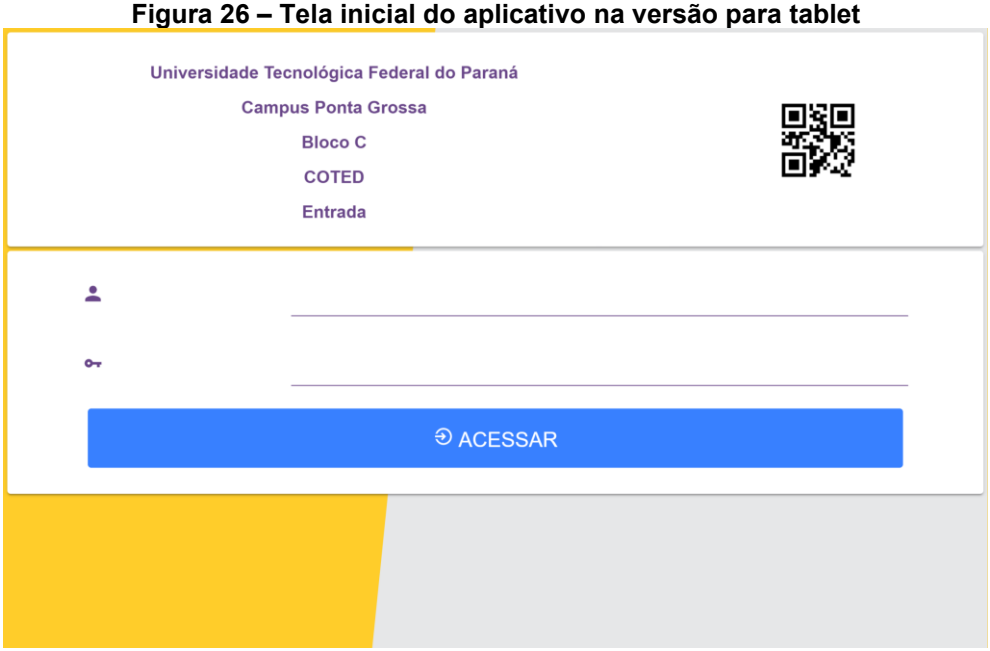
3.2.3 Aplicação para Dispositivo Móvel - Usuário

A aplicação para dispositivos móveis foi desenvolvida em Ionic, um framework de desenvolvimento de aplicativos multiplataforma para dispositivos móveis, com base em Angular. Um dispositivo móvel pode ser identificado como um smartphone ou tablet.

Por este aplicativo é possível interagir com uma fechadura a partir da leitura do QRCode gerado no gerenciamento de ambientes, na aplicação WEB (seção 3.2.2). Porém, como proposto pelo trabalho, existe a possibilidade de utilizar um tablet anexado próximo a uma fechadura e, com isso, foi desenvolvido duas versões do aplicativo.

A versão para tablet possui uma interface simplificada de interação rápida e momentânea com a fechadura. A mesma possui o QRCode referente ao ambiente ilustrado na tela para que possa ser utilizada com o celular pessoal dos usuários e, assim, interagir com o sistema (Figura 26).

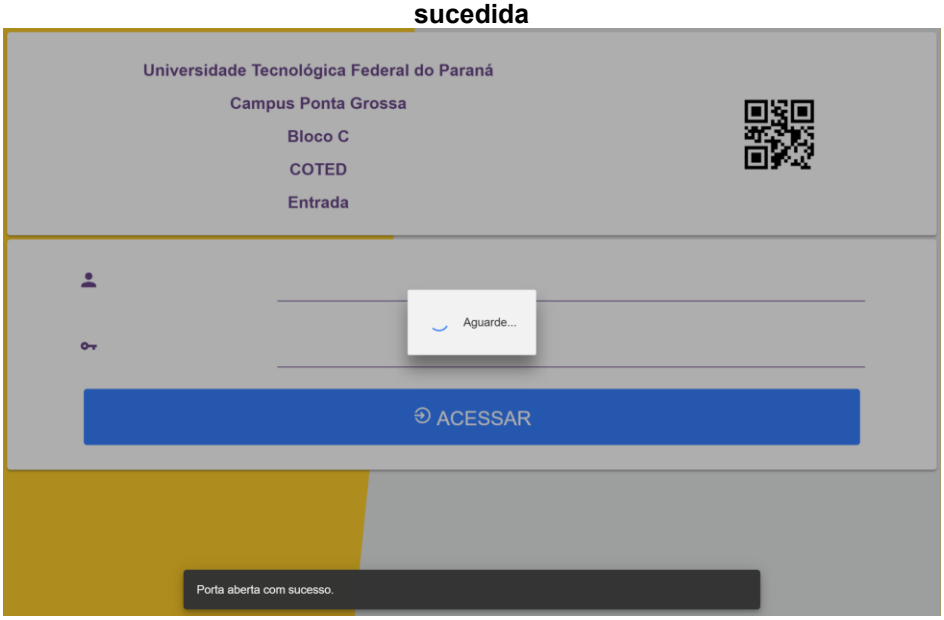
Figura 26 – Tela inicial do aplicativo na versão para tablet



