

Sistema Automático de Gestão Wi-Fi Integrado a Carteirinhas RFID, NFC e QR Code para Controle de Presença de um Laboratório de Pesquisa e Extensão

Carlos Eduardo Lopes Fenos
Centro Federal de Educação
Tecnológica de Minas Gerais -
Campus Leopoldina
carlos.27@aluno.cefetmg.br

Bruno Reiff Gonçalves
Centro Federal de Educação
Tecnológica de Minas Gerais -
Campus Leopoldina
goncalves@aluno.cefetmg.br

Luís Augusto Mattos Mendes
Centro Federal de Educação
Tecnológica de Minas Gerais -
Campus Leopoldina
luisaugusto@cefetmg.br

Alexandre Martins Gama de
Deus
Centro Federal de Educação
Tecnológica de Minas Gerais -
Campus Leopoldina
alexandremartins@cefetmg.br

Galba Falce de Almeida
Centro Federal de Educação
Tecnológica de Minas Gerais -
Campus Leopoldina
galba.almeida@cefetmg.br

Abstract

The growth of research and extension activities at Centro Federal de Educação Tecnológica de Minas Gerais - Campus Leopoldina has increased the need for systems capable of ensuring security, traceability, and efficiency in user management and access control within the Laboratório de Iniciação Científica e Extensão da Computação (LINCE). In this context, an intelligent system was developed integrating RFID, NFC, and QR Code technologies into digital identification cards, combined with the automated generation of temporary Wi-Fi authentication vouchers. The solution also includes an updated interface for the existing project management system, enhancing usability, clarity, and information organization. The development followed a structured software engineering approach, encompassing analysis of related systems, requirements elicitation, modeling, and initial implementation. Partial results include the definition of the system architecture, complete database modeling, and prototyping of the main interfaces. As a contribution, the proposed system aims to modernize physical and digital access control, strengthen institutional security, and improve support for research and extension activities.

Keywords

Access Management; RFID; NFC; QR Code; Wi-Fi authentication.

1 Introdução

No contexto das instituições federais de ensino superior a criação de programas de iniciação científica e extensão tecnológica desenvolvida pelo Conselho Nacional de Desenvolvimento Tecnológico (CNPq) contribui para a formação de jovens para as carreiras de ciência e tecnologia, além da formação científica de profissionais aptos a enfrentarem os desafios da sociedade[1].

Dessa forma, com o objetivo de incentivar os projetos científicos e de extensão no Centro Federal de Educação Tecnológica de Minas Gerais - Campus Leopoldina, foi criado em 2019 o Laboratório de Iniciação Científica e Extensão da Computação (LINCE). O referido laboratório é caracterizado como um ambiente de desenvolvimento

de projetos que oportuniza o convívio e a troca de experiências entre servidores e alunos, contribuindo para a formação pessoal e profissional, além de fortalecer o desenvolvimento de projetos de natureza científica, tecnológica e de extensão direcionados para auxiliar na resolução de problemas da sociedade ou no aprimoramento de processos existentes.

Com a criação do laboratório e o crescimento significativo dos projetos desenvolvidos no LINCE, observou-se a necessidade de desenvolver um sistema para gestão que possibilitou a contagem de projetos em andamento, de todos os discentes e docentes que já participaram de projetos, possibilitando gerar indicadores do laboratório[2]. Entretanto, ainda não há um controle de uso eficiente do laboratório, visto que, o controle de acesso dos usuários e permanência no laboratório é feito de forma manual utilizando-se de papel e caneta.

Portanto, diante desse cenário, identificou-se a necessidade de adotar ferramentas que facilitem o controle de usuários para gestão do laboratório permitindo gerar, de forma automatizada, indicadores como: membros associados à determinado projeto, professores e seus respectivos orientandos, tempo de permanência dos usuários no laboratório, tempo de utilização dos recursos tecnológicos do laboratório por usuário.

Além disso, identificou-se outro problema relacionado ao controle de acesso físico ao laboratório. Atualmente, a retirada da chave para acesso ao laboratório, assim como das demais salas do campus Leopoldina, é centralizada na portaria, a qual funciona como ponto único de registro de entrada e saída. Sendo assim, uma lista constantemente atualizada contendo os nomes dos usuários autorizados a efetuar a retirada da chave do laboratório é disponibilizada na portaria. Contudo, devido ao crescimento contínuo no número de alunos vinculados a projetos, manter essa lista atualizada é um desafio para os gestores do laboratório. Essa falha no controle de acesso às chaves do laboratório pode resultar em situações de inconsistência na verificação de autorização, aumentando o risco de acesso indevido ao laboratório e comprometendo a segurança dos equipamentos e das atividades realizadas no ambiente, as quais demandam confidencialidade e privacidade.

Diante desse cenário, identificou-se a necessidade de desenvolver um sistema automático de gestão de rede Wi-Fi integrado a carteirinhas digitais com tecnologias RFID, NFC e QR Code para controle de acesso físico ao laboratório e identificação dos pesquisadores e extensionistas vinculados aos projetos em andamento. Essas carteirinhas também permitirão o gerenciamento do acesso à chave do laboratório, reduzindo ocorrências de uso indevido e os problemas ocasionados pela desatualização das listas de autorização ao LINCE. A utilização de biometria também foi considerada, porém não foi adotada devido ao maior custo de implantação, à necessidade de infraestrutura específica e a preocupações relacionadas à privacidade e ao tratamento de dados biométricos sensíveis [3].

Além do controle físico, o sistema integrará as carteirinhas ao serviço de rede sem fio (Wi-Fi), possibilitando a emissão de vouchers temporários exclusivamente para usuários autorizados. Essa solução permitirá registrar quem está conectado, em que momento e por quanto tempo, favorecendo uma gestão mais eficiente e segura dos recursos tecnológicos do laboratório. Por fim, o projeto também contempla a modernização do layout do sistema de gestão de projetos previamente desenvolvido [2], buscando aprimorar sua usabilidade, desempenho e experiência de uso de forma mais intuitiva e eficiente.

Portanto, o presente artigo aborda o processo de desenvolvimento deste produto de software. Além desta introdução, este artigo está organizado em mais 5 seções. A Seção 2 fundamenta o Referencial Teórico; a Seção 3 apresenta os Trabalhos Relacionados; a Seção 4 descreve os Materiais e Métodos utilizados para o desenvolvimento do produto de software; a Seção 5 trata os Resultados e, por fim, a Seção 6 apresenta as Considerações Finais, seguida dos Agradecimentos e Referências Bibliográficas.

