

## **SEGURANÇA NO CAMPUS: FECHADURA INTELIGENTE COM IOT PARA CONTROLE DE ACESSOS NO LABORATÓRIO DE COMPUTAÇÃO APLICADA DA UFPA CASTANHAL**

**DOI: 10.5281/zenodo.13763902**

Karol Wojtyla Sousa Nascimento<sup>1</sup>

<sup>1</sup>Bacharelado em Engenharia de Computação – Universidade Federal do Pará (UFPA)

E-mail: karolwojtyla360@gmail.com

Lattes: <http://lattes.cnpq.br/6351448948601591>

Aridan Silva Pantoja<sup>2</sup>

<sup>2</sup>Bacharelado em Engenharia de Computação – Universidade Federal do Pará (UFPA)

E-mail: aridanpantoja@gmail.com

Lattes: <http://lattes.cnpq.br/8205729413400984>

Alícia de Almeida Maia<sup>3</sup>

<sup>3</sup>Bacharelado em Engenharia de Computação – Universidade Federal do Pará (UFPA)

E-mail: aliciaengcomp@gmail.com

Lattes: <http://lattes.cnpq.br/6904596930587739>

Sarah de Oliveira Cabral<sup>4</sup>

<sup>4</sup>Bacharelado em Engenharia de Computação – Universidade Federal do Pará (UFPA)

E-mail: sarah000cabral@gmail.com

Lattes: <https://lattes.cnpq.br/9275569788697680>

Bruno Souza Lyra Castro<sup>5</sup>

<sup>5</sup>Docente da Faculdade de Computação (Facomp) – Universidade Federal do Pará (UFPA)

E-mail: bruno@ufpa.br

Lattes: <http://lattes.cnpq.br/1897829604434609>

**RESUMO:** Neste trabalho foi proposto um projeto que aborda o desenvolvimento e funcionamento de uma fechadura inteligente que visa aprimorar controle de acesso seguro ao laboratório de computação por alunos, professores e servidores da UFPA Castanhal. O processo de construção desta ferramenta inclui a utilização da tecnologia RFID para identificação e rastreamento eficaz do acesso ao espaço, juntamente com a atuação do arduino uno e outros componentes de hardware para facilitação e reconhecimento de comportamentos do sistema; vale ressaltar também o uso de software para fazer o gerenciamento das informações adquiridas com base nas interações com o meio físico. A integração, tanto do hardware quanto do software, indica um potencial significativo para aplicação prática, posicionando o dispositivo como uma solução viável e robusta para as necessidades específicas do sistema em questão. O projeto destaca a importância da tecnologia IoT para a gestão de segurança em espaços universitários, promovendo uma abordagem inovadora e prática.

**Palavras-chave:** Controle de Acesso; Fechadura Inteligente; IoT; Sistemas Embarcados.

### **1. INTRODUÇÃO**

Nos últimos anos, os avanços tecnológicos têm transformado a interação humana com o mundo ao redor. Atualmente, não se avalia apenas o que os produtos fazem em termos de funcionalidade principal, mas também como os dados são coletados, interpretados e utilizados para identificar comportamentos e automatizar tarefas (Magrani, 2018). Nesse cenário, surgem sistemas como o controle automatizado de luzes e eletrodomésticos, monitoramento de sinais vitais por dispositivos vestíveis (*wearables*) e soluções de segurança que, embora destoem em suas aplicações, compartilham um conceito comum: a Internet das Coisas (IoT).

A IoT é o grande motor dessa transformação da interação humana para com o ambiente. Santos et al. (2016) define a IoT como uma extensão da internet que é aplicada em dispositivos do dia-a-dia e os torna aptos a ter uma capacidade computacional e de comunicação para além de suas funções regulares. Com o surgimento desse conceito, foi possível redesenhar processos e métodos, de modo a torná-los mais robustos e, conseqüentemente, mais eficazes para seus propósitos.

Um exemplo claro dessa aplicação está nos sistemas de segurança, essenciais para o funcionamento de diversos setores. Sabe-se que o acesso irrestrito a ambientes residenciais, empresariais e de pesquisa representa um risco à sua integridade física e produtiva. Nesse contexto, a IoT surge como uma solução eficaz ao substituir métodos tradicionais, como fechaduras e chaves, por tecnologias mais avançadas, como impressão digital, biometria reticular e, especificamente, a *Radio Frequency Identification* (RFID) – tomado como foco deste estudo (Peixer, 2023).