Fonte: Autoria própria (2022)

Com a inserção dos dados de autenticação corretos e com o usuário permitido a interagir com a fechadura de acordo com as agendas criadas, tem-se o resultado, ilustrado na Figura 27, de sucesso.

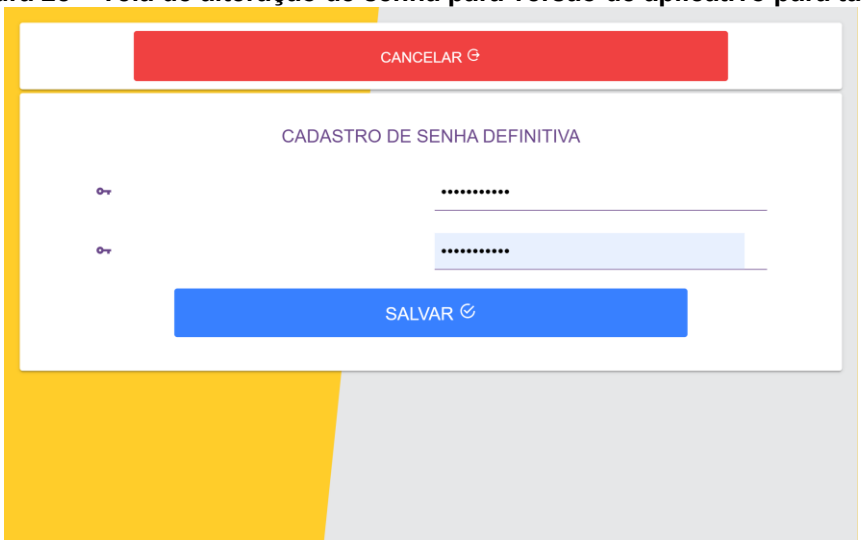
Figura 27 – Tela de carregamento de ação em fechadura após autenticação e permissão sucedida



Fonte: Autoria própria (2022)

Caso o usuário precise alterar a senha devido ao primeiro acesso, a tela ilustrada na Figura 28 é exibida.

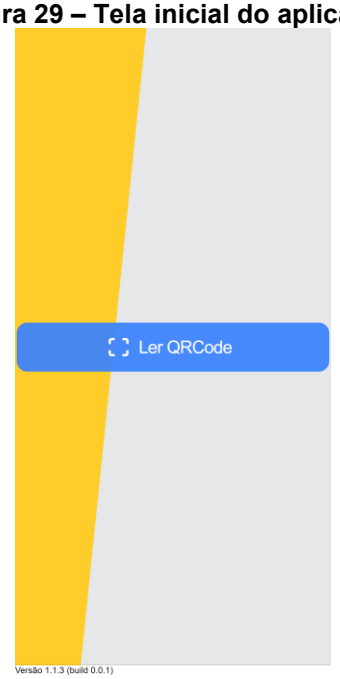
Figura 28 – Tela de alteração de senha para versão de aplicativo para tablet



Fonte: Autoria própria (2022)

A versão do aplicativo para uso em smartphone pessoal, possui uma tela inicial que exige o uso da câmera do dispositivo para leitura do QRCode.