2 Referencial Teórico

A gestão eficiente de acesso físico e digital em ambientes acadêmicos e laboratórios de pesquisa demanda processos bem estruturados e sistemas integrados de identificação e autenticação. Soluções tecnológicas, como RFID (Identificação por Radiofrequência), NFC (Comunicação por Campo de Proximidade) e QR Code (Código de Resposta Rápida) têm se tornado cada vez mais adotadas em instituições de ensino, visto que, não apenas agilizam processos de gestão, mas também possibilitam a segurança e organização das atividades desenvolvidas no ambiente acadêmico.

No âmbito dessas tecnologias de apoio à gestão e organização, o RFID é uma tecnologia de identificação automatizada de objetos, pessoas, bens e produtos por meio de ondas de rádio. Seu funcionamento é fundamentado basicamente em três elementos: uma etiqueta (ou TAG), que está presa ao objeto e armazena o identificador numa memória; o leitor com antena, que faz transmissão e recepção de dados com a TAG; e a unidade de controle, responsável pelo processamento e pela produção de um resultado. Nos últimos anos o uso dessa tecnologia tem crescido significativamente, principalmente por sua versatilidade e pela vantagem de não exigir contato físico direto entre os dispositivos [4].

O NFC é uma tecnologia de identificação sem fio de curto alcance inspirada pelo padrão do RFID. Por isso os componentes de um sistema RFID e NFC são os mesmos, diferindo apenas a forma

como eles interagem. O NFC também permite a troca de dados entre dois dispositivos, mas com alcance minimizado, limitado a dez centímetros de distância. Esses equipamentos utilizados possuem um microchip NFC que contém uma memória suficiente para armazenar uma pequena quantidade de dados e que pode estar dentro de um chaveiro, de um cartão, de uma etiqueta (TAG), de um leitor ou de um smartphone compatível com a tecnologia NFC [5]. A Figura 1 apresenta os componentes básicos de um sistema RFID/NFC.

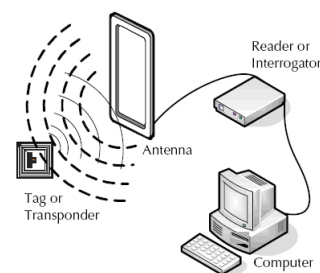


Figura 1: Componentes Básicos de um Sistema RFID/NFC [4].

Diferentemente do RFID e do NFC, que utilizam radiofrequência para comunicação, o QR Code baseia-se na leitura óptica por meio de câmeras ou scanners específicos. Trata-se de um código bidimensional capaz de armazenar informações em padrões gráficos que podem ser rapidamente interpretados por dispositivos digitais[5]. Entre suas principais vantagens estão o baixo custo de implementação, a facilidade de geração e a ampla compatibilidade com smartphones.

O monitoramento de acesso a redes sem fio em ambientes institucionais constitui uma prática relevante para a garantia da segurança da informação e da rastreabilidade das conexões realizadas. As redes Wi-Fi modernas adotam diferentes mecanismos de proteção, como o padrão WPA3 e a utilização de portais cativos (captive portals), os quais permitem validar a identidade do usuário antes da liberação do acesso à Internet Wi-Fi Protected Access 3 Captive portal. Esses mecanismos são amplamente empregados em instituições de ensino e organizações que necessitam controlar o uso da infraestrutura de rede, garantindo autenticação adequada e registro das sessões de conexão.

Nesse contexto, soluções baseadas em autenticação centralizada e geração de credenciais temporárias, como vouchers de acesso, têm sido adotadas por possibilitarem limitação temporal de uso, associação entre usuário e sessão ativa e maior controle administrativo da rede. A conectividade wireless desempenha papel essencial em ambientes acadêmicos e laboratoriais, uma vez que viabiliza mobilidade, acesso distribuído a recursos computacionais e integração entre diferentes dispositivos, exigindo, portanto, mecanismos de controle compatíveis com tais demandas.

3 Trabalhos Relacionados

Para contextualização do tema, foram analisados os trabalhos a seguir, cada um contribuindo parcialmente para realização do projeto.

Um dos principais referenciais foi o Sistema de Carteirinhas com QR Code da União Brasileira dos Estudantes Secundaristas (UBES), desenvolvido em parceria com a União Nacional dos Estudantes

(UNE) e a Associação Nacional de Pós-Graduandos (ANPG). Esse sistema é reconhecido nacionalmente por comprovar a condição estudantil e assegurar direitos garantidos por lei [6]. Sua estrutura evidencia a importância de oferecer aos estudantes um meio físico ou digital de identificação, funcionando como comprovação de vínculo e facilitando o acesso a benefícios. Essa perspectiva dialoga diretamente com um dos objetivos deste projeto, que busca fornecer aos pesquisadores e extensionistas uma forma prática e segura de comprovar seu vínculo ao Laboratório de Iniciação Científica e Extensão da Computação (LINCE).

No contexto da adoção de tecnologias baseadas em RFID, a Universidade Federal de Juiz de Fora (UFJF) se destaca, especialmente por empregar essa tecnologia em sistemas de controle de acesso e gerenciamento de passagem.

Em 2024, a instituição obteve três registros de programa de computador junto ao Instituto Nacional da Propriedade Industrial (INPI), todos relacionados a soluções de autenticação e automação. Os registros no INPI utilizam classificações padronizadas que indicam tanto o campo de aplicação quanto o tipo de programa envolvido. Em relação ao campo de aplicação, o código SV-01 refere-se a sistemas voltados a serviços e segurança, categoria diretamente alinhada a soluções de controle de acesso, enquanto TC-02 diz respeito a tecnologias de comunicação, apropriado para aplicações que fazem gerenciamento de passagem e autenticação distribuída. Já as categorias de tipo de programa detalham a natureza técnica das soluções: CD-04 e CD-01 contemplam softwares de controle e diagnóstico, IA-02 indica funcionalidades de identificação e autenticação, e PD-03 e PD-05 caracterizam programas de processamento de dados e gerenciamento operacional. Os códigos AP-03 e AT-05 relacionam-se a aplicações de automação e controle tecnológico, enquanto AV-02 se refere a avaliação e verificação, GI-04 a gestão de informações, PD-01 ao processamento inicial de dados e SO-05 a elementos de suporte a operações de sistemas.

