INSTITUTO FEDERAL DE ALAGOAS
CAMPUS ARAPIRACA
CURSO SUPERIOR DE SISTEMAS DE INFORMAÇÃO

EDUARDO CARLOS BARBOZA NETO

UMA PROPOSTA DE SOLUÇÃO PARA GESTÃO DE TCCs NO IFAL: UM MECANISMO ANTIFRAUDE BASEADO EM BLOCKCHAIN

ARAPIRACA, AL.
2026

EDUARDO CARLOS BARBOZA NETO

UMA PROPOSTA DE SOLUÇÃO PARA GESTÃO DE TCCs NO IFAL: UM MECANISMO ANTIFRAUDE BASEADO EM BLOCKCHAIN

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Sistemas de Informação do Instituto Federal de Alagoas, campus Arapiraca, como requisito parcial para obtenção de grau de Bacharel em Sistemas de Informação.

Orientador(a): Prof. Me. Anderson Felinto Barbosa

ARAPIRACA, AL.
2026

Dados Internacionais de Catalogação na Publicação
Instituto Federal de Alagoas
***Campus* Arapiraca**

005.436
B239p Barboza Neto, Eduardo Carlos.

Uma proposta de solução para gestão de TCCs no IFAL: um mecanismo antifraude baseado em Blockchain / Eduardo Carlos Barboza Neto – Dados eletrônicos (1 arquivo : 6,6 MB). – 2026.

Sistema requerido: Adobe Acrobat Reader.
Modo de acesso: Internet.
Orientação: Prof. Me. Anderson Felinto Barbosa.

Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal de Alagoas, *Campus* Arapiraca, Arapiraca, 2026.

1. Blockchain permissionada. 2. Hyperledger fabric. 3. Armazenamento distribuído. 4. Integridade documental. 5. Informática na educação. I. Título.

Luciete Barbosa da Silva | Bibliotecária – CRB-4/1739

EDUARDO CARLOS BARBOZA NETO

UMA PROPOSTA DE SOLUÇÃO PARA GESTÃO DE TCCS NO IFAL: UM MECANISMO ANTIFRAUDE BASEADO EM BLOCKCHAIN

Monografia apresentada ao curso de Sistemas de Informação do Instituto Federal de Educação, Ciência e Tecnologia de Alagoas, campus Arapiraca, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

Trabalho aprovado. Alagoas, 06 de fevereiro de 2026

Me. ANDERSON FELINTO BARBOSA
Instituto Federal de Alagoas - Campus Arapiraca

Dr. TARSIS MARINHO DE SOUZA
Instituto Federal de Alagoas - Campus Arapiraca

Drª. CLEDJA KARINA ROLIM DA SILVA
Instituto Federal de Alagoas - Campus Arapiraca

ALAGOAS
2026

AGRADECIMENTOS

Primeiramente, quero agradecer a Deus por ter sido tão generoso comigo, ter me proporcionado essa oportunidade de cursar esta graduação e ter me dado forças para alcançar mais uma etapa importante na minha vida.

Agradeço ao Instituto Federal de Alagoas, que me acolheu e proporcionou um ambiente de crescimento e amadurecimento ao longo da minha trajetória. Durante os oito anos percorridos, desde o ensino médio até a graduação, a instituição se tornou, para mim, mais do que um espaço de formação, ela se tornou uma segunda casa.

Agradeço também aos meus professores, que foram peças fundamentais para minha formação acadêmica e profissional. Eles me proporcionaram ensinamentos importantes, cada um contribuindo de maneira significativa.

Em especial, dedico estes agradecimentos aos meus orientadores. Ao professor Anderson Felinto, que, com paciência, dedicação e orientação, me conduziu neste trabalho da melhor forma que eu poderia imaginar. Mesmo cansado, esteve me auxiliando não apenas no Trabalho de Conclusão de Curso, mas em todo o panorama do meu currículo acadêmico. Agradeço também ao professor Matheus Torquato, cuja contribuição foi essencial para que este trabalho ganhasse forma, por meio dos debates e discussões, possibilitando a aplicação da tecnologia blockchain no contexto acadêmico. Ele me mostrou que sempre há novos horizontes para seguir e que as coisas são menos complicadas do que parecem.

Dedico também estas palavras ao professor Tarsis Marinho e à professora Cledja Rolim, cuja importância ao longo dessa jornada acadêmica profissional é imensurável. Em meios de cobranças, puxões de orelha e incentivos, me acompanharam desde o período do ensino médio até a conclusão desta graduação, marcando para sempre minha vida.

Agradeço aos meus colegas de graduação, Victor, Guilherme e Samila, que tornaram essa jornada mais leve e significativa. Com eles, compartilhei muitas emoções durante a graduação, desde desafios acadêmicos, que ficarão marcados em mim, até as conquistas e experiências construídas. Sem dúvida, essa caminhada não seria a mesma sem eles. Levarei comigo a saudade e as risadas inacabáveis em memória.

Por último, e não menos importante, agradeço à minha família, que sempre esteve ao meu lado, oferecendo apoio, incentivo e compreensão em todos os momentos. Minha família foi minha base e não há dúvidas de que sem eles nada disso seria possível.

RESUMO

A Segurança da Informação é um aspecto essencial para a confiabilidade de sistemas que lidam com dados, tendo como pilares a integridade, a autenticidade e a disponibilidade das informações. No contexto das instituições de ensino, esses princípios tornam-se ainda mais relevantes, uma vez que documentos acadêmicos, possuem valor institucional, acadêmico e jurídico. A ausência de mecanismos padronizados para o gerenciamento e a verificação desses documentos pode torná-los vulneráveis a perdas, adulterações e fraudes. Diante desse cenário, este trabalho propõe o desenvolvimento de um sistema para a gestão do processo de defesa de TCC para o Instituto Federal de Alagoas (IFAL), utilizando a tecnologia blockchain como mecanismo antifraude, baseado em blockchain permissionada com o Hyperledger Fabric, integrada a um sistema de armazenamento distribuído (IPFS), no qual os documentos acadêmicos são armazenados de forma segura, enquanto apenas seus identificadores e provas de integridade são registrados na blockchain. O sistema contempla funcionalidades como agendamento de defesas, submissão e versionamento de documentos, fluxo de aprovação entre alunos, orientadores e coordenação, além da verificação de autenticidade documental. Para validação da proposta, foi desenvolvido um protótipo funcional com interface web e API integrada à rede blockchain, permitindo simular sua aplicação no contexto acadêmico. Os resultados obtidos demonstram que a solução contribui para o aumento da confiabilidade, rastreabilidade e transparência dos registros acadêmicos.

Palavras-chave: *Blockchain* Permissionada. *Hyperledger Fabric*. Armazenamento Distribuído. Integridade Documental. Informática na Educação.

ABSTRACT

Information security is an essential aspect for the reliability of systems that handle data, with integrity, authenticity, and availability of information as its pillars. In the context of educational institutions, these principles become even more relevant, since academic documents have institutional, academic, and legal value. The absence of standardized mechanisms for managing and verifying these documents can make them vulnerable to loss, alteration, and fraud. Given this scenario, this work proposes the development of a system for managing the thesis defense process for the Federal Institute of Alagoas (IFAL), using blockchain technology as an anti-fraud mechanism, based on permissioned blockchain with Hyperledger Fabric, integrated with a distributed storage system (IPFS), in which academic documents are securely stored, while only their identifiers and integrity proofs are recorded on the blockchain. The system includes functionalities such as scheduling defenses, document submission and versioning, approval workflow between students, advisors, and coordinators, as well as document authenticity verification. To validate the proposal, a functional prototype was developed with a web interface and API integrated into the blockchain network, allowing for the simulation of its application in an academic context. The results obtained demonstrate that the solution contributes to increasing the reliability, traceability, and transparency of academic records.

Keywords: Permissioned Blockchain. Hyperledger Fabric. Distributed Storage. Document Integrity. Informatics in Education

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
CA	Certificate Authority
CID	Content Identifier
CSS	Cascading Style Sheets
E2E	End-to-End
gRPC	gRPC Remote Procedure Calls
HTTPS	Hypertext Transfer Protocol Secure
IFAL	Instituto Federal de Alagoas
IPFS	InterPlanetary File System
JWT	JSON Web Token
mTLS	Mutual Transport Layer Security
MSP	Membership Service Provider
P2P	Peer-to-Peer (Ponto a Ponto)
PBFT	Practical Byzantine Fault Tolerance
PDF	Portable Document Format
PKI	Public Key Infrastructure (Infraestrutura de Chaves Públicas)
PoS	Proof of Stake
PoW	Proof of Work
RAFT	Raft Consensus Algorithm
RBAC	Role-Based Access Control
SMTP	Simple Mail Transfer Protocol
TCC	Trabalho de Conclusão de Curso

SUMÁRIO

1 INTRODUÇÃO

A credibilidade das instituições acadêmicas é dependente da confiabilidade de seus registros institucionais. Quando registros acadêmicos são falsificados ou adulterados, essa confiança se fragiliza e gera impactos que ultrapassam o ambiente institucional (VANDERLEY NETO, 2021).