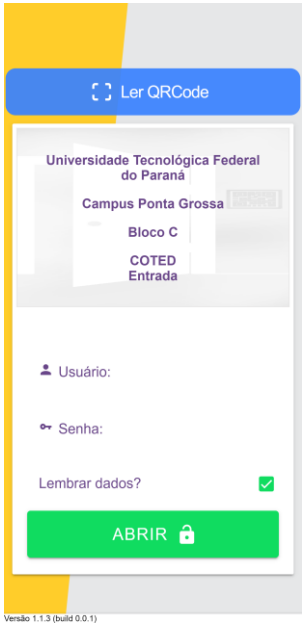
Figura 29 – Tela inicial do aplicativo



Fonte: Autoria própria (2022)

Com a leitura bem sucedida, é realizado uma consulta do estado atual da fechadura para que possa ser ilustrada ao usuário como nas Figura 30 e 31.

Figura 30 – Tela do aplicativo pós leitura de QRCode com estado da fechadura como fechada



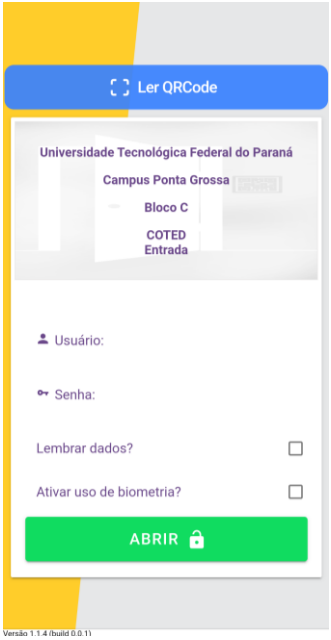
Fonte: Autoria própria (2022)

Figura 31 – Tela do aplicativo pós leitura de QRCode com estado da fechadura como aberta

Fonte: Autoria própria (2022)

Como um acesso alternativo, existem smartphones com leitor biométrico, e para aumentar a segurança e a facilidade do uso pelo usuário, tem-se a tela alterativa (Figura 32) quando é detectada tal funcionalidade no dispositivo.

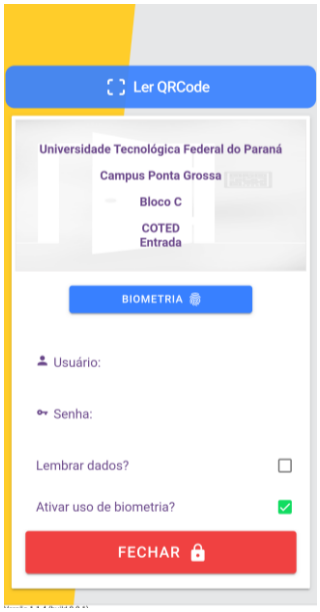
Figura 32 – Tela do aplicativo ao detectar funcionalidade de leitor biométrico no dispositivo



Fonte: Autoria própria (2022)

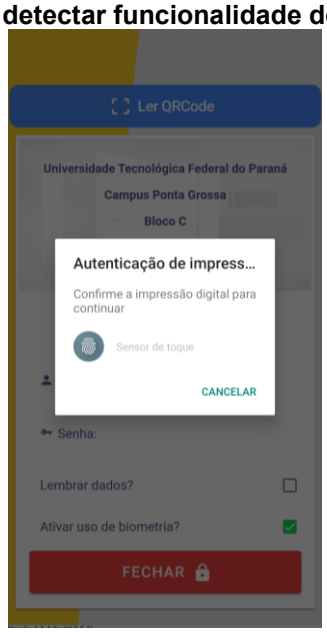
Ao ativado o uso de biometria para autenticação, é necessário inserir os dados de usuário e senha inicialmente para que estes dados sejam configurados para uso da biometria. Com os dados de autenticação validados é possível utilizar a funcionalidade a partir de um novo botão, como ilustrado na Figura 33 e Figura 34.