Desse modo, o presente trabalho tem como objetivo documentar o desenvolvimento de uma fechadura eletrônica com tecnologia RFID integrada, baseada em IoT e projetada para gerenciar e auditar o acesso dos colaboradores ao laboratório de computação aplicada da Faculdade de Computação (Facomp), no campus Castanhal da Universidade Federal do Pará (UFPA). O projeto busca, além de controlar o acesso de forma segura e eficiente, garantir a rastreabilidade das entradas de colaboradores e adicionar/remover acessos quando necessário, promovendo maior transparência e segurança no uso das instalações. Dessa forma, espera-se que o sistema proposto contribua para a otimização dos processos de segurança e gerenciamento de acessos no ambiente acadêmico.

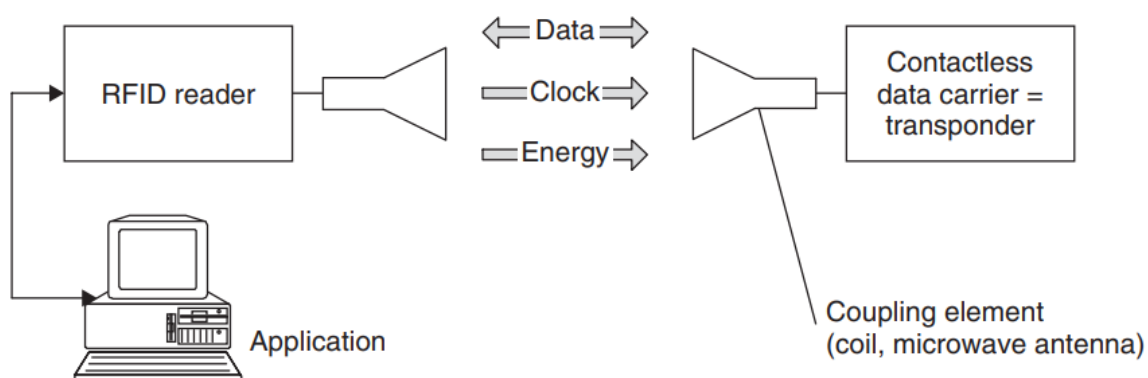
## **2. METODOLOGIA**

Para o desenvolvimento do projeto, inicialmente foi realizada uma revisão bibliográfica, a fim de entender, de uma maneira geral, como o sistema deveria funcionar em situações ideais,

mapeando seus requisitos funcionais e não-funcionais, bem como seus requisitos de *hardware*. Partindo desse princípio, inicialmente é importante enfatizar a tecnologia de identificação por radiofrequência que, por sua vez, desempenha um papel crucial no pleno funcionamento da solução, haja vista que a identificação de colaboradores do laboratório utilizará fundamentalmente essa tecnologia.

O RFID é uma tecnologia amplamente utilizada tanto para a identificação quanto para o rastreamento de objetos, animais e pessoas de forma automática e sem a necessidade de contato direto. Em suma, esse mecanismo funciona através da comunicação entre um leitor de RFID e uma *tag* RFID – objeto passivo de identificação única – que contém microchips capazes de transmitir dados via ondas de rádio (Want, 2006). Este projeto funcionará com *tags* RFID passivas, isto é, *tags* que não possuem fonte de alimentação própria, visando a melhor portabilidade e menor custo para a solução. Desse modo, o funcionamento da transferência de dados pode ser observado conforme a figura 1.

**Figura 1** - Transferência de dados entre leitor e tag RFID



**Fonte:** Finkenzeller, 2010.

Neste cenário, o leitor RFID emite um sinal de rádio que, por conseguinte, gera um campo eletromagnético que energiza a antena (microchip) interna da *tag*. A energia gerada faz com que a *tag* “responda” ao leitor, enviando os dados nela armazenados (Finkenzeller, 2010). O armazenamento de dados pode comportar diversas informações, no entanto, para este projeto, o principal dado armazenado é de um código de identificação único hexadecimal, que desempenhará o papel de identificador do colaborador (Borin, 2023).

Vale destacar que o leitor de RFID, por si só, é apenas um módulo responsável pela leitura dos dados armazenados na *tag*. Para que o sensor seja mantido sempre ativo e o tanto o processamento dos dados quanto a tomada de decisão sobre a liberação ou bloqueio de acessos

seja feita, se faz necessária a utilização de outros componentes tecnológicos, partindo desde a camada “física” do projeto – que engloba os microcontroladores e demais sensores para interação do usuário – até a parte lógica – na qual serão acessadas as informações processadas pelo meio físico (Peixer, 2023).