A inexistência de mecanismos de verificação, rastreabilidade e auditoria dos ciclos de vida dos documentos institucionais amplia a exposição a riscos e dificulta a identificação de inconsistências, contribuindo de forma negativa, como nos casos das chamadas *degree mills*[1]. Esse cenário torna ainda mais sensíveis os efeitos da circulação de credenciais inautênticas, que podem comprometer a validade de comprovações acadêmicas e produzir consequências profissionais relevantes perante terceiros (RUSTEMI et al., 2023).

A gestão de documentos, comumente tratada como processos administrativos, representa um ponto de destaque para a confiabilidade institucional, podendo ser realizada de forma física ou virtual, mas que, independentemente do contexto, exige a definição de políticas e procedimentos institucionais para assegurar a qualidade do processo (PESSANHA; SALES; PIMENTA, 2025).

A literatura reconhece que a transição entre os suportes físico e digital representa uma fase crítica para a integridade documental. Em Carmo (2023), o termo "digitalização selvagem" é utilizado para descrever processos sem padrões definidos, sem controle adequado de qualidade e de armazenamento, o que maximiza os riscos de perda de autenticidade e confiabilidade dos registros digitalizados, ressaltando, assim, a necessidade das políticas e procedimentos organizacionais para assegurar os pilares da Segurança da Informação.

Nesse cenário, a tecnologia *blockchain* surge como uma alternativa para ampliar a transparência, reduzir a dependência de um ponto único de falha e fortalecer a integridade das informações por meio de registros imutáveis e verificáveis. Sua arquitetura descentralizada, aliada ao uso de *hashes* criptográficos e mecanismos de consenso distribuído, confere à *blockchain* um papel relevante no enfrentamento da fraude documental (ALMEIDA, Murilo; OLIVEIRA, Flávio; 2022), sendo aplicada no contexto acadêmico. Esse potencial já se reflete em propostas, por exemplo, na plataforma voltada à verificação de diplomas acadêmicos (Mili, 2021), um modelo de registro distribuído de conquistas e credenciais educacionais baseado em blockchain privada, conforme proposto por Sharples e Domingue (2016), e na

[1] Organizações que comercializam diplomas falsos.

abordagem de consenso distribuído para a validação de registros universitários (Medeiros, 2019).

1.1 OBJETIVOS

Este trabalho tem como objetivo desenvolver um protótipo de solução tecnológica para a gestão dos processos de defesa de TCC dos cursos de graduação do Instituto Federal de Alagoas, fundamentado em uma arquitetura antifraude baseada em *blockchain.*

Para atingir o objetivo, foram definidos os seguintes objetivos específicos:

I. Analisar o processo de defesa de Trabalhos de Conclusão de Curso (TCC) em conformidade com a Portaria nº 1483/GR;
II. Definir uma arquitetura conceitual de sistema baseada em blockchain permissionada para apoiar a gestão do processo de defesa de TCC;
III. Propor mecanismos para o registro, assinatura consensual, consulta e verificação de documentos acadêmicos;
IV. Implementar um sistema de armazenamento descentralizado e seguro dos documentos acadêmicos;
V. Desenvolver protótipo de solução para o gerenciamento das defesas de TCC;
VI. Validar o protótipo desenvolvido quanto ao atendimento aos requisitos.

1.2 JUSTIFICATIVA E CONTRIBUIÇÕES DO TRABALHO

No Instituto Federal de Educação, Ciência e Tecnologia de Alagoas (IFAL), a Portaria nº 1483/GR, de 19 de setembro de 2012, orienta o processo de elaboração, apresentação e avaliação dos Trabalhos de Conclusão de Curso (TCC) dos cursos de graduação, destacando obrigações e documentos acadêmicos-administrativos que devem ser criados durante o desenvolvimento do trabalho, porém, não há orientações quanto aos procedimentos organizacionais para o gerenciamento dos documentos exigidos. Tal ausência representa um risco à segurança da informação contida nos documentos, destacando a necessidade de implementação de soluções que mitiguem esse risco.

Diante disso, a contribuição deste trabalho está no desenvolvimento de um protótipo de solução para gestão dos processos de defesa de TCC dos cursos superiores do IFAL, bem como dos documentos “Ata de Defesa” e “Ficha de Avaliação”, fundamentada no

uso da *blockchain* permissionada *Hyperledger Fabric*[2], solucionando a lacuna existente quanto aos procedimentos para a gestão de documentos referentes à defesa de TCC. O uso da *blockchain* permitirá, a partir da definição de contratos inteligentes, automatizar validações e registros dos documentos por diferentes setores institucionais, alinhando a infraestrutura tecnológica à governança organizacional (HYPERLEDGER FABRIC, 2025).

Uma segunda contribuição do trabalho pode ser verificada na viabilidade da adoção da *blockchain* de código aberto *Hyperledger Fabric* em instituições públicas, dadas as restrições orçamentárias e exigências de transparência tecnológica. Além disso, espera-se contribuir com a segurança jurídica e a integridade das informações acadêmicas ao fortalecer a auditabilidade, a transparência e a resistência à adulteração de documentos e informações, por meio dos registros das evidências de validação e metadados verificáveis, e ao aplicar regras de aprovação multiatores.

1.3 ESTRUTURA DO DOCUMENTO

Este trabalho está organizado em seis capítulos, além de apêndices e anexos, estruturados de forma a conduzir o leitor desde a contextualização do problema até a apresentação da solução desenvolvida e de seus resultados.

Inicialmente, o Capítulo 1 apresenta a contextualização do problema, os objetivos do trabalho, a justificativa da pesquisa e suas principais contribuições.

Em seguida, o Capítulo 2 desenvolve a fundamentação teórica, abordando conceitos de Segurança da Informação, blockchain, criptografia, armazenamento distribuído (IPFS) e o f*ramework Hyperledger Fabric*, que servem de base para a solução proposta.

A partir desse embasamento, o Capítulo 3 descreve a solução proposta, contemplando a visão geral do sistema, seus subsistemas, o projeto de software, bem como as arquiteturas lógica e física e as tecnologias utilizadas na implementação do protótipo.

Na sequência, o Capítulo 4 apresenta os resultados obtidos com a implementação do sistema, destacando as principais funcionalidades por meio das interfaces desenvolvidas, dos fluxos de uso, de exemplos práticos de aplicação no contexto da gestão de defesas de TCC e dos testes de validação realizados para verificar o correto funcionamento da aplicação e a integridade das informações.

Posteriormente, o Capítulo 5 reúne as conclusões do trabalho, analisando os objetivos alcançados, as contribuições da solução desenvolvida, as limitações identificadas e as possibilidades de trabalhos futuros.

[2] Disponível em: https://github.com/hyperledger/fabric

Por fim, o Capítulo 6 apresenta as referências bibliográficas utilizadas no desenvolvimento do trabalho. De forma complementar, os Apêndices reúnem materiais adicionais, como a especificação dos requisitos da solução, o diagrama de entidade e relacionamento do banco de dados e a documentação dos endpoints da API.

Os anexos apresentam documentos institucionais relacionados ao processo de defesa de TCC, conforme a regulamentação vigente.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta as principais bases teóricas para a compreensão do problema e das tecnologias envolvidas no desenvolvimento do trabalho. São apresentados temas relacionados à integridade e autenticidade documental, *blockchain*, armazenamento distribuído e criptografia, além de algumas aplicações da tecnologia blockchain em contextos acadêmicos.

2.1 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação constitui um dos pilares para a confiabilidade e a continuidade dos sistemas informacionais nas organizações. Seu propósito vai além da proteção puramente técnica, abrangendo a definição e aplicação de políticas, normas e processos voltados à mitigação de riscos associados ao uso e à gestão da informação. Nesse sentido, busca proteger os ativos informacionais contra ameaças internas e externas (MACHADO, 2013).

Os três pilares fundamentais da Segurança da Informação, denominados Confidencialidade, Integridade e Disponibilidade, são amplamente reconhecidos como a base de qualquer política de segurança eficaz. A confidencialidade visa garantir que as informações sejam acessadas apenas por pessoas autorizadas, protegendo contra vazamentos, espionagem e acessos indevidos; A integridade tem como objetivo assegurar que a informação não seja modificada de forma não autorizada, preservando sua veracidade e completude ao longo de todo o seu ciclo de vida; e a disponibilidade garante que a informação esteja acessível e utilizável sempre que necessário, especialmente em sistemas considerados críticos.