Figura 33 – Tela do aplicativo ao detectar funcionalidade de leitor biométrico no dispositivo



Fonte: Autoria própria (2022)

Figura 34 – Tela do aplicativo ao detectar funcionalidade de leitor biométrico no dispositivo



Fonte: Autoria própria (2022)

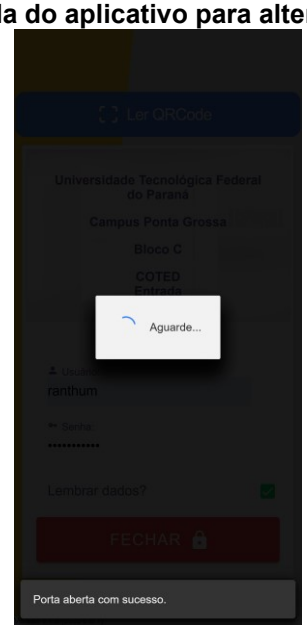
Assim como na versão para tablet, os usuários, como funcionários terceirizados e estagiários, poderão alterar a senha em seu primeiro acesso também (Figura 35).

Figura 35 – Tela do aplicativo para alteração de senha

Fonte: Autoria própria (2022)

Por fim, com a inserção de credenciais válidas e com uma agenda que permite acesso ao ambiente, tem-se o resultado exemplificado na Figura 36 com uma ação de abrir porta.

Figura 36 – Tela do aplicativo para alteração de senha



Fonte: Autoria própria (2022)

4 EXPERIMENTOS E RESULTADOS

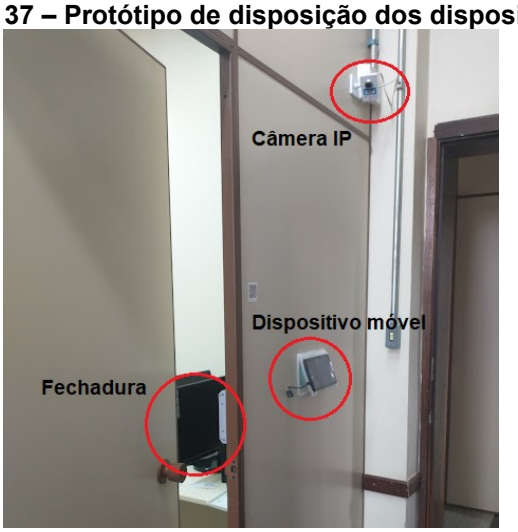
Para validar as implementações propostas, este capítulo aborda alguns testes com o sistema instalado em um ambiente real (seção 4.1) e análise de seus respectivos resultados (seção 4.2).

4.1 Experimento em ambiente real

O trabalho foi desenvolvido e instalado no ambiente do departamento COTED (Coordenação de Tecnologia na Educação) na UTFPR campus Ponta Grossa. Com o intuito de analisar o comportamento do sistema em uso diário, o mesmo foi configurado com agendas para acesso ao local por estagiários e o professor responsável do departamento.

Um protótipo de distribuição de componentes físicos pode ser visualizado na Figura 37.

Figura 37 – Protótipo de disposição dos dispositivos



Fonte: Autoria própria (2022)

A instalação física foi composta de um Raspberry Pi, fechaduras eletromagnéticas para três portas distintas, sendo elas duas portas comuns de abrir e uma de correr (ilustrada na Figura 38), fios elétricos para conexão entre os dispositivos, um tablet anexado a entrada de uma das portas e o QRCode impresso e anexado próximo a cada entrada controlada. Além disso, foi utilizado câmeras IP

de segurança já utilizadas no âmbito da universidade para obter imagens dos momentos de interação com as fechaduras.