Nesse contexto, ainda na etapa de revisão bibliográfica, foi realizado um levantamento para embasar a escolha e análise dos insumos necessários ao desenvolvimento do projeto. No que diz respeito ao *hardware*, os componentes selecionados estão detalhados na Tabela 1:

**Tabela 1** - Listagem de componentes de *hardware* da fechadura eletrônica

Componente	Quantidade
Arduino Uno R3	1
Módulo RFID RC522	1
Chave Push Button	1
Módulo Relé 5V	1
Fonte 12V	1
Fechadura elétrica	1
LED Difuso 5mm Verde	1
LED Difuso 5mm Vermelho	1
Resistor 220R	2
Protoboard 400 Pontos	1
Buzzer	1

**Fonte:** autores.

Dentre os componentes observados na tabela, destacam-se:

- a) Arduino Uno R3:** o Arduino é uma plataforma de *hardware* e *software open source* baseada em microcontroladores e utilizada em projetos eletrônicos interativos. A placa Arduino vem equipada com um microcontrolador e diversas portas de entrada

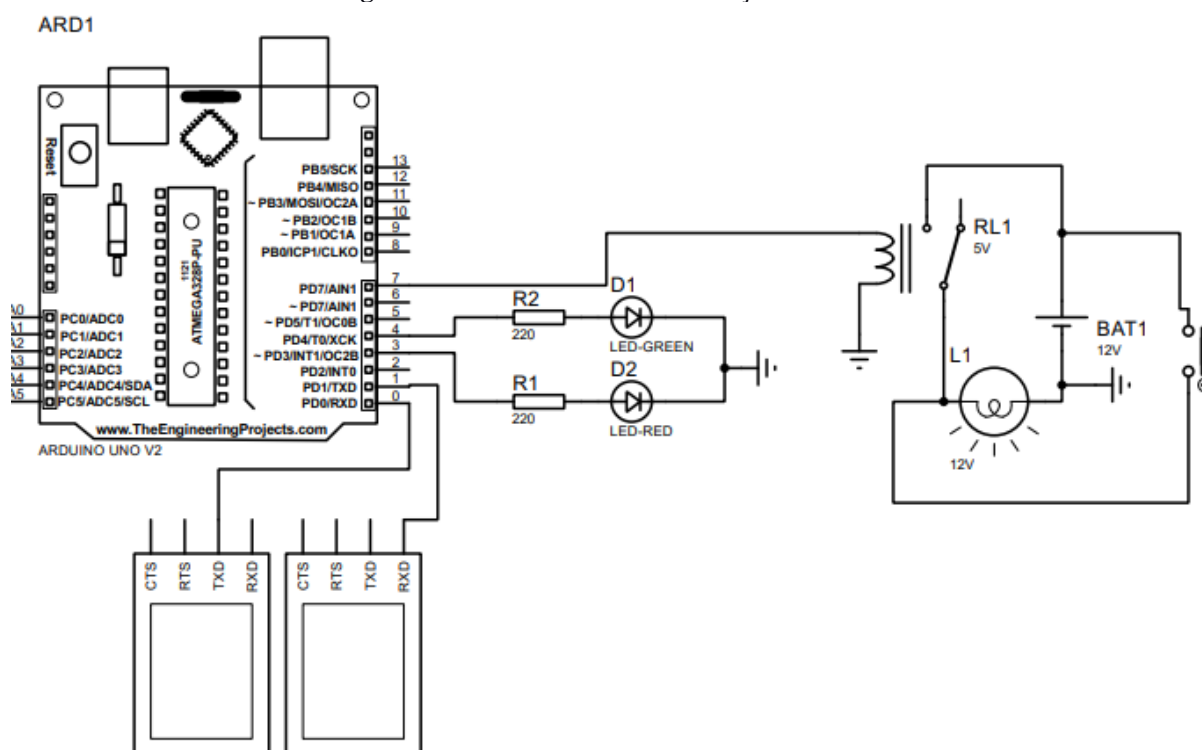
e saída, utilizadas para a alocação de módulos – como o leitor RFID (Kondaveeti, 2021). Para o projeto, o Arduino será o ponto focal no controle dos dados, gerenciando a leitura das *tags* RFID, processando as informações, acionando os LEDs e o buzzer para *feedback* do usuário, comandando o sistema de abertura e fechamento da fechadura e enviando os registros de entrada de pessoas para o banco de dados (Barros, 2019).