Nesse sentido, o primeiro deles, o Sistema de Controle de Acesso – SCA [7], enquadra-se no campo de aplicação SV-01 e é classificado nos tipos de programa CD-04, IA-02, PD-03 e PD-05. Já o U2Pass Web [8], também registrado em SV-01, abrange um conjunto mais amplo de categorias, incluindo AP-03, AV-02, CD-04, GI-04, PD-01, PD-03, PD-05 e SO-05. Por fim, o sistema U2Pass [9], classificado nos campos SV-01 e TC-02, contempla os tipos AP-03, AT-05, CD-01, CD-04, IA-02, PD-03 e PD-05. As duas primeiras soluções foram desenvolvidas em PHP, enquanto o terceiro registro corresponde a uma implementação em C++. Esses softwares refletem a consolidação institucional do uso de RFID na UFJF, especialmente no controle de acesso de docentes às salas de aula e no gerenciamento da entrada de estudantes no Restaurante Universitário. No conjunto, essas classificações evidenciam que o SCA, o U2Pass Web e o U2Pass são softwares concebidos para garantir autenticação confiável, automação de processos de entrada e gestão segura do fluxo de usuários, reforçando a adoção da tecnologia RFID na UFJF para acesso a salas e ao Restaurante Universitário.

De forma semelhante, a Universidade Federal de Lavras (UFLA) adotou o uso do RFID para gerenciamento de acervo de sua biblioteca universitária. Segundo Oliveira et al. [10], a implementação do sistema resultou em melhorias significativas na eficiência dos processos de empréstimo, devolução e inventário, reduzindo o tempo de atendimento e otimizando a gestão do acervo.

Já para o uso da tecnologia NFC e QR Code, o sistema de controle de acesso desenvolvido por graduandos da Engenharia de Computação da Faculdade do Amazonas de Ensino Pesquisa e Inovação (FAMEPI) serviu como principal referência. Esse trabalho apresenta uma solução completa, abordando desde o levantamento de requisitos até a implementação prática das tecnologias em dispositivos físicos.

Outra referência relevante é o Sistema Hórus, desenvolvido pela Superintendência de Tecnologia da Informação (STI) da Universidade de São Paulo (USP), voltado para a identificação e o controle de acesso em ambientes institucionais. O Hórus permite a autenticação de usuários por meio de carteirinhas físicas ou digitais (e-Card via QR Code), integrando-se diretamente aos dispositivos de controle, como portões, catracas e cancelas. Além disso, o sistema realiza comunicação com as bases corporativas da universidade para gerenciar dados de discentes, docentes, visitantes e veículos, automatizando o processo de liberação de acesso e registro de entradas. Seu desenvolvimento interno, sem dependência de softwares externos, garante maior autonomia tecnológica, segurança e escalabilidade, demonstrando como soluções institucionais podem aliar gestão acadêmica e controle físico de acesso em uma única plataforma [11, 12]. Essa abordagem inspirou o presente projeto ao evidenciar a viabilidade da integração entre autenticação digital e controle de acesso físico em um contexto educacional.

No contexto da autenticação Wi-fi, o trabalho desenvolvido por Moreira [13], na Universidade Federal do Pará (UFPA), propôs a reestruturação do acesso à rede Wi-Fi destinada a visitantes por meio da implantação de um sistema de controle de acesso seguro baseado em portal cativo. A solução permite a autenticação centralizada de usuários, o registro de dispositivos conectados e a criação de políticas de acesso, garantindo que cada atividade realizada na rede possa ser associada a um usuário específico. O autor destaca que, antes da adoção dessa abordagem, a instituição não possuía mecanismos adequados de identificação, o que representava riscos legais à luz do Marco Civil da Internet (Lei n.º 12.965/2014)[14]. Dessa forma, o estudo demonstra a importância de mecanismos de autenticação, rastreabilidade e gestão de permissões em ambientes acadêmicos, reforçando a necessidade de soluções que assegurem tanto a segurança quanto a responsabilização no uso da rede.

De modo geral, observa-se que cada uma das soluções analisadas adota tecnologias distintas para atender necessidades específicas, mas todas compartilham o objetivo comum de aprimorar mecanismos de identificação e controle de acesso.

Portanto, a partir dessa revisão bibliográfica, o sistema proposto visa oferecer ao Centro Federal de Educação Tecnológica de Minas Gerais - Campus Leopoldina melhorias na organização, segurança e qualidade das atividades do laboratório de iniciação científica e extensão. O projeto integra diferentes tecnologias analisadas, como autenticação Wi-Fi por geração de vouchers, RFID, NFC e QR Code, de modo a aprimorar o controle de acesso, a rastreabilidade e o monitoramento da presença dos participantes. Além disso, busca-se centralizar e sincronizar automaticamente os dados de discentes e docentes vinculados a projetos, permitindo maior precisão e confiabilidade no gerenciamento de informações institucionais.

Entre seus principais objetivos estão a integração dos dados de discentes e docentes vinculados a projetos, a criação de carteirinhas físicas e digitais com múltiplos métodos de autenticação, e a

automatização do registro de presença e uso dos laboratórios. Por fim, ao concentrar dados, registros e informações de atividades em uma única plataforma, o sistema favorece a divulgação estruturada das ações de pesquisa e extensão, permitindo que os resultados e produções do LINCE sejam acessados de forma clara por usuários internos e externos. Com isso, a solução reforça o compromisso institucional com transparência, gestão eficiente e incentivo à participação acadêmica, contribuindo para a valorização e visibilidade das iniciativas desenvolvidas no laboratório.

4 Materiais e Métodos

A metodologia adotada para o desenvolvimento do produto seguiu o Método de Engenharia definido pela Febrace [15], adaptado por Soares[16], Aguiar[17] e Luz et al.[18] em 6 etapas. Iniciando pela ETAPA 1: Levantamento de referências e sistemas correlatos; ETAPA 2: Elicitação de requisitos e modelagem do software utilizando técnicas de Engenharia de Software e Banco de Dados; ETAPA 3: Desenvolvimento do produto de software; ETAPA 4: Planejamento e realização de testes para o software desenvolvido; ETAPA 5: Operar manutenções no software de acordo com os erros reportados na etapa de testes; ETAPA 6: Disponibilização online do software desenvolvido. A Figura 2 mostra a metodologia adotada.