Figura 38 – Sistema de fechadura instalada em porta de correr

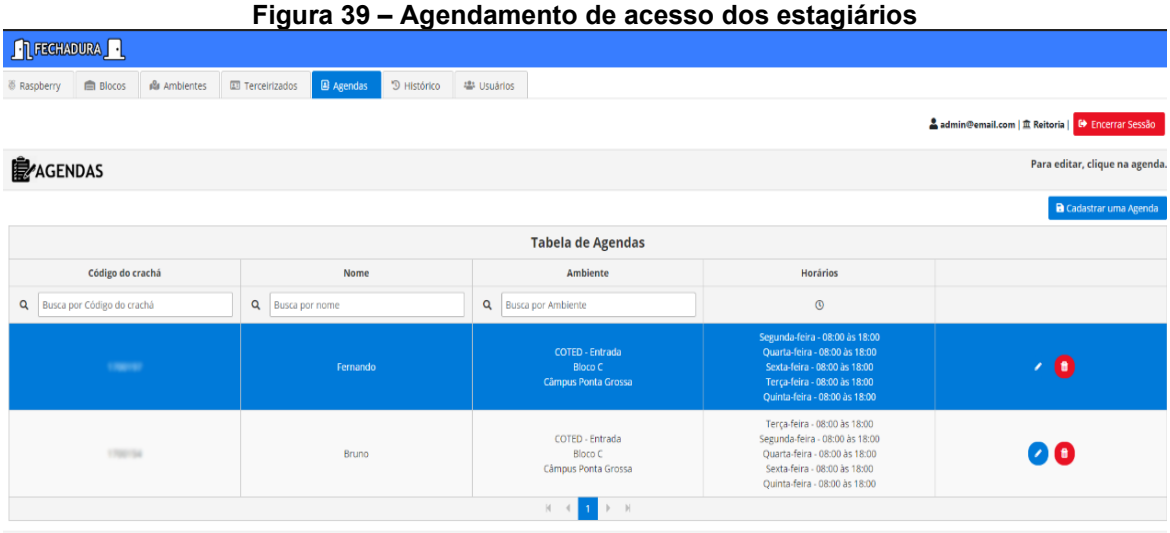
Fonte: Autoria própria (2022)

O acesso aos ambientes do departamento foi delimitado da seguinte maneira:

- O professor tem acesso a qualquer momento.
- Os estagiários/alunos tem acesso de Segunda-feira à Sexta-feira das 8 às 18 horas.

As configurações de agenda utilizados no sistema pode ser visualizado na Figura 39.

Figura 39 – Agendamento de acesso dos estagiários



Fonte: Autoria própria (2022)

4.2 Análise dos resultados

Com o intuito de analisar o comportamento do sistema proposto em diversas situações cotidianas, foi listado alguns testes e seus resultados, conforme mostra o quadro a seguir:

Quadro 1 – Testes aplicados ao trabalho proposto

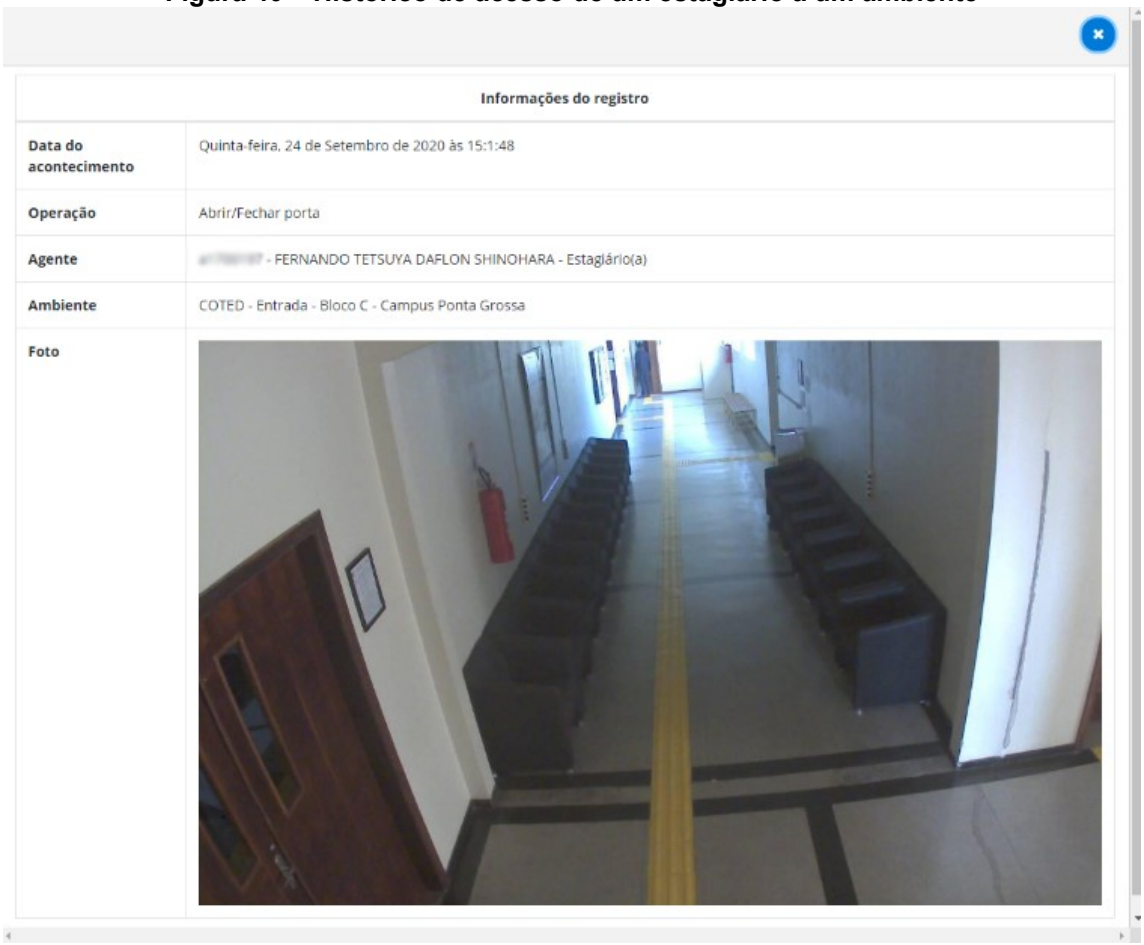
Descrição	Resultado
1. Acesso a um ambiente por usuário permitido por agenda.	Obteve-se resultado esperado. O usuário teve acesso ao ambiente e o ato foi registrado no histórico do sistema.
2. Acesso a um ambiente por professor.	Obteve-se resultado esperado. O professor teve acesso ao ambiente e o ato foi registrado no histórico do sistema.
3. Acesso a um ambiente por usuário não permitido.	Obteve-se resultado esperado. O usuário não teve acesso ao ambiente.
4. Queda energética. Sistema sustentando pela bateria.	Obteve-se resultado esperado. O sistema permaneceu em perfeito funcionamento por dois dias.
5. Queda energética e bateria sem carga.	Obteve-se resultado esperado. As fechaduras eletromagnéticas deixaram de funcionar e a porta ficou dependente apenas do sistema de tranca tradicional (chave mecânica).

Fonte: Autoria própria (2022)

Assim como descrito no Quadro 1, foram obtidos resultados positivos em relação ao funcionamento básico do sistema. Na Figura 40 pode-se visualizar um

histórico obtido a partir de um dos testes com acesso a um ambiente por um usuário estagiário permitido por agenda.

Figura 40 – Histórico de acesso de um estagiário a um ambiente



Fonte: Autoria própria (2022)

Durante o processo de testes tiveram algumas situações adversas consequentes do local de aplicação, no caso, a UTFPR Campus Ponta Grossa, como por exemplo, a impossibilidade de utilizar uma rede LAN dedicada para o sistema proposto. Com isso, alguns problemas de comunicação entre os dispositivos móveis e o sistema foi identificado como demora de resposta da fechadura devido ao congestionamento da rede, porém, não impossibilitou o uso do mesmo.

5 CONCLUSÃO

Este trabalho propôs o desenvolvimento de um sistema de controle de acesso, baseado em conceitos de Internet das Coisas, integrado com um sistema de fechadura eletromagnética visando baixo custo e menor impacto negativo financeiro e físico possível a sistemas de segurança já utilizados em um local.

Para atender aos requisitos do projeto, foi realizada uma pesquisa bibliográfica e de trabalhos correlatos com o intuito de buscar recursos e tecnologias já existentes e analisa-las para desenvolver uma solução de baixo custo e eficiente. Todos os dispositivos físicos utilizados são de fácil obtenção e instalação.

Por se tratar de um projeto com conceitos IoT, o uso de dispositivos modernos que possibilitam comunicação mútua foi de grande importância na facilidade de desenvolvimento do projeto físico e o uso por qualquer perfil de usuário. A utilização das tecnologias que permitem comunicação por protocolo HTTP prepara o sistema a suportar futuros incrementos e melhorias, pois o Raspberry Pi tem capacidade de controlar diversos outros eletrônicos.