Além desses pilares clássicos, outros atributos relevantes para a Segurança da Informação devem ser considerados nos Sistemas de Informação, tais como: a autenticidade que assegura que a informação seja genuína e que sua origem possa ser verificada; a legalidade que visa garantir que os dados sejam tratados conforme a legislação vigente, e a irretratabilidade (ou não-repúdio) que impossibilita que um autor negue a autoria de determinada ação ou transação digital. Contudo, a literatura da área também destaca que o tema não deve ser abordado apenas sob a perspectiva da tecnologia, também devem ser incorporados aspectos relacionados ao comportamento humano, sendo esse considerado o elemento central (SÊMOLA, 2014).

Para Machado (2013), os riscos relacionados à Segurança da Informação não se restringem à infraestrutura tecnológica, estão diretamente ligados à cultura organizacional e às

práticas adotadas no tratamento da informação. Logo, a ausência de políticas e procedimentos, tecnológicos ou não, que assegurem a Segurança da Informação, pode impactar negativamente nos ativos da organização, acarretando prejuízos financeiros ou subjetivos, tornando necessária a adoção de práticas que assegurem de forma contínua a Segurança da Informação nas organizações e nos Sistemas de Informação.

Aplicável em diferentes cenários, porém, com destaque para o contexto desse trabalho, pode-se citar a importância da Segurança da Informação no contexto das instituições educacionais. Dada a natureza dos dados e informações manipuladas, tais como informações pessoais, acadêmicas e administrativas, frequentemente associadas a direitos individuais e a processos institucionais formais, são exigidos mecanismos de proteção capazes de preservar sua autenticidade, integridade e confiabilidade (ALBUQUERQUE JUNIOR; SANTOS, 2015). A fragilidade desses mecanismos expõe documentos acadêmicos a riscos como fraudes, adulterações e perdas, comprometendo tanto a credibilidade institucional quanto a validade jurídica dos registros (VANDERLEI NETO, 2021).

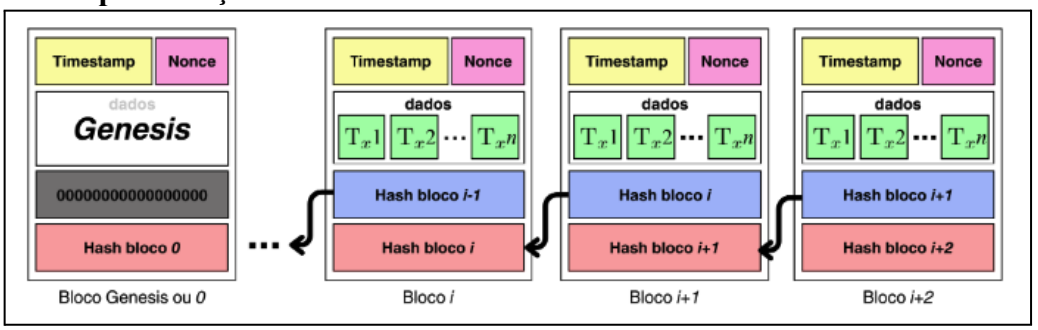
2.2 BLOCKCHAIN

A *Blockchain* é uma tecnologia de registro distribuído, ou seja, um sistema em que as informações não ficam armazenadas em um único lugar, mas que são compartilhadas entre vários participantes de uma rede. Esse modelo elimina a necessidade de uma autoridade central para controlar ou validar os dados, aumentando a confiabilidade das informações registradas (FREITAS et al., 2023).

Paralelamente, para Ferreira et al. (2024, p. 5), a *blockchain* é compreendida como uma sequência de blocos de informações ligados entre si em forma de cadeia, onde cada bloco armazena um conjunto de transações e é conectado ao bloco anterior por meio de um código criptográfico *hash*, que funciona como um “resumo” do bloco anterior. Esse encadeamento faz com que qualquer alteração em um bloco afete toda a cadeia, dificultando fraudes e manipulações, conforme ilustrado na Figura 1.

Embora a blockchain tenha surgido inicialmente no contexto financeiro, especialmente associada às criptomoedas, seu uso não se restringe a esse cenário. Atualmente, a tecnologia vem sendo aplicada em diversas áreas por oferecer segurança, transparência e confiabilidade no registro de informações (FERREIRA et al., 2024).

Figura 1 – Representação da estrutura interna de uma *blockchain*



Fonte: Ferreira et al. (2019).

O modelo da *blockchain* permite que cada membro da rede mantenha uma cópia local da *blockchain* e contribua para a validação dos registros, tornando o sistema transparente, auditável e verificável pelos participantes autorizados. A segurança é resultado da combinação entre replicação distribuída, criptografia e mecanismos de consenso, que garantem que apenas registros válidos sejam adicionados à cadeia, mesmo diante de falhas ou comportamentos maliciosos. Além disso, a integridade, a autenticidade e o não repúdio dos dados são assegurados pelo encadeamento criptográfico dos blocos, pelo uso de assinaturas digitais e pelo caráter permanente e auditável dos registros (FREITAS et al., 2023).

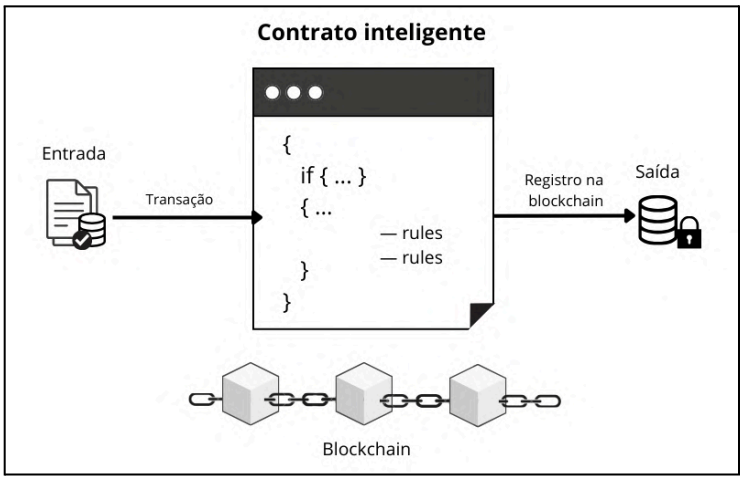
Os modelos de *blockchains* podem ser classificados em dois grandes grupos: as não permissionadas (públicas) e as permissionadas (privadas). Nas não permissionadas, como *Bitcoin*[3] e *Ethereum*[4], qualquer participante pode ingressar na rede sem necessidade de identificação ou autenticação prévia, sendo o consenso alcançado por mecanismos como Proof-of-Work (PoW)[5] ou Proof-of-Stake (PoS)[6]. Por outro lado, nas permissionadas, a participação ocorre de forma controlada, com nós previamente identificados e autorizados. Esse modelo possibilita o uso de algoritmos de consenso mais eficientes, como PBFT[7] (*Practical Byzantine Fault Tolerance*) e Raft[8], além de reduzir custos computacionais e energéticos. Em ambientes institucionais e corporativos, essa abordagem é especialmente relevante, pois permite maior controle sobre identidade, governança e operação da rede, requisitos geralmente não atendidos por blockchains públicas abertas (FREITAS et al., 2023; FERREIRA et al., 2024).

---

[3] Criptomoeda descentralizada utilizada para transações financeiras em uma rede blockchain.
[4] Criptomoeda nativa da rede Ethereum, usada para transações e taxas da plataforma.
[5] Mecanismo de consenso baseado na resolução de problemas computacionais para validação de blocos.
[6] Mecanismo de consenso no qual a validação de blocos é realizada com base na participação econômica dos validadores na rede.
[7] Algoritmo de consenso que permite à rede alcançar acordo mesmo na presença de nós maliciosos ou defeituosos, dentro de um limite tolerável.
[8] Algoritmo de consenso que tolera falhas por parada, no qual um nó líder é eleito para coordenar e replicar as operações entre os demais nós.

De modo geral, o funcionamento das redes *blockchain* depende dos chamados contratos inteligentes ou *smart contracts*. Estes assumem a forma de programas computacionais que executam instruções automaticamente que, na prática, vão além da simples validação de condições, eles executam ações específicas conforme regras previamente definidas, sem necessidade de intervenção humana, desempenhando o papel de mecanismos de coordenação e automação, conforme a Figura 2. A lógica desses contratos é incorporada ao próprio sistema, permitindo uma execução autônoma e distribuída na rede, o que contribui para ganhos de eficiência, rastreabilidade e confiabilidade nos processos (FERREIRA et al., 2024).

Figura 2 – Esquema do fluxo de entrada e saída de dados em um contrato inteligente



Fonte: Autoria própria.

Armazenados e executados na própria infraestrutura da *blockchain*, esses contratos herdam propriedades da blockchain como descentralização, imutabilidade e auditabilidade, reduzindo a dependência de servidores centralizados, permitindo que a lógica de negócio seja validada de forma compartilhada entre os participantes autorizados da rede.