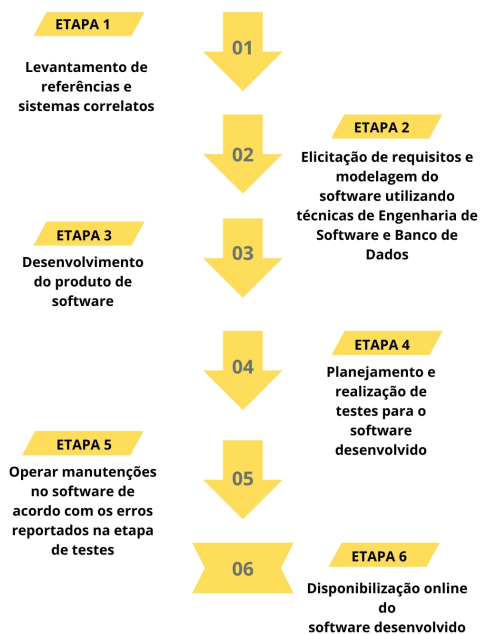


Figura 2: Etapas do Método de Engenharia adaptado[16][17].

A ETAPA 1 caracterizou-se pelo levantamento da literatura relacionada ao projeto e a pesquisa por sistemas correlatos existentes no mercado e no ambiente acadêmico. A ETAPA 2 iniciou-se com o mapeamento das necessidades do sistema. Nesta etapa foram estabelecidas as definições dos requisitos, modelando o Diagrama de Caso de Uso (DCU) e a criação do Diagrama de Entidade-Relacionamento (DER). Além disso, essa etapa contou com o redesign do layout do sistema existente e a especificação das novas interfaces para as

funcionalidades que serão incorporadas. O Adobe Color¹ foi utilizado para definir a paleta de cores e o Figma² para a prototipagem do sistema. Para o design da carteirinha utilizou-se da ferramenta Canva³.

Para a ETAPA 3, que consiste no desenvolvimento do produto de software, utilizou-se da biblioteca React JS⁴, uma biblioteca JavaScript que permite construir interfaces dinâmicas e responsivas por meio de componentes reutilizáveis e de um mecanismo eficiente de atualização da interface. Também utilizou-se o Node JS⁵ uma plataforma que permite a execução de JavaScript fora do navegador, que possibilita a construção de serviços web leves e escaláveis, responsáveis por executar a lógica de negócio, tratar requisições do cliente e interagir com o banco de dados de forma ágil e segura. A escolha dessas tecnologias deve-se à sua ampla adoção no mercado e na comunidade de desenvolvimento, à facilidade de integração entre o front-end e o back-end e à vasta disponibilidade de bibliotecas e documentação, fatores que favorecem o desenvolvimento ágil, seguro e consistente para aplicações web, conforme apontado por Swacha e Kulpa [19].

O banco de dados escolhido foi o MySQL⁶ devido à familiaridade da equipe e por ser amplamente reconhecido como um dos Sistemas Gerenciadores de Banco de Dados mais utilizados do mundo, principalmente para aplicações web[20][21][22]. A ETAPA 4 se caracteriza pela fase de testes, cujo o objetivo é garantir que todas as funcionalidades do software estejam funcionando perfeitamente. Finalizada a etapa de teste, na ETAPA 5 são feitas manutenções com o erros reportados na etapa anterior. Por fim, na ETAPA 6 ocorre a implantação e a disponibilização online do software.

5 Resultados

Esta seção detalha o progresso das fases de desenvolvimento do sistema abordando os principais resultados obtidos durante a fase de modelagem do software, já concluída. Além disso, é apresentado o status do desenvolvimento do produto de software indicando que o projeto avançou para a ETAPA 3.

5.1 Modelagem

A modelagem de sistemas e bancos de dados é de extrema importância para a construção de um produto de software com integridade, segurança e eficiência na manipulação dos dados[23]. A modelagem do Diagrama de Casos de Uso (DCU), Diagrama Entidade-Relacionamento (DER) e a prototipação das interfaces são abordados a seguir.

O Diagrama de Casos de Uso (DCU), é um diagrama proposto pela UML (Unified Modeling Language - Linguagem de Modelagem Unificada), que segundo Booch, Raubaug e Jacobson [24], é fundamental para visualização das interações entre os usuários e o sistema, sendo uma ferramenta-chave para compreender e comunicar os requisitos funcionais do sistema. Por meio do diagrama UML é possível detalhar todas as funcionalidade do sistema, de maneira

¹<https://color.adobe.com/pt/>

²<https://www.figma.com/>

³<https://www.canva.com/>

⁴<https://react.dev/>

⁵<https://nodejs.org/pt>

⁶<https://www.mysql.com/>

que seja compreensível para todos os envolvidos no projeto. Para criação do DCU utilizou-se o software Astah UML versão 10.1.0⁷.

É possível observar na Figura 3, as interações entre os atores e o sistema, através do DCU. Com base no diagrama, o sistema organiza suas funcionalidades em torno de três atores principais: Usuário, Administrador e Leitor. O Usuário pode autenticar-se na rede Wi-Fi, visualizar seus projetos e gerar vouchers, além de acessar funcionalidades adicionais por meio da associação a projetos. O Administrador possui um conjunto ampliado de operações, incluindo a manutenção de carteirinhas, processo que se estende para ações como bloquear carteirinhas, gerar PDF (Portable Document Format), vincular tecnologias RFID/NFC e gerar QR Codes. Também é responsabilidade do Administrador associar usuários ao sistema e gerenciar sua vinculação a projetos. Já o Leitor atua como agente de registro, permitindo identificar e registrar acessos e presenças no laboratório por meio das carteirinhas digitais.

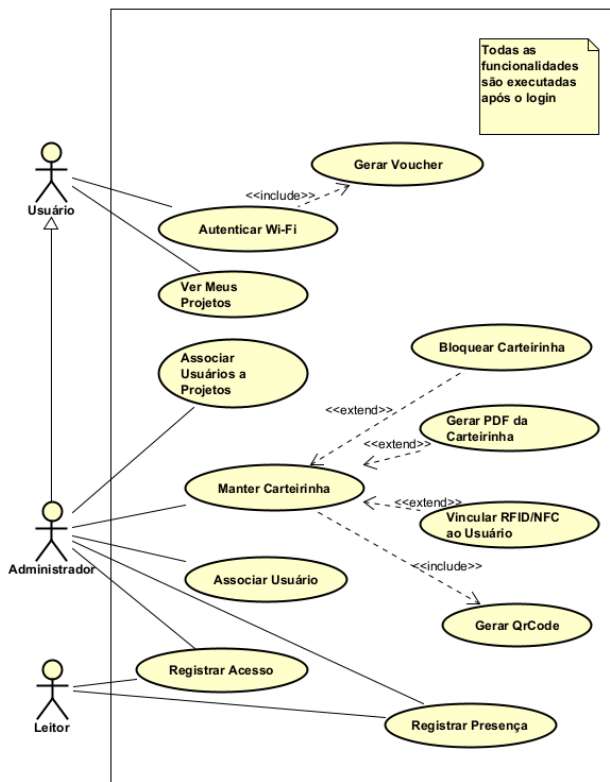


Figura 3: Diagrama de Casos de Uso (DCU) do sistema.