No processo de implantação do sistema, pode-se citar como principal dificuldade o uso de uma rede LAN terceirizada, que pode interferir no bom funcionamento do sistema devido as configurações de segurança e tráfego de dados que independem do projeto proposto. Além disso, o uso de um dispositivo como um tablet anexado próximo às portas monitoradas pelo sistema, pode ser considerado como um ponto vulnerável, pois no trabalho proposto não foi projetado como o dispositivo pode ser disponibilizado para o usuário de maneira segura, evitando o furto do mesmo.

5.1 Trabalhos futuros

Como sugestão para trabalhos futuros pode-se citar: utilizar versões do microcomputador Raspberry Pi mais recentes para melhor desempenho e capacidade de processamentos dos dados; estudo aprimorado do uso de uma rede LAN dedicada e/ou conectada a internet; melhorias nas interfaces gráficas e informações necessárias para o uso da aplicação web e da aplicação para

dispositivos móveis; implementar e integrar o sistema com outro dispositivo eletrônico além da fechadura eletromagnética, como, por exemplo, ar condicionado, computador, entre outros. Além disso, pode-se desenvolver uma nova funcionalidade em que seja possível monitorar o estado de todos os eletrônicos conectados ao sistema em uma única tela na aplicação web, aprimorando a segurança dos ambientes.

REFERÊNCIAS

ACADEMIC. **Eletromagnetic lock.** Disponível em: https://en-academic.com/dic.nsf/enwiki/11677157. Acesso em: 27 abr. 2022.

ANDREAS; ALDAWIRA, C. R.; PUTRA, H. W.; HANAFIAH, N.; SURJARWO, S.; WIBISURYA, A. Door Security System for Home Monitoring Based on ESP32. **Procedia Computer Science**, v. 157, p. 673-682, set. 2019. doi: 10.1016/j.procs.2019.08.218.

BANKMYCELL. **How many phones are in the world?** Disponível em: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world. Acesso em: 15 de fevereiro de 2022.

BARMPATSALOU, K.; CRUZ, T.; MONTEIRO, E.; SIMOES, P. Current and Future Trends in Mobile Device Forensics: A Survey. **ACM Computing Surveys,** v. 51, n. 46, p. 1-31, abr. 2018. doi: 10.1145/3177847

BASHA, S. N.; JILANI, S. A. K.; ARUN, S. An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT. **International Journal Engineering Trends and Technology**, v. 33, n. 2, p. 84-89, mar. 2016. doi: 10.14445/22315381/IJETT-V33P217.

BOOTH, D.; HAAS, H.; MCCABE, F.; NEWCOMER, E.; CHAMPION, M.; FERRIS, C.; ORCHARD, D. **Web Services Architecture**. 2004. Disponível em: https://www.w3.org/TR/2004/NOTE-ws-arch-20040211/. Acesso em: 01 out. 2022.

DEVMEDIA. **WildFly – Do básico ao ambiente de produção.** Disponível em: https://www.devmedia.com.br/wildfly-do-basico-ao-ambiente-de-producao/33653#modulo-mvp. Acesso em: 22 abr. 2022.

GLBALTECHBRASIL. **A importância de se ter um sistema de câmeras de segurança em sua residência ou comércio.** 2019. Disponível em: https://blog.globaltechbrasil.com/a-importancia-de-se-ter-um-sistema-de-cameras-de-seguranca-em-sua-residencia-ou-comercio/. Acesso em: 27 abr. 2022.

GRIFFITH, C. **Mobile App Development with Ionic, Revised Edition:** Cross-Platform Apps with Ionic, Angular, and Cordova. 1. ed. Estados Unidos da América: O'Reilly Media, 2017.

INTELBRAS. **O que é e como funciona a tecnologia IP para monitoramento.** 2020. Disponível em: https://blog.intelbras.com.br/o-que-e-e-como-funciona-a-tecnologia-ip-para-monitoramento/. Acesso em 27 abr. 2022.

IONIC. **About us.** Disponível em: https://ionic.io/about. Acesso em: 22 abr. 2022.

JUNIOR, P. J. **Java Guia do Programador:** Atualizado para Java 16. 4. ed. São Paulo: Novatec Editora, 2021.