- b) Fechadura elétrica:** as fechaduras elétricas são mecanismos abertos por eletricidade ao invés da abertura manual tradicional. A fechadura escolhida tem seu estado inicial como trancado até que um cartão autorizado seja lido. Ao acontecer isso, um pulso elétrico de 12V é mandado à fechadura, que por sua vez tem seu eletroímã energizado e “atrai” a trava metálica da fechadura para trás, fazendo com que a porta seja destravada e o acesso à sala seja liberado (Borin, 2023).
- c) LEDs Vermelho e Verde:** os LEDs empregados ao escopo do projeto terão um papel crucial enviado ao *feedback* do usuário. O LED verde acenderá quando o acesso for autorizado, enquanto o LED vermelho será ativado em caso de tentativa de acesso não autorizado. Esses sinais são importantes para fornecer um retorno visual imediato ao usuário, facilitando a compreensão do estado do sistema (Barros, 2019).
- d) Buzzer:** os buzzers são dispositivos sonoros que complementarão o *feedback* visual inicialmente fornecido pelos LEDs. Eles emitem um som quando uma ação relevante ocorre, como a tentativa de acesso autorizada, não autorizada ou quando o sistema está operando corretamente. O uso de sinais sonoros garante que, além da sinalização luminosa, o usuário também receba um alerta auditivo, aumentando a acessibilidade e a clareza das respostas do sistema (Peixer, 2023).
- e) Fonte, resistores e relé:** a fonte de alimentação escolhida para o projeto é de 12V, sendo responsável por fornecer energia para todo o circuito, com destaque especial para a fechadura eletrônica. Como a fonte gera corrente contínua, é necessário o uso de um módulo relé para garantir que a voltagem seja enviada à fechadura apenas quando um cartão autorizado for lido pelo leitor RFID. Isso assegura que a fechadura só seja acionada nos momentos corretos, aumentando a segurança do sistema. Além disso, os resistores são utilizados para limitar o fluxo de corrente elétrica, convertendo o excesso de energia em calor. Essa limitação é essencial para proteger componentes eletrônicos mais sensíveis, garantindo que recebam apenas a carga necessária para seu funcionamento adequado dentro do projeto (Borin, 2023).

**f) Chave Push Button:** este componente será utilizado para facilitar a saída dos colaboradores do laboratório, uma vez que o sistema RFID é destinado exclusivamente ao controle de entrada, e a auditoria de acessos também se concentra na entrada. Quando pressionada, a chave push button enviará um pulso de voltagem para a fechadura eletrônica, acionando-a e permitindo a abertura da porta pelo lado interno. Esse mecanismo oferece uma solução simples e eficiente para o controle de saída, garantindo que a porta possa ser aberta rapidamente sem a necessidade de autenticação adicional.

Para a validação do funcionamento inicial do sistema com os componentes escolhidos, neste segundo momento da pesquisa, foi desenvolvida uma etapa de prototipagem em ambiente controlado, utilizando o simulador Proteus, que já conta com boa parte dos componentes listados na tabela 1 deste trabalho (Faludi, 2010). Um dos entraves encontrados para a simulação no Proteus foi especificamente a ausência do sensor RFID e da fechadura elétrica. No entanto, para fins de simulação de interação entre componentes, foi possível desenvolver o esquemático presente na figura 2, substituindo a fechadura elétrica por uma lâmpada de 12V com comportamento similar:

**Figura 2 - Circuito elétrico da simulação no Proteus**

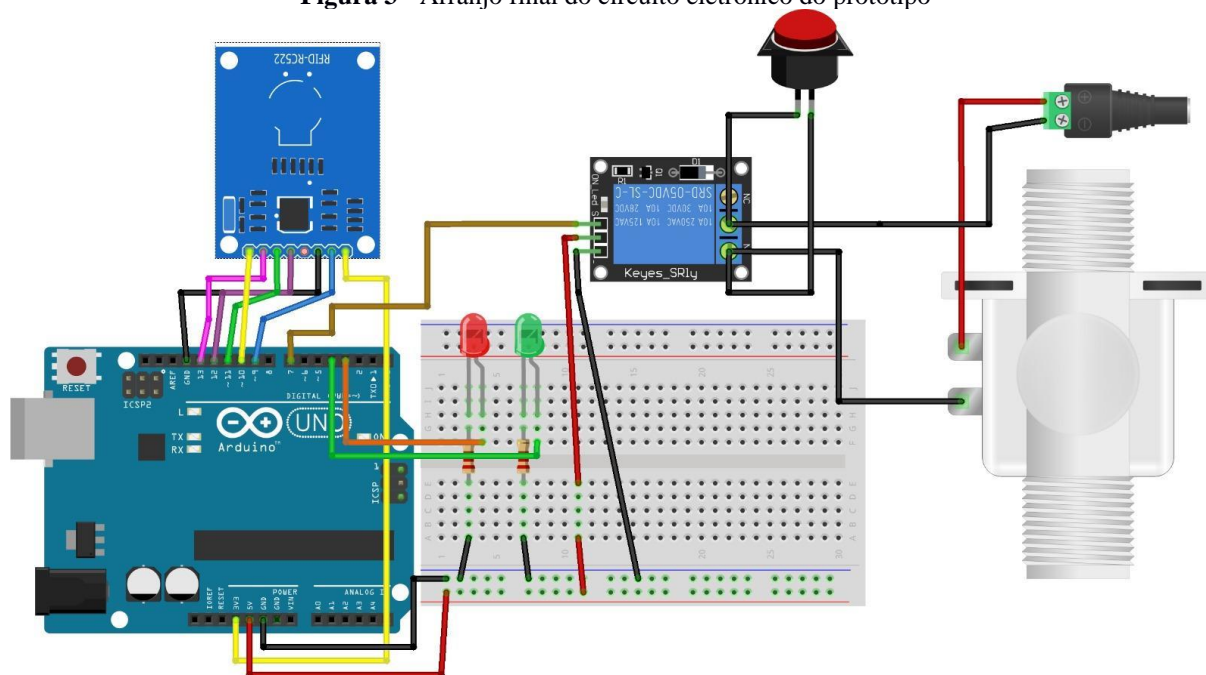


**Fonte:** autores.



Dessa forma, foi possível analisar a interação dos componentes entre si e pensar em formas de otimizar o desempenho e a futura interface com o banco de dados para a aplicação web. A partir disso, foi possível obter o seguinte esquemático do circuito integrado final:

**Figura 3** - Arranjo final do circuito eletrônico do protótipo



**Fonte:** autores.

Com a parte física do projeto estruturada, iniciou-se o trabalho de integração do sistema com a internet, transformando-o numa solução completa de IoT (Magrani, 2018). Para que o sistema cumpra seu papel de possibilitar o registro e auditoria de acessos em tempo real através de uma interface web conectada a um banco de dados, é indispensável a presença de um mediador entre o sistema físico e a internet (Rosa, 2022). No projeto, foi utilizado um computador dedicado exclusivamente a esse fim.

Dessa maneira, o microcontrolador realiza a leitura de uma tag RFID através do leitor RC522, capturando o ID único presente no chip e processando essa informação. Após o processamento, o Arduino transmite os dados para o computador via comunicação serial, que, por meio de um script em python, recebe o ID e faz uma requisição HTTP POST, para uma API desenvolvida em Node.js com o framework Fastify, sendo uma escolha altamente escalável e eficiente para o tratamento das requisições (Fastify, 2024).

Após a requisição, a API consulta um banco de dados PostgreSQL para verificar se o ID está registrado e se o usuário possui permissão de acesso à sala. O PostgreSQL é um sistema de gerenciamento de banco de dados relacional altamente versátil e portátil (PostgreSQL, 2024),

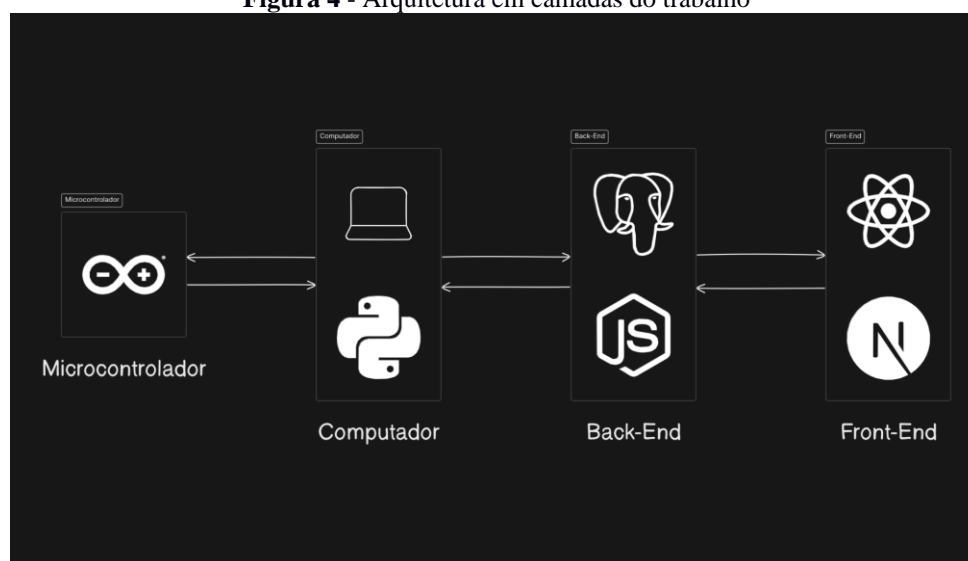
que permite que a aplicação armazene registros detalhados das tentativas de acesso ao laboratório, bem como informações sobre os usuários autorizados e não autorizados.