A seguir, tem-se o Diagrama de Entidade-Relacionamento (DER), cujo o modelo conceitual do banco de dados foi criado utilizando o BrModelo⁸. A estruturação do banco de dados permite o suporte eficiente de todas as operações do sistema, além de aderir a segurança e a privacidade dos dados. Segundo Elmasri e Navathe[25], a modelagem é uma fase crítica para que o banco de dados mantenha

⁷<https://astah.net/products/astah-uml/>
⁸<https://www.sis4.com/brModelo/index.html>

sua precisão e confiabilidade ao longo do tempo, evidenciando a relevância de um planejamento bem estruturado.

A Figura 4 ilustra a estrutura do DER, que inclui as entidades Usuário, Professor, Aluno, Projeto, EntAssoss, Carteirinha, Tecnologia, AutenticaWiFi e Presença, bem como seus respectivos relacionamentos, tais como solicita, atua, participa, emite, possui e valida. Além disso, cada entidade possui seus respectivos atributos. Destaca-se a entidade Tecnologia, cujos atributos permitem representar os diferentes métodos de identificação utilizados pelo sistema, como RFID, NFC e QR Code.

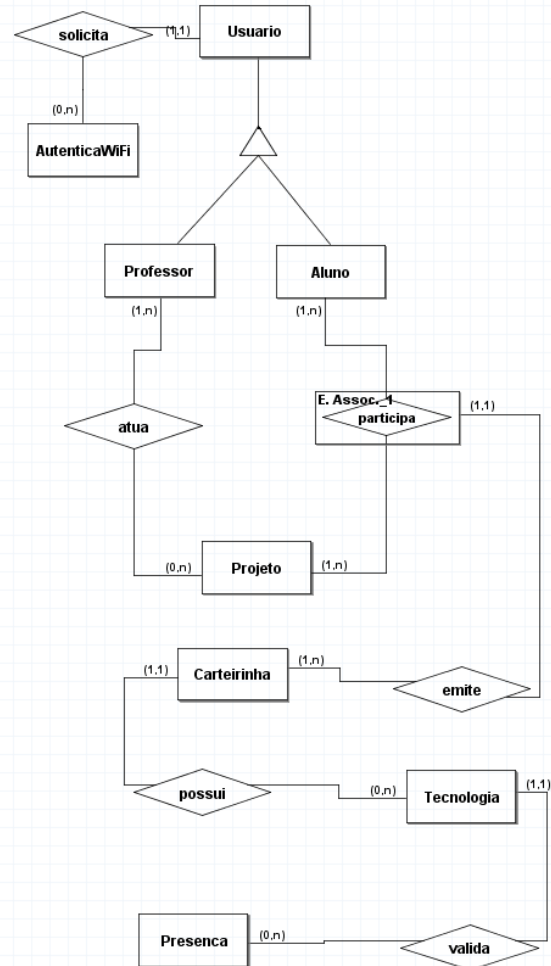


Figura 4: Diagrama de Entidade-Relacionamento (DER) do sistema.

Esses atributos organizam e distinguem as tecnologias empregadas para autenticação e validação de presença, possibilitando que o sistema suporte múltiplos mecanismos de leitura e identificação de forma estruturada. O DER destaca as interações essenciais, como a solicitação de autenticação Wi-Fi, a atuação de professores em projetos, a participação de alunos em atividades de pesquisa e extensão, a emissão e associação de carteirinhas aos usuários e a validação de presença.

Por, fim a prototipação das interfaces é importante no desenvolvimento de um produto de software. Segundo Theis[26], "a prototipação é fundamental no design de interfaces por favorecer a materialização das ideias, permitindo melhor compreensão e feedback dos envolvidos no projeto". Desse modo, para a prototipação das interfaces e o design da carteirinha, utilizou-se das ferramentas de design, Figma⁹ e o Canva¹⁰. Essas ferramentas permitem a simulação de interfaces de interação entre usuário e o sistema, o que é essencial para validar as funcionalidades antes de codificar.

5.2 Desenvolvimento do Produto de Software

Nessa perspectiva, a ferramenta foi desenvolvida seguindo a arquitetura cliente-servidor, um modelo amplamente empregado em aplicações web modernas pela sua capacidade de separar responsabilidades e facilitar a escalabilidade do sistema. Nessa abordagem, o cliente é responsável pela interação com o usuário e pelo envio das requisições. Nessa parte, utilizou-se o React JS. Já o servidor recebe as requisições e concentra toda a lógica de processamento dos dados, regras de negócio e acesso ao banco de dados, utilizando Node JS. Segundo Tanenbaum e Steen [27], a arquitetura cliente-servidor promove modularidade e permite que componentes sejam distribuídos entre máquinas distintas, aumentando a flexibilidade e o desempenho. De forma semelhante, Stallings [28] destaca que essa separação contribui para maior segurança, manutenção simplificada e possibilidade de reutilização dos serviços em múltiplas aplicações, características essenciais para sistemas web robustos e escaláveis.

As telas descritas a seguir ilustram como os conceitos e funcionalidades previamente discutidos foram materializados no ambiente visual da aplicação, evidenciando a organização das informações e a experiência oferecida aos usuários.

A Figura 5 mostra a tela inicial do sistema. Essa tela é visualizada por todos os usuários, logados e não logados. A partir dela, é possível visualizar indicadores dos projetos em andamento, discentes e docentes que participaram do LINCEe o público alcançado em eventos que ocorreram a apresentação desses projetos. Além disso, a página inicial apresenta uma interface organizada que facilita o acesso às principais funcionalidades, servindo como ponto de entrada para navegação no sistema. Essa disposição intuitiva contribui para uma melhor experiência do usuário, permitindo que informações essenciais sejam rapidamente compreendidas logo no primeiro contato com a aplicação.