MACHADO, E. S.; JUNIOR, F. S. M. **Autenticação Integrada Baseada em Serviço de Diretório LDAP**. 2006. Disponível em: https://linux.ime.usp.br/~cef/mac499-06/monografias/erich/monografia.pdf. Acesso em: 22 abr. 2022.

KOSMATOS, E.; TSELIKAS, N.; BOUCOUVALAS, A. Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. **Advances in Internet of Things**, v. 1, n. 1, p. 5-12, abr. 2011. doi: 10.4236/ait.2011.11002.

LEE, I.; LEE, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. **Business Horizons**, v. 8, n. 4, p. 431-440, ago. 2015. doi: 10.1016/j.bushor.2015.03.008.

MADAKAM, S.; RAMASWAMY, R.; TRIPATHI, S. Internet of Things (IoT): A Literature Review. **Journal of Computer and Communications**, v. 3, n. 5, p. 164-173, mai. 2015. doi: 10.4236/jcc.2015.35021.

MILANI, A. **MySQL:** Guia do Programador. São Paulo: Novatec Editora, 2006.

MORIMOTO, C. E. Definição de LDAP. **Hardware.com.br**. 2004. Disponível em: https://www.hardware.com.br/termos/ldap. Acesso em: 22 abr. 2022.

NEHETE, P. R.; CHAUDHARI, J. P.; PACHPANDE, S. R.; RANE, K. P. Literature Survey on Door Lock Security Systems. **International Journal of Computer Applications**, v. 153, n. 2, p. 13-18, nov. 2016. doi: 10.5120/ijca2016911971.

PI4J. Pin Numbering - Raspberry Pi 3B+. **The Pi4J Project.** 2019. Disponível em: https://pi4j.com/1.2/pins/model-3b-plus-rev1.html. Acesso em: 15 abr. 2022.

PIRES, J. **O que é API? REST ou RESTFul? Conheça as definições e diferenças!** 2017. Disponível em: https://becode.com.br/o-que-e-api-rest-e-restful/. Acesso em: 23 abr. 2022.

RASPBERRY PI FOUNDATION. **What is a Raspberry Pi?** Disponível em: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/. Acesso em: 15 abr. 2022.

RAVULAVARU, A. **Learning Ionic:** Build hybrid mobile applications with HTML5, SCSS, and Angular. 2. ed. Birmingham: Packt Publishing, 2017.

RED HAT. **What is a REST API?** 2020. Disponível em: https://www.redhat.com/en/topics/api/what-is-a-rest-api. Acesso em: 23 abr. 2022.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World. **Internet Society.** 15 out. 2015. Disponível em: https://www.internetsociety.org/resources/doc/2015/iot-overview/. Acesso em: 19 abr. 2022.

SANDOVAL, J. **RESTFul Java Web Services:** Master core REST concepts and create RESTFul web services in Java. Birmingham: Packt Publishing, 2009.

SANKAR, S.; SRINIVASAN, P. Internet of Things Based Digital Lock System. **Journal of Computational and Theoretical Nanoscience**, v. 15, n. 9-10, p. 2758-2763, set. 2018. doi: 10.1166/jctn.2018.7535.

STANTON, C. Raspberry Pi 3 Model B Plus (B+) Technical Specifications. **Community Element14.** 9 mar. 2018. Disponível em: https://community.element14.com/products/raspberry-pi/w/documents/3453/raspberry-pi-3-model-b-plus-b-technical-specifications. Acesso em: 15 abr. 2022.

V-GUARD. **Como funciona a fechadura eletromagnética?** 2019. Disponível em: https://vguard.net.br/como-funciona-a-fechadura-eletromagnetica/. Acesso em: 29 abr. 2022.

VONGCHUMYEN, C.; WATANACHATURAPORN, P.; JINJAKAM, C.; WATCHARAPUPONG, A.; KASEMSIRI, W.; TONGPRASERT, K.; WALAIRACHT A.; PENPOKAI, T.; JENWEERAWAT, T.; HAMI, A. Door Lock System via Web Application. **International Electrical Engineering Congress**, p. 1-4, mar. 2017. doi: 10.1109/IEECON.2017.8075909.