Caso o ID esteja registrado no banco de dados, o script em Python no computador recebe uma resposta com status 200 e um campo success definido como verdadeiro, enviando um comando ao Arduino para liberar o acesso e acionar a fechadura. No entanto, se o acesso for negado, o script recebe um status 403 e o campo success será falso.

Os dados presentes no banco de dados são consumidos por uma aplicação web, desenvolvida utilizando-se React e Next.js. O React é uma biblioteca JavaScript amplamente utilizada para a criação de interfaces de usuário dinâmicas e responsivas, permitindo que a aplicação ofereça uma experiência fluida e interativa aos usuários (React, 2024). Já o Next.js é um poderoso framework que complementa o React, fornecendo recursos como renderização no lado do servidor e geração estática de páginas, o que melhora o desempenho e a SEO da aplicação (Next.js, 2024). Com essa combinação, a solução permite que os dados sejam acessados em tempo real, garantindo que os gestores possam monitorar e auditar os acessos ao laboratório de forma eficaz e eficiente, em qualquer lugar com acesso à internet.

A arquitetura completa do trabalho pode ser observada na figura 4:

**Figura 4 - Arquitetura em camadas do trabalho**



**Fonte:** autores.

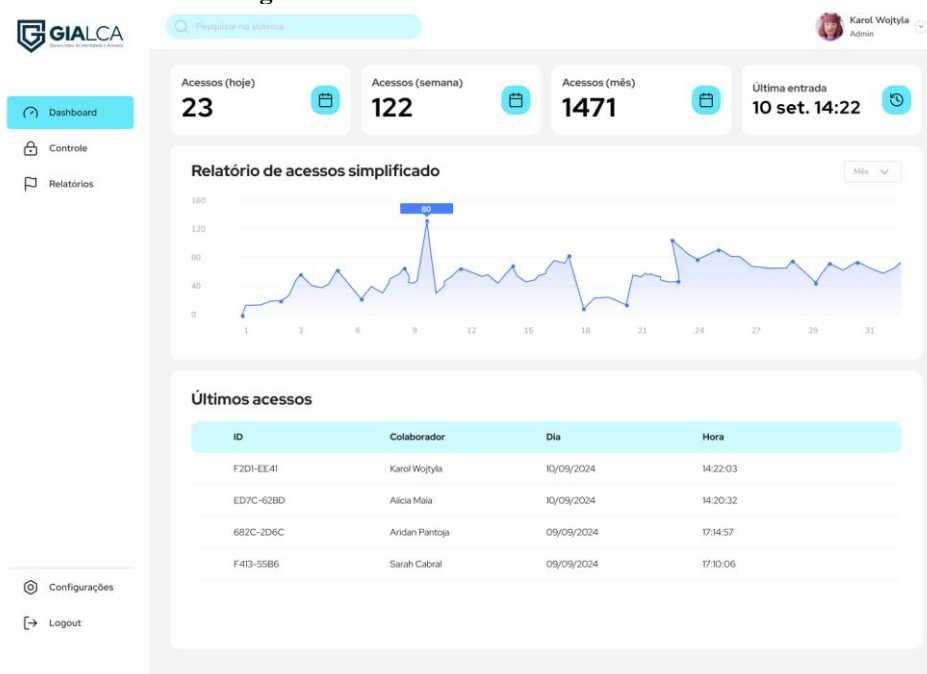
### **3. RESULTADOS E DISCUSSÃO**

Mediante a realização da bateria de simulações, implantação e testes no sistema proposto, foi possível identificar sua funcionalidade em casos reais de uso. Um dos principais pontos observados foi a eficiência da solução no enfrentamento da problemática apresentada



neste estudo. O tempo de resposta para a leitura da tag RFID e consequente liberação do acesso, após múltiplas tentativas, apresentou uma média de 2 segundos, demonstrando a consistência e agilidade do sistema. Além disso, o envio dos dados de acesso do colaborador para o banco de dados e sua posterior transmissão à plataforma web integrada ocorre de forma imediata, sendo possível observar a entrada logo após o acesso.