Ao clicar em Login, o usuário é direcionado para a tela de autenticação, onde deve informar um e-mail válido e uma senha. Vale destacar que o cadastro de usuários é realizado internamente pelos administradores do sistema. Após a validação das credenciais, o usuário é redirecionado para a interface principal, onde poderá acessar e utilizar as funcionalidades disponíveis no sistema. Como ilustrado na Figura 6, pode-se observar que alguns dos botões exibem um ícone de cadeado, indicando que o usuário não possui acesso àquela funcionalidade. As permissões de acesso são definidas no momento do cadastro, quando é selecionado o cargo do usuário. No exemplo apresentado, trata-se de um usuário que não possui cargo de administrador. Caso seja um administrador, todas as funcionalidades estarão desbloqueadas. Essa restrição garante maior segurança

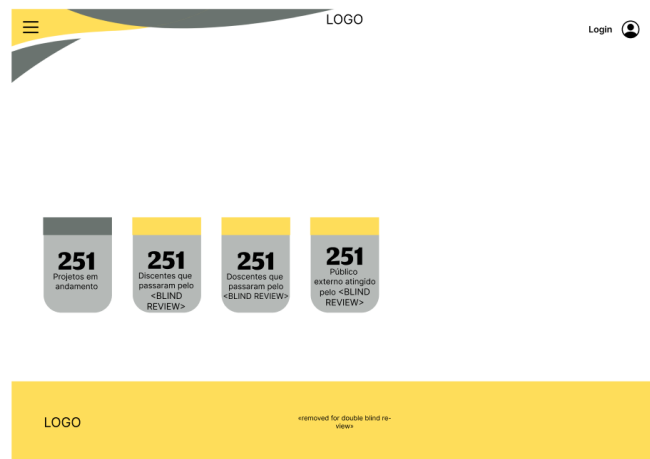


Figura 5: Tela inicial.

e integridade nas operações realizadas no sistema. Dessa forma, cada usuário tem acesso apenas às ferramentas necessárias para desempenhar suas atividades.

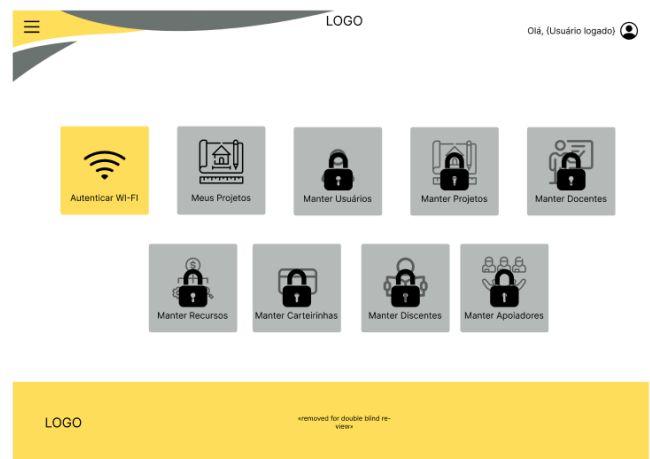


Figura 6: Tela Home com funcionalidades do sistema.

Por meio dessa página é possível acessar funcionalidades como, Autenticar Wi-Fi e Meus Projetos, que são permitidas para todos os tipos de usuários e Manter Usuários, Projetos, Discentes, Docentes, Recursos, Carteirinhas e Apoiadores, liberadas somente para administradores.

Nesse contexto, ao ter o cargo de administrador e clicar em Manter Carteirinha é possível visualizar todos os pesquisadores e extensionistas que estão vinculados a um projeto, conforme ilustra a Figura 7.

Nesta tela, o administrador encontra funcionalidades como selecionar todas as carteirinhas ou apenas uma delas, gerar um arquivo PDF a partir da seleção dos usuários, visualizar cada carteirinha individualmente e ordenar a lista em ordem alfabética de acordo com o nome dos alunos. Um ponto importante dessa tela é que a criação de carteirinhas só é permitida para usuários que estejam

⁹<https://www.figma.com/>

¹⁰<https://www.canva.com/>

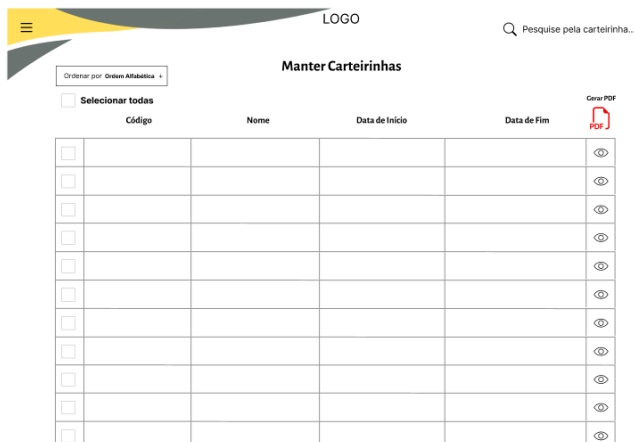


Figura 7: Tela Manter Carteirinhas.

vinculados a um projeto em andamento. Essa restrição evita a duplicação de carteirinhas caso o mesmo usuário participe de mais de um projeto em momentos distintos.

Portanto, com a construção desses dados dos discentes vinculados aos projetos e tutores, é possível solucionar um dos problemas identificados. A necessidade de emitir carteirinhas para acesso a chave do LINCE, que minimiza o acesso de usuários indevidos e a desatualização das listas de autorização. Com isso, como citado no parágrafo acima, é possível gerar um arquivo PDF para impressão das carteirinhas e disponibilização aos pesquisadores e extensionistas. Na Figura 8 é possível visualizar o protótipo da carteirinha emitida pelo sistema.



Figura 8: Carteirinha emitida pelo sistema.

Todos os dados encontrados na carteirinha são obtidos através do servidor que tem acesso ao banco de dados, onde fica toda a base de dados do sistema. Como mostrado na Figura 8, o campo destinado à fotografia é fundamental para a identificação do usuário na portaria. Entretanto, caso não sido colocado uma foto durante o cadastro, o sistema utiliza, por padrão, a logo oficial do laboratório.