Na plataforma de *blockchain* permissionada *Hyperledger Fabric*, os contratos inteligentes, denominados *chaincodes,* são executados em ambiente controlado, com participantes previamente identificados e autenticados (HYPERLEDGER FABRIC, 2025), corroborando com a adesão da tecnologia em contextos que exigem controle de acesso. No entanto, apesar das garantias de integridade e confiabilidade oferecidas pela *blockchain*, o armazenamento de grandes volumes de dados ou documentos completos na rede não é recomendado, dadas as limitações técnicas (baixa escalabilidade e boas práticas arquiteturais em blockchain armazenar apenas metadados, hashes e referência), sendo necessário a

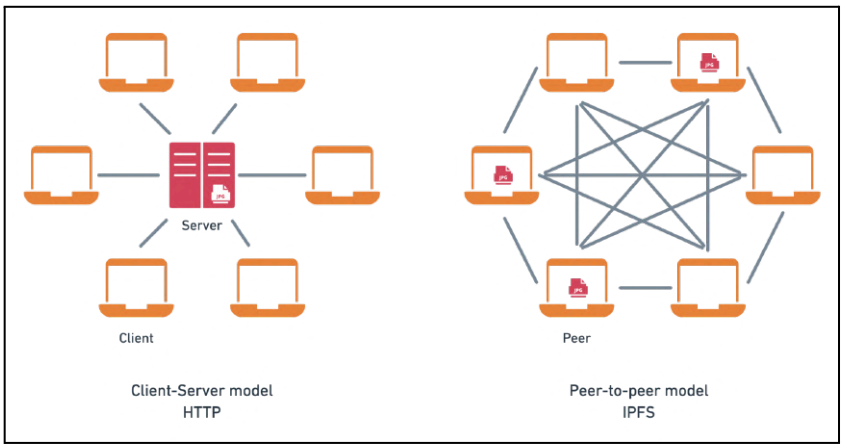
utilização de outros mecanismos de armazenamento de forma complementar ao utilizado na *blockchain.*

2.2.1 Serviço de Armazenamento Distribuído IPFS

O *InterPlanetary File System* (IPFS) é um sistema de armazenamento distribuído baseado em rede ponto a ponto (P2P) e endereçamento por conteúdo, no qual os arquivos são identificados por um identificador criptográfico (CID) derivado de seu conteúdo.

Diferentemente do modelo tradicional cliente-servidor, o IPFS não depende de um servidor central para disponibilização dos dados (Figura 3), permitindo que o mesmo conteúdo seja recuperado a partir de qualquer nó que o possua (BENET, 2014; WEN et al., 2024).

Figura 3 – Comparação entre arquitetura centralizada e arquitetura descentralizada em redes distribuídas



Fonte: Adaptado de IPFS (2022).

Apesar da arquitetura distribuída, o IPFS pode ser acessado de forma transparente por aplicações web tradicionais por meio de *gateways*, permitindo o acesso a dados endereçados por conteúdo diretamente via navegadores convencionais, sem que seja necessário executar um nó local. Além disso, o serviço pode ser configurado para operar em ambientes privados, por meio da definição de *swarms* restritos, possibilitando o controle de participação na rede, sendo mais utilizada a implementação do protocolo Kubo (antigo *go-ipfs*), por viabilizar essas funcionalidades e permitir o uso em ambientes de produção e em arquiteturas integradas a sistemas distribuídos e *blockchain* (IPFS, 2022).

No IPFS, a disponibilidade e a persistência dos dados estão diretamente associadas à replicação do conteúdo entre os nós da rede. Assim, os dados permanecem acessíveis enquanto houver ao menos um nó responsável por manter sua réplica, característica que confere tolerância a falhas e reduz a dependência de infraestrutura centralizada.

Os principais aspectos do modelo de armazenamento distribuído do IPFS são sintetizados no Quadro 1.

Quadro 1 – Aspectos técnicos do IPFS

Aspecto	IPFS
Persistência dos dados	A persistência dos dados está associada à replicação do conteúdo entre os nós da rede, sendo necessária a adoção de estratégias de manutenção para garantir a disponibilidade contínua.
Disponibilidade	O conteúdo permanece acessível enquanto houver ao menos um nó mantendo sua réplica, característica típica de sistemas distribuídos.
Uso prolongado	Pode operar de forma contínua quando integrado a políticas de replicação e gestão de nós, especialmente em ambientes controlados ou permissionados.
Tolerância a falhas	A arquitetura distribuída permite a continuidade do acesso mesmo diante de falhas pontuais de nós individuais.
Integridade dos dados	Garantida por identificadores criptográficos derivados do conteúdo, possibilitando a verificação de alterações nos dados armazenados.
Rastreabilidade	Pode ser ampliada quando integrada a soluções de blockchain, permitindo o acompanhamento de versões e alterações por meio de identificadores de conteúdo.
Confidencialidade	Deve ser assegurada por mecanismos complementares, como criptografia e controle de acesso, conforme o contexto de aplicação.

Fonte: Autoria própria.

2.3 CRIPTOGRAFIAS

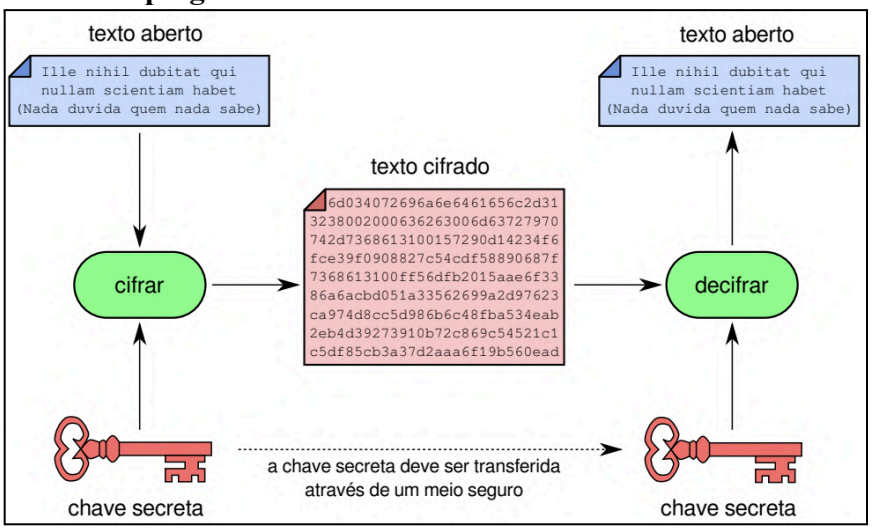
A criptografia envolve técnicas voltadas à proteção da informação por meio de transformações matemáticas aplicadas aos dados. De modo geral, esses mecanismos podem ser organizados em criptografia simétrica e criptografia assimétrica.

A criptografia simétrica é um modelo no qual uma mesma chave é utilizada para criptografar e descriptografar os dados, devendo a essa chave ser compartilhada entre o emissor e receptor (OLIVEIRA, 2012). Esse tipo de criptografia distingue-se pela eficiência computacional, simplicidade de implementação e baixo custo de processamento, características que tornam esse tipo amplamente utilizado na proteção de grandes volumes de dados (LUDWIG; REBELATTO; SILVA, 2020) e, mesmo quando os algoritmos são de conhecimento público, a segurança das informações é mantida desde que a chave secreta permaneça protegida, conforme no fluxo descrito na Figura 4.

A criptografia assimétrica, ou de chave pública, utiliza um par de chaves distintas e matematicamente relacionadas: uma pública e uma privada (OLIVEIRA, 2012). Esse modelo elimina a necessidade de compartilhamento prévio de chaves e possibilita garantir

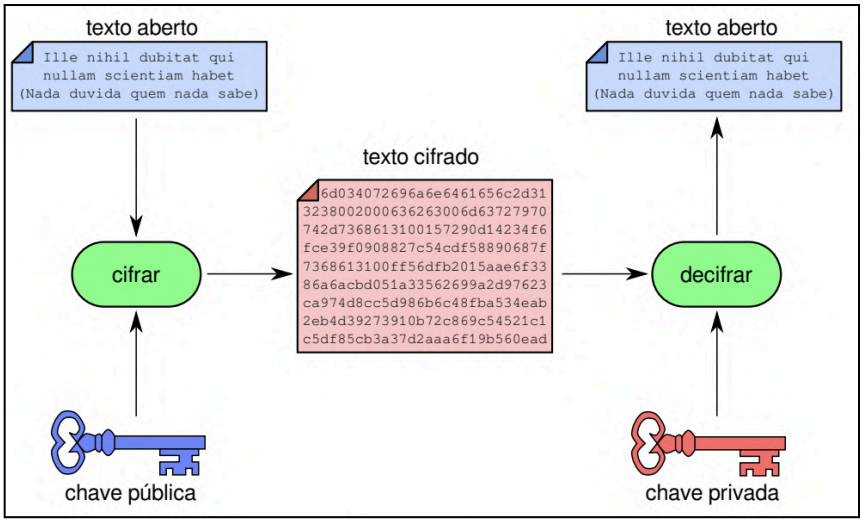
confidencialidade, autenticidade, integridade e não repúdio. Segundo Ludwig et al. (2020), seu principal diferencial está na capacidade de validar a origem e a integridade das informações em ambientes abertos. Esse tipo de criptografia é fundamental em mecanismos como assinaturas digitais, certificados digitais e infraestruturas de chaves públicas (PKI), sendo amplamente empregada em sistemas distribuídos e tecnologias como *blockchain* (MAZIEIRO, 2019), conforme representado na Figura 5.