**Figura 5** - Dashboard inicial da ferramenta

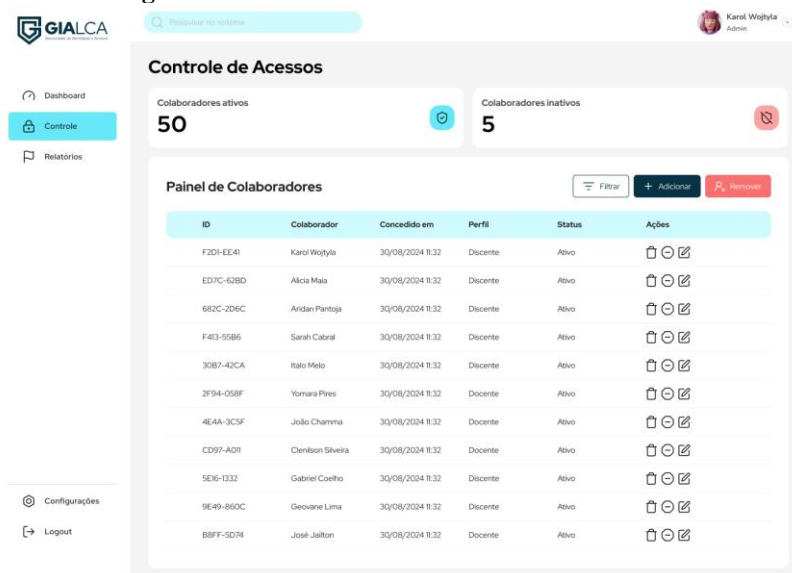


**Fonte:** autores.

Na *dashboard*, além dos acessos mais recentes, é possível também observar já um relatório breve especificando a quantidade de acessos no dia, na semana e no mês da exibição, além de um gráfico de contabilização da entrada de colaboradores em relação a um período de tempo - dia, semana ou mês -, que apoia o administrador na visualização, análise e gera *insights* para possíveis tomadas de decisão, agregando um teor estratégico à ferramenta (Soares, 2019).

Para a administrar os colaboradores aptos a acessar o laboratório, a solução entrega uma interface de gestão de acessos, baseada nas disciplinas de *Identity and Access Management* (IAM) adotadas por grandes empresas, cujo objetivo é especificar quem pode acessar e que recursos podem acessar dentro de um ambiente (Glockler, 2023). A ferramenta traz ainda a possibilidade de verificar quantos colaboradores estão ativos ou inativos, editar um colaborador, excluí-lo ou suspendê-lo conforme necessidade, conforme ilustra a figura 6:

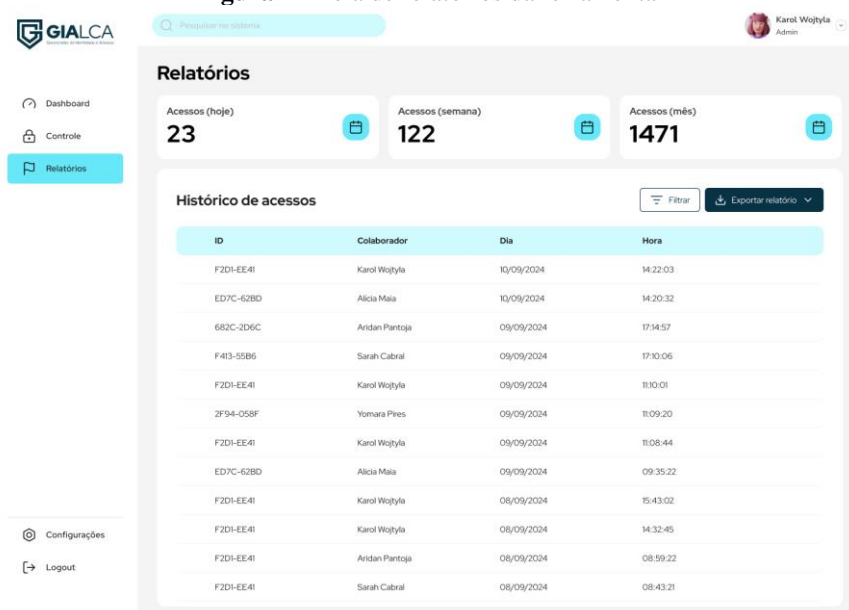
**Figura 6** - Tela de controle de acessos da ferramenta



Fonte: autores.

Para facilitar os processos de auditoria de acessos ao laboratório, foi implementada a função de relatórios, permitindo o acesso a um histórico detalhado dos colaboradores que entraram no laboratório, bem como a data e hora dos respectivos acessos. Essa funcionalidade oferece uma visão ampla dos registros, com a opção de "Filtrar" para buscar períodos, colaboradores ou perfis específicos. Além disso, os relatórios, filtrados ou completos, podem ser exportados para arquivos .CSV ou .XLSX, tanto para fins de *backup* quanto para análise em ferramentas de gestão de dados.