Até o momento, o projeto se encontra na fase do desenvolvimento de produto de software, onde estão sendo estudadas e codificadas soluções para garantir tanto a operação das funcionalidades principais quanto a integração entre as tecnologias utilizadas e a comunicação eficiente com o banco de dados. Nessa fase, os ajustes contínuos na interface e na arquitetura são extremamente importantes, visando aprimorar a usabilidade e a robustez da aplicação assegurando que o sistema ofereça uma experiência coerente e alinhada às necessidades institucionais.

6 Considerações Finais

Devido ao aumento do desenvolvimento das ações de pesquisa e extensão no ambiente acadêmico, o sistema inteligente integrado ao Laboratório de Iniciação Científica e Extensão da Computação (LINCE) apresenta-se como uma solução essencial para aprimorar os processos administrativos e operacionais. A análise das práticas atuais evidenciou fragilidades significativas relacionadas ao controle de acesso físico, à gestão de usuários e ao monitoramento da infraestrutura de rede Wi-Fi. Tais limitações comprometem a segurança, a organização e a rastreabilidade das atividades realizadas no laboratório, especialmente diante do crescimento constante dos projetos e do número de participantes vinculados ao LINCE.

A implementação de carteirinhas digitais com uso das tecnologias RFID, NFC e QR Code, associada ao gerenciamento automatizado de acesso, representa um avanço relevante na modernização da infraestrutura do laboratório. Essa abordagem permite maior precisão na identificação dos usuários, agilidade no fluxo de entrada e saída e maior garantia de que os ambientes estejam sendo utilizados exclusivamente por pessoas autorizadas. Paralelamente, a implementação de vouchers temporários para autenticação Wi-Fi contribui diretamente para a segurança digital, ao possibilitar a rastreabilidade dos dispositivos conectados e ao restringir o uso da rede aos pesquisadores e extensionistas devidamente cadastrados. Essas funcionalidades, em conjunto, promovem um ambiente mais protegido e alinhado às boas práticas de gestão acadêmica.

Além disso, a reformulação geral da interface do sistema tem potencial para aprimorar significativamente a experiência de navegação dos usuários, tornando os processos mais intuitivos e acessíveis. Uma interface mais clara e responsiva favorece o uso cotidiano do sistema, reduz a ocorrência de erros operacionais e amplia o engajamento dos participantes com as ferramentas disponibilizadas. Assim, o conjunto de melhorias propostas busca atender às necessidades atuais do laboratório, ao mesmo tempo em que prepara sua infraestrutura para suportar futuras expansões de forma mais organizada e eficiente.

Já foram concluídas as etapas - ETAPA 1: Levantamento de referências e sistemas correlatos e a ETAPA 2: Elicitação de requisitos e modelagem do software utilizando técnicas de Engenharia de Software e Banco de Dados. No momento, o projeto se encontra na ETAPA 3: Desenvolvimento do Produto de Software. Após a finalização dessa etapa, será dado prosseguimento às etapas posteriores de forma sistemática e sequencial, incluindo a etapa de testes, que será realizada em ambiente real de uso, com o objetivo de realizar uma avaliação empírica do funcionamento e da aplicabilidade do sistema.

Assim, ao final de todo o processo de desenvolvimento, espera-se entregar ao Laboratório de Iniciação Científica e Extensão da Computação (LINCE) um sistema completo, capaz de apoiar o controle de acesso físico e digital, otimizar a gestão de projetos e usuários e fortalecer a segurança e a organização das atividades realizadas no laboratório. Com isso, o ambiente torna-se mais eficiente, confiável e alinhado às demandas contemporâneas de pesquisa e extensão, contribuindo diretamente para a consolidação de um ecossistema acadêmico mais moderno e integrado.

Agradecimentos

Nossos agradecimentos ao Centro Federal de Educação Tecnológica de Minas Gerais - Campus Leopoldina, à Diretoria de Graduação do CEFET-MG e ao Laboratório de Iniciação Científica e Extensão da Computação (LINCE) pelo apoio e disponibilização de sua infraestrutura para a realização deste trabalho.