Figura 4 – Fluxo da criptografia simétrica.



Fonte: Adaptado de MAZIEIRO (2019).

Figura 5 – Representação do processo de criptografia assimétrica.



Fonte: Adaptado de MAZIEIRO (2019).

2.3.1 Funções Hash Criptográficas

Uma função *hash* criptográfica, também conhecida como resumo criptográfico, é uma função que transforma uma entrada de tamanho variável em uma saída curta e de tamanho fixo, sendo definida formalmente como: $y = hash(x)$ (MAZIEIRO, 2019).

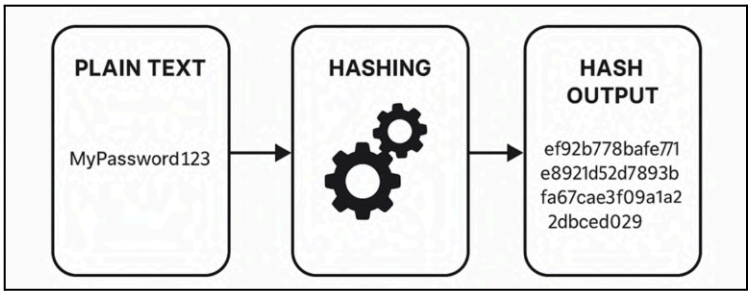
Sua principal aplicação está na verificação de integridade, em virtude de que qualquer alteração mínima no conteúdo original resulta na modificação do valor *hash*, permitindo a detecção de adulterações sem a necessidade de acesso ao conteúdo (MAZIEIRO, 2019). Sob a perspectiva arquivística, esse mecanismo contribui para a identidade e integridade do documento ao longo do tempo, requisito funcional da autenticidade de documentos digitais (CONARQ, 2012).

Além disso, essas funções apresentam propriedades formais que asseguram a confiabilidade, como unidirecionalidade, sensibilidade a leves alterações na entrada (efeito avalanche) e resistência a colisões entre *hash* de documentos distintos. Mesmo com algoritmos publicamente conhecidos, essas características dificultam ataques e tornam os hashes mecanismos eficazes para a verificação de integridade dos dados (MAZIERO, 2019; LUDWIG et al., 2020).

Em sistemas que integram *blockchain* e IPFS, as funções *hash* criptográficas desempenham papel central na garantia da integridade e da confiabilidade dos documentos acadêmicos digitais. Para esse fim, são utilizados dois mecanismos distintos, ambos fundamentados no algoritmo SHA-256, porém aplicados em camadas diferentes da arquitetura do sistema: o *hash* criptográfico SHA-256 e o Content Identifier (CID) empregado pelo IPFS. Essa abordagem permite dissociar a verificação de integridade do documento de seu mecanismo de endereçamento em ambiente de armazenamento distribuído.

O algoritmo SHA-256 (Figura 6) é utilizado para gerar um resumo criptográfico do conteúdo dos documentos acadêmicos em formato *Portable Document Format* (PDF), produzindo um identificador de 256 bits que atua como prova de integridade. Esse valor é registrado na *blockchain*, possibilitando a verificação de eventuais alterações no conteúdo original ao longo do tempo.

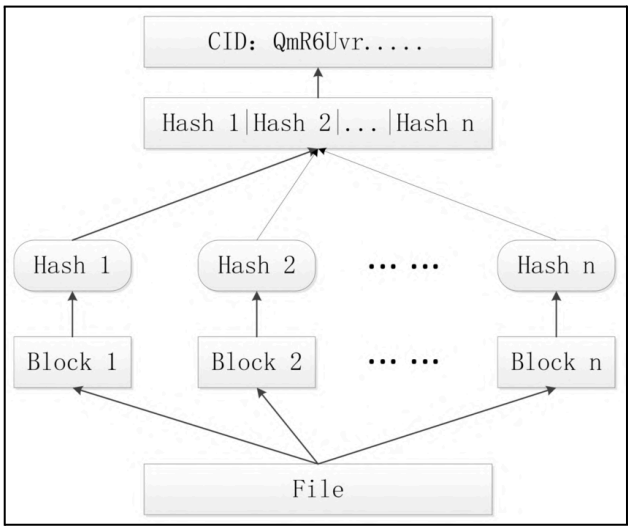
Figura 6 – Representação do funcionamento do algoritmo SHA-256.



Fonte: Adaptado de CheapSSLsecurity (2024).

De forma complementar, o *Content Identifier* (CID), ilustrado na figura 7, é empregado como mecanismo de identificação dos documentos com base em seu conteúdo no IPFS, sendo derivado diretamente dos dados do arquivo por meio de funções *hash* baseadas em SHA-256, associadas a mecanismos de codificação próprios do protocolo, que resultam em um identificador único e determinístico. Enquanto o SHA-256 permite verificar se o documento foi alterado, o CID possibilita seu endereçamento e recuperação em um ambiente de armazenamento distribuído, tornando ambos os mecanismos complementares no contexto do sistema proposto.

Figura 7 – A figura ilustra o princípio de geração do Content Identifier (CID).



Fonte: Adaptado de Wang et al. (2022).

2.3.2 Certificados Digitais X.509

Em ambientes digitais, a associação confiável entre identidades e chaves criptográficas é um elemento central para a segurança da informação. Nesse contexto, os certificados digitais desempenham o papel de vincular uma chave pública a uma entidade reconhecida, possibilitando a identificação segura dos participantes de uma comunicação. O

padrão X.509 estabelece como essa vinculação é estruturada e validada, utilizando uma Autoridade Certificadora como base do modelo de confiança adotado (MAZIERO, 2019).

Na prática, certificados X.509 são utilizados para confirmar a autenticidade de chaves públicas e possibilitar a verificação de assinaturas digitais. Esse mecanismo permite que partes que não possuem relação prévia possam confiar umas nas outras em ambientes digitais. Por esse motivo, o padrão é amplamente empregado em sistemas distribuídos e institucionais. Em *blockchains* permissionadas, como o *Hyperledger Fabric*, seu uso é fundamental para atender requisitos de identificação e autenticação dos participantes, aspectos diretamente ligados à governança da rede (HYPERLEDGER FABRIC, 2025).

2.4 FRAMEWORK HYPERLEDGER FABRIC

O *Hyperledger Fabric* é um *framework* de blockchain permissionada, mantido pela *Linux Foundation*[9] e voltado para o uso corporativo e institucional. O *Hyperledger* surgiu quando o uso da *blockchain* foi além de criptomoedas, passando a atender cenários nos quais governança, controle de participantes e integração entre sistemas são requisitos centrais (FERREIRA et al., 2024).

Esse framework foi projetado para cenários que exigem controle de participação e a responsabilização dos atores envolvidos é um elemento fundamental. Por isso, sua adoção é recorrente em contextos organizacionais que lidam com informações sensíveis e exigem garantias de integridade, não repúdio e controle de acesso aos dados (FREITAS et al., 2023).

Diferentemente de outras abordagens, ele não faz uso de criptomoeda nativa, nem de mecanismos de consenso baseados em prova de trabalho (PoW) ou prova de participação (PoS), o que contribui para a redução de custos computacionais e do consumo energético (HYPERLEDGER FABRIC, 2025).

Entre os componentes, a troca de informação é realizada por meio do protocolo *gRPC Remote Procedure Calls (*gRPC)[10], utilizado como padrão de comunicação entre clientes, *peers* e nós de ordenação. Para a segurança da comunicação entre as partes, o *framework* adota um modelo de autenticação mútua baseado em certificados digitais X.509, implementado por meio de *Mutual Transport Layer Security* (mTLS)[11]. Logo, somente entidades previamente autenticadas conseguem participar da rede, e os dados transmitidos

[9] https://www.linuxfoundation.org/

[10] Protocolo de comunicação de alto desempenho baseado em chamadas de procedimento remoto, amplamente utilizado em sistemas distribuídos.

[11] Mecanismos de segurança em que cliente e servidor se autenticam mutuamente por meio de certificados digitais, garantindo comunicação segura.