**Figura 7** - Tela de relatórios da ferramenta



**Fonte:** autores.

Dessarte, percebe-se que a ferramenta não somente sana a problemática inicialmente proposta, como também gera insumos para futuras análises e medidas no acesso ao laboratório, fornecendo uma base sólida de dados que pode ser utilizada para otimizar processos de segurança e gestão, além de possibilitar o desenvolvimento de melhorias contínuas na solução implementada.

#### **4. CONSIDERAÇÕES FINAIS**

Diante dos resultados obtidos, é possível concluir que o sistema desenvolvido possui um desempenho satisfatório, tendo em vista os tempos de respostas rápidos e uma integração robusta do sistema físico com a plataforma web. Além disso, a possibilidade de geração e exportação de relatórios de acesso para análise adicional configura um importante insumo para a gestão e auditoria dos acessos, oferecendo ao administrador uma visão abrangente e detalhada das atividades no laboratório.

A solução proposta também destaca a importância da integração de tecnologias como RFID e IoT na criação de sistemas de controle de acesso mais seguros e eficientes. A ferramenta desenvolvida não só resolve a questão de segurança apresentada, mas também serve como uma plataforma para futuras melhorias e análises aprofundadas nos processos do laboratório.

A análise de custo-benefício do projeto revela sua plena eficácia, uma vez que utiliza componentes de baixo custo na parte física e não incorre em despesas adicionais na parte web. Apesar desses fatores econômicos, o sistema oferece uma experiência altamente eficiente e diferenciada, tanto para os gestores do laboratório quanto para os colaboradores que o utilizam diariamente.

Para trabalhos futuros, recomenda-se a exploração de tecnologias adicionais de permissionamento e IAM, e a expansão das funcionalidades do sistema, visando aprimorar a experiência do usuário e fortalecer ainda mais a segurança do ambiente. A aplicação de técnicas avançadas de análise de dados e a integração com outras soluções de segurança poderão oferecer novas perspectivas e soluções inovadoras para o controle de acessos.

#### **REFERÊNCIAS**

##### **Artigo em Revista:**

FASTIFY. Fastify: **Fast and low overhead web framework, for Node.js**. Disponível em: <https://fastify.dev/>. Acesso em: 04 set. 2024.

GLÖCKLER, J. et al. **A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity.** Business & Information Systems Engineering, p. 1-20, 2023.

KONDAVEETI, H. K. et al. **A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations.** Computer Science Review, v. 40, p. 100364, 2021.

NEXT.js. **Documentação do Next.js.** Disponível em: <https://nextjs.org/docs>. Acesso em: 04 set. 2024.

POSTGRESQL. PostgreSQL: **The World's Most Advanced Open Source Relational Database.** Disponível em: <https://www.postgresql.org/>. Acesso em: 04 set. 2024.

REACT. React: **The library for web and native user interfaces.** Disponível em: <https://react.dev/>. Acesso em: 04 set. 2024.

ROSA, A.; TEIXEIRA, D.; ALVES JR, N. **Comunicações seguras entre dispositivos IoT utilizando o ESP32.** NOTAS TÉCNICAS, v. 12, n. 2, 2022.

WANT, R.. **An introduction to RFID technology.** IEEE Pervasive Computing, v. 5, n. 1, p. 25-33, 2006.

**Dissertação, Tese e Trabalho de Conclusão de Curso:**  
BARROS, O. P. **Desenvolvimento de fechadura inteligente utilizando tecnologia RFID.** 2019.

BORIN, P. H. B.; PERPÉTUO, V. O. **Abertura de fechadura elétrica por aproximação com RFID passivo.** 2023.

PEIXER, F. M. et al. **Desenvolvimento de um protótipo de um sistema de controle de acesso via RFID.** 2023.

SOARES, D. R. **Análise de Dados em Processos de Auditoria.** 2019. Tese de Doutorado. Universidade Estadual de Campinas.

**Livro:**  
FALUDI, R.. **Building Wireless Sensor Networks: with ZigBee, XBee, Arduino, and Processing.** O'Reilly Media, 2010.

FINKENZELLER, K. **RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.** John Wiley & Sons, 2010.

MAGRANI, E.. **A internet das coisas.** Editora FGV, 2018.

SANTOS, B. P. et al. **Internet das Coisas: da Teoria à Prática.** [S.l.], Belo Horizonte: Departamento de Ciência da Computação, Universidade Federal de Minas Gerais. 2016.