Referências

- [1] Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Programas institucionais de iniciação científica e tecnológica, 2025. URL <https://www.gov.br/cnpq/pt-br/aceso-a-informacao/acoes-e-programas/programas/programas-ict>. Acesso em: 18 Out.2025.
- [2] Luis Augusto Mattos Mendes Daniel Mescolin Damasceno Crespo, Juan Helpes Albano and Gustavo Montes Novaes. Sistema para gestão de projetos de um laboratório de pesquisa e extensão. *Congresso Brasileiro de Ensino de Engenharia (COBENGE)*, 2024. doi: 10.37702/2175-957X.COBENGE.2023.4457. Acesso em: 18 Out.2025.
- [3] Shahriar Md Arman, Tao Yang, Shahadat Shahed, Alanoud Al Mazroa, Afraa Attiah, and Linda Mohaisen. A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. *Computers, Materials & Continua*, 78(2):2087–2110, 2024. doi: 10.32604/cmc.2024.047870.
- [4] Guilherme Dantas Couto and Tarsius Sergio Malafaia. Rfid – radio frequency identification. Trabalho da disciplina Redes de Computadores 1 – 2019.1, Departamento de Engenharia Eletrônica e de Computação, Universidade Federal do Rio de Janeiro (UFRJ), 2019. URL <https://www.gta.ufrj.br/ensino/eel878/redes1-2019-1/vf/rfid/>. Acesso em: 7 nov. 2025.
- [5] Daniel Santos Silva, Guilherme Cruz de Aquino, João Vitor Silva Lima Fernandes, Luiz Miguel de Souza Bastos, and Pedro Lucas Soares da Silva. Sistema para controle de acesso à universidade utilizando nfc e qr code. *Brazilian Journal of Development*, 8(5):34560–34566, may 2022. doi: 10.34117/bjdv8n5-125. URL <https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/download/47614/pdf/119111>.
- [6] União Brasileira dos Estudantes Secundaristas (UBES). Carteirinha da ubes. Online, 2025. URL <https://www.ubes.org.br/2025/carteirinhaaãSdaããSubes/>. Acessado em: 21Out.2025.
- [7] Eduardo Julio and T. Machado. Sistema de controle de acesso - sca. In *Proceedings of Computer on the Beach (Computer on the Beach 2026)*. INPI / UFJF, 2024. Patente: Programa de Computador. Registro INPI n. 512024003886-8; data de registro: 17/10/2024. Campo de Aplicação: SV-01. Tipos de Programa: CD-04, IA-02, PD-03, PD-05. Implementação: PHP.
- [8] Eduardo Julio, A. G. B. Almeida, T. Machado, T. M. F. Mello, and G. P. Leonel. U2pass web. In *Proceedings of Computer on the Beach (Computer on the Beach 2026)*. INPI / UFJF, 2024. Patente: Programa de Computador. Registro INPI n. 512024003891-4; data de registro: 17/10/2024. Campo de Aplicação: SV-01. Tipos de Programa: AP-03, AV-02, CD-04, GI-04, PD-01, PD-03, PD-05, SO-05. Implementação: PHP.
- [9] Eduardo Pagani Julio and A. G. B. Almeida. U2pass. In *Proceedings of Computer on the Beach (Computer on the Beach 2026)*. INPI / UFJF, 2024. Patente: Programa de Computador. Registro INPI n. 512024003888-4; data de registro: 17/10/2024. Campo de Aplicação: SV-01 / TC-02. Tipos de Programa: AP-03, AT-05, CD-01, CD-04, IA-02, PD-03, PD-05. Implementação: C++.
- [10] Nivaldo Oliveira, Rosiane Maria Oliveira, and Fernanda Vasconcelos Amaral. Gerenciamento de acervo através da tecnologia rfid: a experiência da biblioteca universitária da ufla. In *XVIII Seminário Nacional de Bibliotecas Universitárias (SNBU)*, 2014, pages 11–13, 2014. URL <https://www.bu.ufmg.br/snbu2014/wp-content/uploads/trabalhos/259-2256.pdf>. Acesso em: 27 Out.2025.
- [11] Jornal da USP. Sistema desenvolvido pela usp possibilita identificação e controle de acesso, 2024. URL <https://jornal.usp.br/institucional/sistema-desenvolvido-pela-usp-possibilita-identificacao-e-controle-de-aceso/>. Acesso em: 12 nov. 2025.
- [12] CETILQ STI USP. Sistema hórus: controle de acesso e autenticação, 2024. URL <https://cetilq.sti.usp.br/competencias/horus/>. Acesso em: 12 nov. 2025.
- [13] Ruan Pablo Rodrigues Moreira. Reestruturação do modelo de autenticação de usuários da rede sem fio de visitantes da ufpa, 2017. URL <https://bdm.ufpa.br/server/api/core/bitstreams/c0633ee9-5e2b-4492-9fba-ac96083affee/content>. Acesso em: 14 Nov. 2025.
- [14] Brasil. Lei n.º 12.965, de 23 de abril de 2014 (marco civil da internet), 2014. URL https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Disponível em: <https://www.planalto.gov.br/...> Acesso em: 16 nov. 2025.
- [15] Requisitos. Website da FEBRACE: <https://febrace.org.br/participe/planeje-seu-projeto/requisitos/>, 2021. Acesso em: 4 Nov.2025.
- [16] Gabriella Castro Barbosa Costa Dalpra Luis Augusto Mattos Mendes Guilherme Martins Soares, João Victor Domingos e Souza and Luan Soares Oliveira. Sistema para verificação da não conformidade de produtos de software com a lei geral de proteção de dados pessoais (lgpd). In *Anais do XVI Computer on the Beach*, pages 478–482, Itajaí, SC, Brasil, 2025.
- [17] Inácio Matias Leonardo Lopes Luis Augusto Mattos Mendes Bernardo Gomes de Aguiar, Eduardo Lima S. M. de Rezende and Alexandre Martins Gama de Deus. Vintana: uma plataforma para publicação de acervos de rádios. 2024. Fonte: Artigo 06-PPaegle.pdf, página 690.
- [18] Luis Augusto Mattos Mendes Lorenzo Jordani Bertozzi Luz, Lukas Julius Wolf Sicad: Sistema de certificação acadêmica digital. In *Anais do XXXVI Simpósio Brasileiro de Informática na Educação (SBIE 2025)*, XIV Congresso Brasileiro de Informática na Educação (CBIE 2025), pages 1540–1549, 2025. doi: 10.5753/sbie.2025.12410.
- [19] Jakub Swacha and Artur Kulpa. Evolution of popularity and multispectral comparison of widely used web development frameworks. *Electronics*, 12(17): 3563, 2023. doi: 10.3390/electronics12173563. URL <https://www.mdpi.com/2079-9292/12/17/3563>. Acesso em: 12 Nov. 2025.
- [20] Marcello Toledo da Silva and David Luiz de Souza Cavalcanti. Sistemas gerenciais de banco de dados: Um estudo do mysql. *REVELA*, (23):366–382, nov 2018. ISSN 1982-646X. Disponível em: https://fals.com.br/novofals/revela/ed23/ed_23_25.pdf. Acesso em: 12 Nov. 2025.
- [21] Insper. Os bancos de dados mais populares em maio de 2024, 2024. URL <https://www.insper.edu.br/pt/noticias/2024/5/os-bancos-de-dados-mais-populares-em-maio-de-2024>. Acesso em: 16 nov. 2025.
- [22] DB-Engines. Db-engines ranking, 2025. URL <https://db-engines.com/en/ranking>. Acesso em: 16 nov. 2025.
- [23] David Stemple, Eric Simon, Subhasish Mazumdar, and Matthias Jarke. Garantindo a integridade do banco de dados. *Jornal de Gerenciamento de Banco de Dados*, 1:12–27, 1990. doi: 10.4018/JDM.1990070102. URL <https://doi.org/10.4018/JDM.1990070102>. Acesso em: 05 Nov. 2024.
- [24] Grady Booch, James Rumbaugh, and Ivar Jacobson. *The Unified Modeling Language User Guide*. Addison-Wesley Professional, Boston, MA, 2nd edition, 2005.
- [25] Ramez Elmasri and Shamkant B. Navathe. *Sistemas de banco de dados*. Pearson, SãoPaulo, 7ª edition, 2019. ISBN 978-85-430-2500-1. Acesso em: 20 Out.2025.
- [26] Mara Rubia Theis, George André de Souza, Francisco Antônio Pereira Fialho, and Ricardo Pereira. A importância da prototipagem no processo de design e suas relações como mídia do conhecimento. In *Anais do Congresso (Maringá, Brasil)*, pages 1–15, 2021.
- [27] Andrew S. Tanenbaum and Maarten Van Steen. *Distributed Systems: Principles and Paradigms*. Prentice Hall, 2nd edition, 2007.
- [28] William Stallings. *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley Professional, 2018.