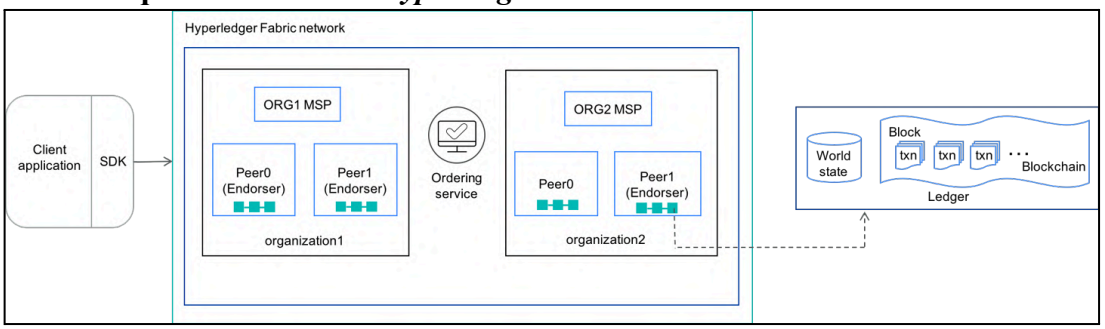
permanecem protegidos contra acessos não autorizados ou alterações indevidas, atendendo às exigências típicas de ambientes corporativos permissionados (ANDROULAKI et al., 2018; HYPERLEDGER FABRIC, 2025).

O *Hyperledger Fabric* organiza sua arquitetura em componentes bem definidos, representados pela Figura 8, cada um com responsabilidades específicas no funcionamento da rede. Essa separação contribui para maior controle sobre a execução das transações, a privacidade das informações e a governança do sistema, características centrais em blockchains permissionadas (HYPERLEDGER FABRIC, 2025). Entre os principais elementos do *framework,* destacam-se:

- O *ledger* corresponde ao livro-razão distribuído mantido pelos peers da rede, reunindo tanto o histórico imutável das transações quanto o estado atual dos ativos. Esse elemento possui dois componentes: *blockchain* e *world state*; estão sintetizados no Quadro 2, que apresenta sua função no contexto da rede.
- Os canais (*channels*) representam instâncias lógicas isoladas dentro da rede, permitindo que subconjuntos de organizações compartilhem dados e transações de forma privada, mesmo operando sobre a mesma infraestrutura física. Esse mecanismo viabiliza confidencialidade e segmentação de informações, sendo um dos principais diferenciais do *Hyperledger Fabric*.
- As organizações (*organizations*) constituem as entidades institucionais participantes da rede e formam a base do modelo de governança. Cada organização administra seus próprios *peers* e define políticas relacionadas à validação de transações, acesso a dados e participação nos canais.
- Os *peers* são responsáveis por manter cópias do *ledger* e executar o *chaincode*, podendo assumir diferentes funções, como *endorsing peers*, *committing peers* e *anchor peers*, detalhados no Quadro 3.
- O serviço de ordenação (*ordering service*) é responsável por organizar as transações endossadas em uma sequência determinística e agrupá-las em blocos, que posteriormente são distribuídos aos *peers* para validação e registro.
- O *Fabric* desacopla logicamente esse serviço dos *peers*, permitindo flexibilidade arquitetural e a adoção de mecanismos de consenso como o Raft, conforme apresentado no Quadro 4.
- A gestão de identidades e a governança da rede são asseguradas pelo *Membership Service Provider* (MSP) e pela Autoridade Certificadora (CA). Enquanto a CA emite e gerencia certificados digitais baseados no padrão X.509, o MSP define

como essas identidades são reconhecidas e utilizadas na rede. As políticas de governança (Quadro 5), incluindo políticas de endosso, de canal e de controle de acesso, estabelecem as regras de funcionamento e tomada de decisão da rede.

Figura 8 – Arquitetura da rede *Hyperledger Fabric*



Fonte: IBM (2026).

Quadro 2 – Elementos complementares do Ledger

Componente	Descrição
Blockchain	Cadeia de blocos contendo o log imutável de todas as transações, estruturada como lista encadeada de blocos.
World State	Banco de dados que mantém o estado atual dos ativos, permitindo consultas rápidas sem percorrer toda a *blockchain* (LevelDB ou CouchDB).

Fonte: Autoria própria.

Quadro 3 – Tipos de Peers

Tipo de *Peer*	Função
Endorsing Peer	Executa os smart contracts e valida transações conforme as políticas de endosso, retornando uma assinatura de aprovação.
Committing Peer	Recebe blocos do ordering service e registra as transações validadas no *ledger*.
Anchor Peer	Facilita a comunicação entre organizações em um canal através do protocolo *gossip*.

Fonte: Autoria própria.

Quadro 4 – Mecanismos de Consenso no Serviço de Ordenação

Mecanismos	Função
Raft	Protocolo de consenso tolerante a falhas de *crash*, recomendado para produção.
Solo	Ordenador único, utilizado apenas para desenvolvimento e testes.

Fonte: Autoria própria.

Quadro 5 – Aspectos de Políticas e Governança

Tipo de política	Função
Endorsement Policy	Define quais organizações devem endossar uma transação para que seja considerada válida.
Channel Policy	Governa a configuração e administração do canal.
Access Control Policy	Define permissões de acesso a recursos específicos.

Fonte: Autoria própria.

3 SOLUÇÃO PROPOSTA

Neste capítulo é apresentada a solução proposta. Na subseção 3.1, é introduzida uma visão geral da solução, com destaque para os três principais subsistemas da solução. Na subseção 3.2, são apresentados os requisitos que regem esse sistema, tais como: requisitos funcionais, requisitos não funcionais e regras de negócio. De forma complementar, na subseção 3.3, foram ilustrados os principais módulos e eventos da solução. Este tem como objetivo fornecer representações gráficas de todos os ângulos da solução, auxiliando a compreensão e o entendimento conceitual da arquitetura e fluxos operacionais do protótipo.

3.1 VISÃO GERAL DA SOLUÇÃO

O *Academic Ledger* é uma solução baseada em tecnologia *blockchain* voltada à gestão e ao registro do processo de defesa do Trabalho de Conclusão de Curso de Graduação.

O regulamento dos Trabalhos de Conclusão de Cursos do IFAL destaca obrigações e processos que devem ser atendidos durante o desenvolvimento do trabalho. Anexo à portaria, são apresentados documentos com a finalidade de regularizar e documentar o processo de orientação, agendamento e defesa do TCC. Quanto à defesa, atualmente, exige-se os documentos (i) “Ata de Defesa” (Anexo I), que contém informações referentes à cerimônia de defesa de TCC, o parecer final do trabalho, discentes autores e membros da banca avaliadora; e a (ii) “Ficha de aprovação de TCC” (Anexo II), que apresenta um conjunto de critérios que devem ser analisados pela banca examinadora durante a defesa do trabalho.

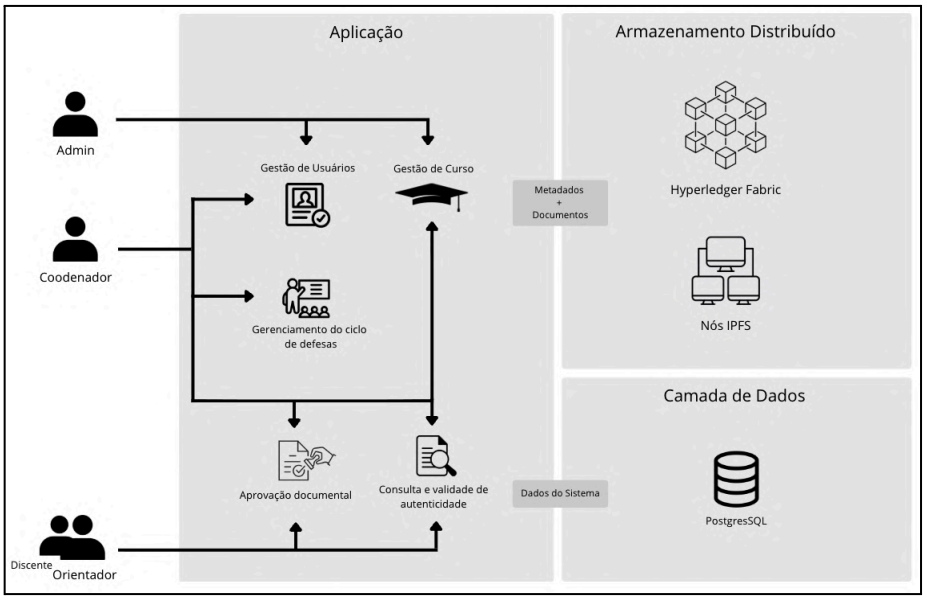
Apesar da exigência, a portaria não descreve como o gerenciamento da documentação criada deve ser realizado, se em meio físico ou digital, deixando os documentos vulneráveis quanto à segurança das informações. Diante disso, é proposto o *Academic Ledger* (Figura 8), uma solução baseada em tecnologia *blockchain* que visa, principalmente, garantir a integridade desses documentos, além de complementar os processos realizados pelas coordenações de cursos de graduação, por meio dos subsistemas “Gerenciamento de Defesas de TCCs” (Subseção 3.1.1), “Aprovação Documental” (Subseção 3.1.2) e “Consulta e Validação de Autenticidade” (Subseção 3.1.3).

A implementação do *Academic Ledger* foi organizada de forma modular e versionada, sendo disponibilizada publicamente em repositórios distintos na plataforma *GitHub*. A solução é composta por quatro repositórios principais: (i) o *frontend*[12], responsável

[12] https://github.com/Edu4rdoCarlos/student-ledger-frontend

pela interface de interação com os usuários do sistema; (ii) o *backend*[13], que concentra a lógica de negócio, o controle de acesso e a integração entre os subsistemas; (iii) o repositório da rede *Hyperledger Fabric*[14], que contempla a configuração da *blockchain* permissionada e dos *chaincodes* utilizados para o registro das informações; e (iv) o repositório relacionado ao IPFS[15], destinado ao armazenamento distribuído dos documentos associados às defesas de TCC.

Figura 8 – Visão Geral da Solução



Fonte: Autoria própria.

3.1.1 Subsistema: Gerenciamento de Defesas de TCC

O módulo de gerenciamento de defesas compreende todas as etapas administrativas relacionadas à defesa de TCC, tais como: o agendamento de defesa; o reagendamento de defesa previamente cadastrada; o cancelamento de defesa; e a submissão da documentação exigida pelo regimento institucional do IFAL. Tais atividades devem ser realizadas pelo coordenador do curso de graduação. Além disso, os discentes, autores e orientadores poderão consultar seus históricos de defesas cadastradas.

Quanto à funcionalidade de "agendamento da defesa", o usuário responsável deve informar: o título do trabalho, horário, data e o local da defesa, orientador(a) do trabalho, os discentes autores[16], nome completo e e-mail dos membros da banca examinadora. Mediante o agendamento, a defesa recebe um status inicial de "Agendada" e todos os envolvidos (discentes, orientador(a) e membros da banca examinadora) serão notificados

[13] https://github.com/Edu4rdoCarlos/student-ledger-api
[14] https://github.com/Edu4rdoCarlos/student-ledger
[15] https://github.com/Edu4rdoCarlos/student-ledger-ipfs
[16] Limitando-se a dois, conforme as normas estabelecidas pela instituição.

automaticamente por e-mail. Ressalta-se que, anterior ao processo de agendamento, faz-se necessário que os(as) discentes autores do trabalho e o(a) docente orientador(a) estejam previamente cadastrados no sistema.

Uma vez agendada, poderá ser feito o reagendamento e/ou cancelamento de defesa, contudo, tais ações só serão realizadas antes do horário da defesa informado no agendamento, também deverá ser informada uma justificativa. Essas ações serão registradas como evento no sistema, garantindo a rastreabilidade dos mesmos.

Por fim, após a realização da defesa, o coordenador deverá submeter as documentações "Ata de Defesa" e "Ficha de Avaliação", ambas no formato PDF, que serão armazenadas no servidor distribuído IPFS, para que possam ser avaliadas e, se aceitas, versionadas no sistema e encaminhadas à *blockchain*. Além dessa documentação, também deve ser informada a nota final atribuída ao TCC. É importante ressaltar que essa ação somente poderá ocorrer após o horário de defesa, informado no agendamento, e que os documentos enviados ficarão com status "Pendentes de Aprovação" até que sejam analisados pelo discente, orientador e coordenador do curso.

Além das atividades administrativas, citadas anteriormente, o módulo de defesa também permitirá aos discentes, orientadores e coordenadores a visualização do histórico de defesas cadastradas e o download das documentações submetidas.

3.1.2 Subsistema: Aprovação Documental

O processo de "Aprovação documental" inicia-se após a submissão da documentação e resultado final do TCC, e consiste no fluxo de aprovações realizado pelos discentes, orientador(a) e coordenador de curso de graduação. Inicialmente, o fluxo de aprovação é realizado em paralelo entre discentes e orientador(a), seguido pelo coordenador do curso, sendo esse responsável por enviar o documento à *blockchain* ou solicitar novos envios de documentos em caso de rejeições anteriores pelos discentes ou orientador(a).

Nesse processo, cada envolvido acessa o sistema por meio de suas credenciais JWT para a avaliação dos documentos *com status* "Pendentes de Aprovação". Na avaliação individual, o usuário deverá alterar o *status* do documento para "Aprovado" ou "Rejeitado", sendo essa alteração válida para a ata e ficha de avaliação do TCC.

Ao aprovar, o usuário confirma que está de acordo com o conteúdo apresentado e reconhece os dados acadêmicos, não apontando inconsistências nos documentos. Caso contrário, na rejeição, uma justificativa deve ser informada a fim de registrar a inconsistência e, então, essa ação suspende o andamento do fluxo de aprovação.

Até o registro na *blockchain*, os documentos submetidos poderão ser substituídos, sendo os envolvidos notificados para a realização da nova avaliação documental. Em caso de 100% de aprovação, será realizado o registro no *Hyperledger Fabric,* encerrando o fluxo de aprovações e consolidação da documentação da defesa como a versão oficial e imutável, impedindo modificações no conteúdo dos documentos. Em caso de necessidade de alteração de documento já registrado na *blockchain*, o usuário deverá submeter novos documentos, e um novo fluxo de aprovação será solicitado e, em caso de 100% de aprovação, os novos documentos passam a ser válidos, sendo criada e registrada uma nova versão dos mesmos e o anterior será invalidado.

3.1.3 Subsistema: Consulta e Validação de Autenticidade Documental

O subsistema de "Consulta e Validação de Autenticidade Documental", que permite ao usuário verificar a autenticidade de uma cópia dos documentos Ata de Defesa ou Avaliação de Desempenho, é legítimo e corresponde a um TCC oficialmente registrado. Essa ação pode ser realizada por qualquer usuário com acesso à plataforma.

Nesse processo, a cópia ou o *hash* do documento informado é comparado com o registro existente na *blockchain*. Caso um registro correspondente seja encontrado, o sistema confirma a autenticidade do documento e exibe informações relevantes da defesa, como discentes, orientador, curso e data de registro, ou o sistema retorna se ele está pendente de aprovação. Caso contrário, o documento é indicado como não registrado, o que pode significar tentativa de fraude, documento ainda não aprovado ou versão legada.

3.2 PROJETO DE SOFTWARE

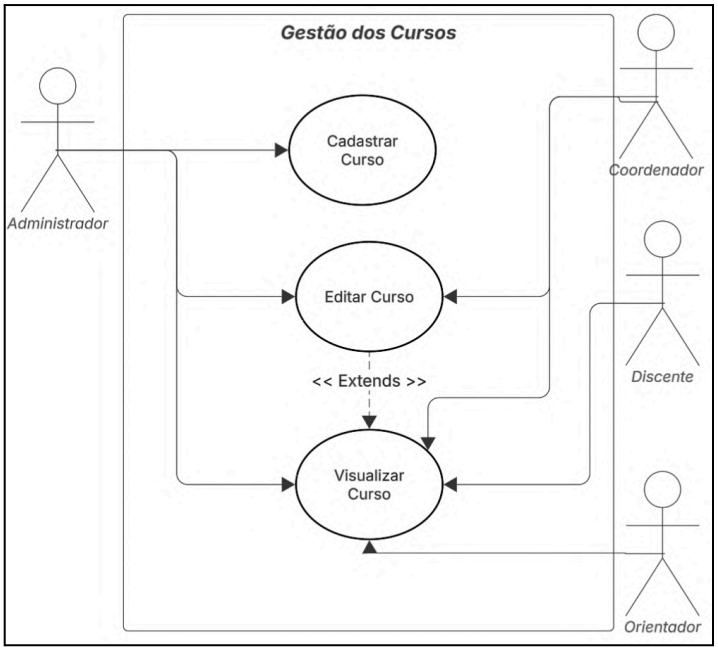
3.2.1 Diagramas de Caso de Uso

Os diagramas de Caso de Uso foram desenvolvidos com base nos subsistemas "Gerenciamento de Defesas de TCC", "Aprovação Documental" e "Consulta e Validação de Autenticidade Documental", destacando as principais funcionalidades e interações entre usuários e o sistema, com base nos requisitos do software apresentados no Apêndice A.

As funcionalidades contidas no "Gerenciamento de Defesas de TCC" foram representadas nos diagramas: Gestão de cursos (Figura 9); Gestão de identidades (Figura 10); Gestão de defesas (Figura 11) e Gestão de documentos (Figura 12). Quanto ao contexto do subsistema "Aprovação Documental", foi criado o diagrama de caso de uso Gestão das aprovações (Figura 13). Por fim, no escopo do subsistema de "Consulta e Validação de Autenticidade Documental", foi criado um diagrama de verificação de documentos (Figura

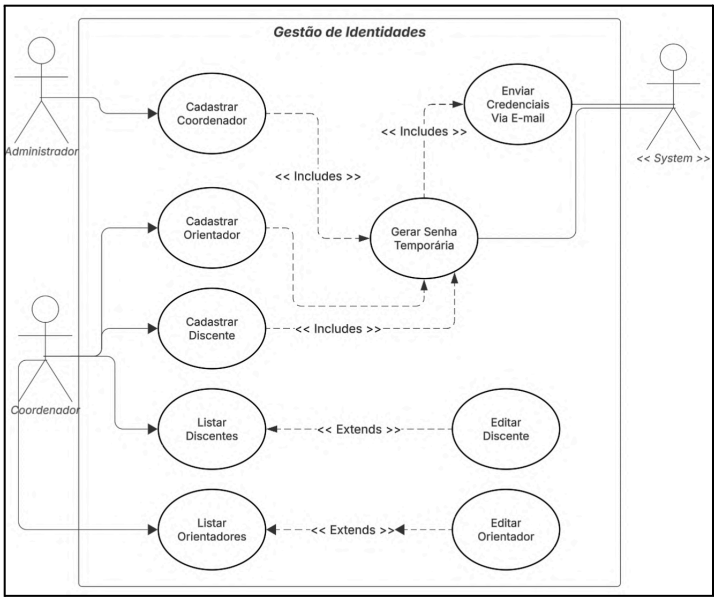
14). Ressalta-se que, apesar de não estar descrito nos diagramas, todas as ações só podem ser realizadas após o login dos usuários na ferramenta, sendo essa ação obrigatória.

Figura 9 – Diagrama de Caso de Uso do Domínio de Gestão de Cursos



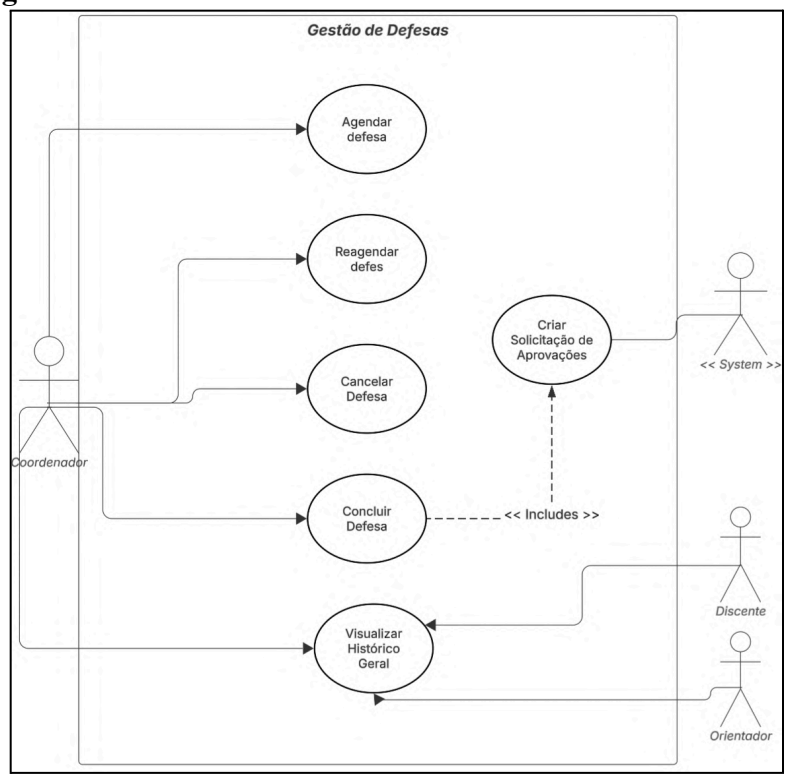
Fonte: Autoria própria.

Figura 10 – Diagrama de Caso de Uso do Domínio de Gestão de Identidades.



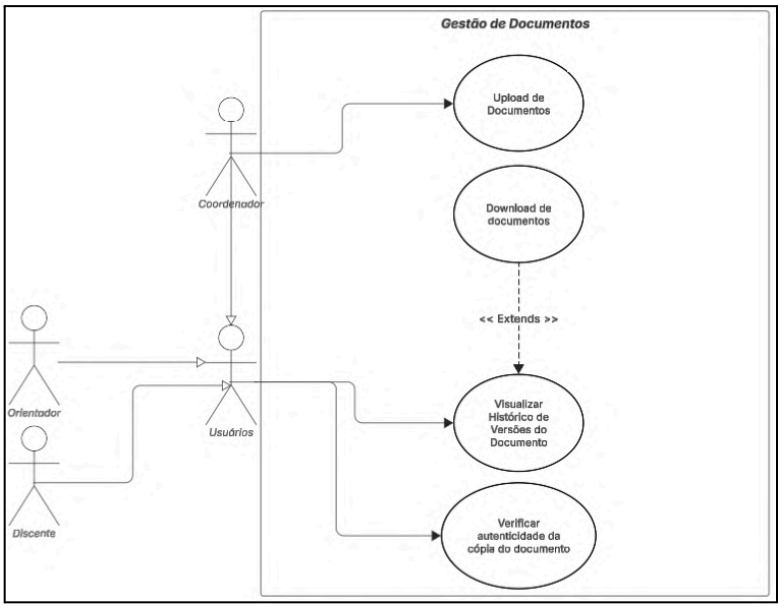
Fonte: Autoria própria.

Figura 11 – Diagrama de Caso de Uso do Domínio de Gestão de Defesas.



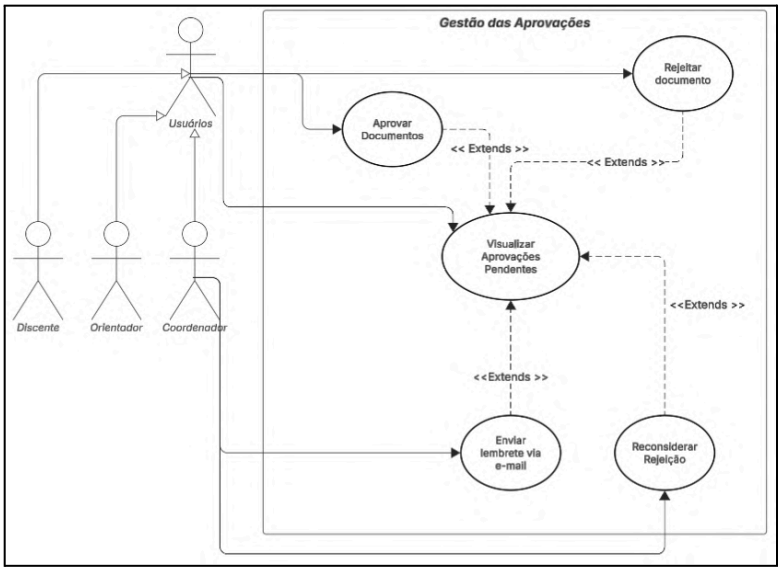
Fonte: Autoria própria.

Figura 12 – Diagrama de Caso de Uso do Domínio de Gestão de Documentos



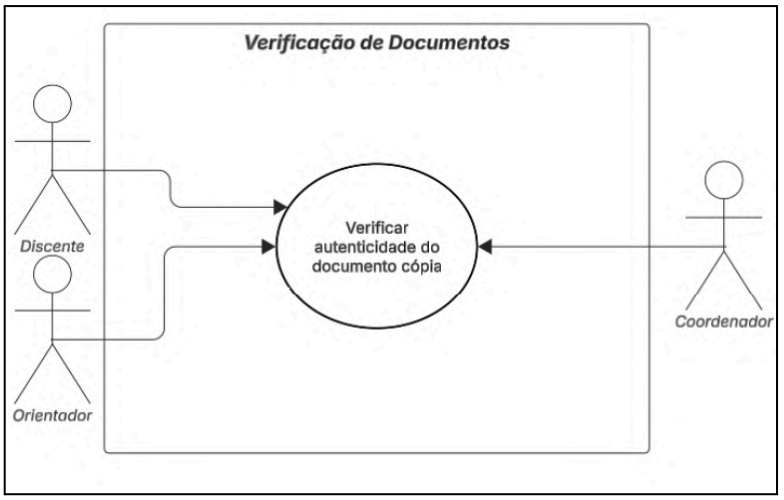
Fonte: Autoria própria.

Figura 13 – Diagrama de Caso de Uso do Domínio de Gestão de Aprovações



Fonte: Autoria própria.

Figura 14 – Diagrama de Caso de Uso da Verificação de Documento



Fonte: Autoria própria.

3.2.2 Diagramas de Sequência

Considerando o objetivo desse trabalho com foco na *blockchain* e integridade da informação, foram definidos cinco diagramas de sequência para a compreensão da solução, para as funcionalidades abaixo:

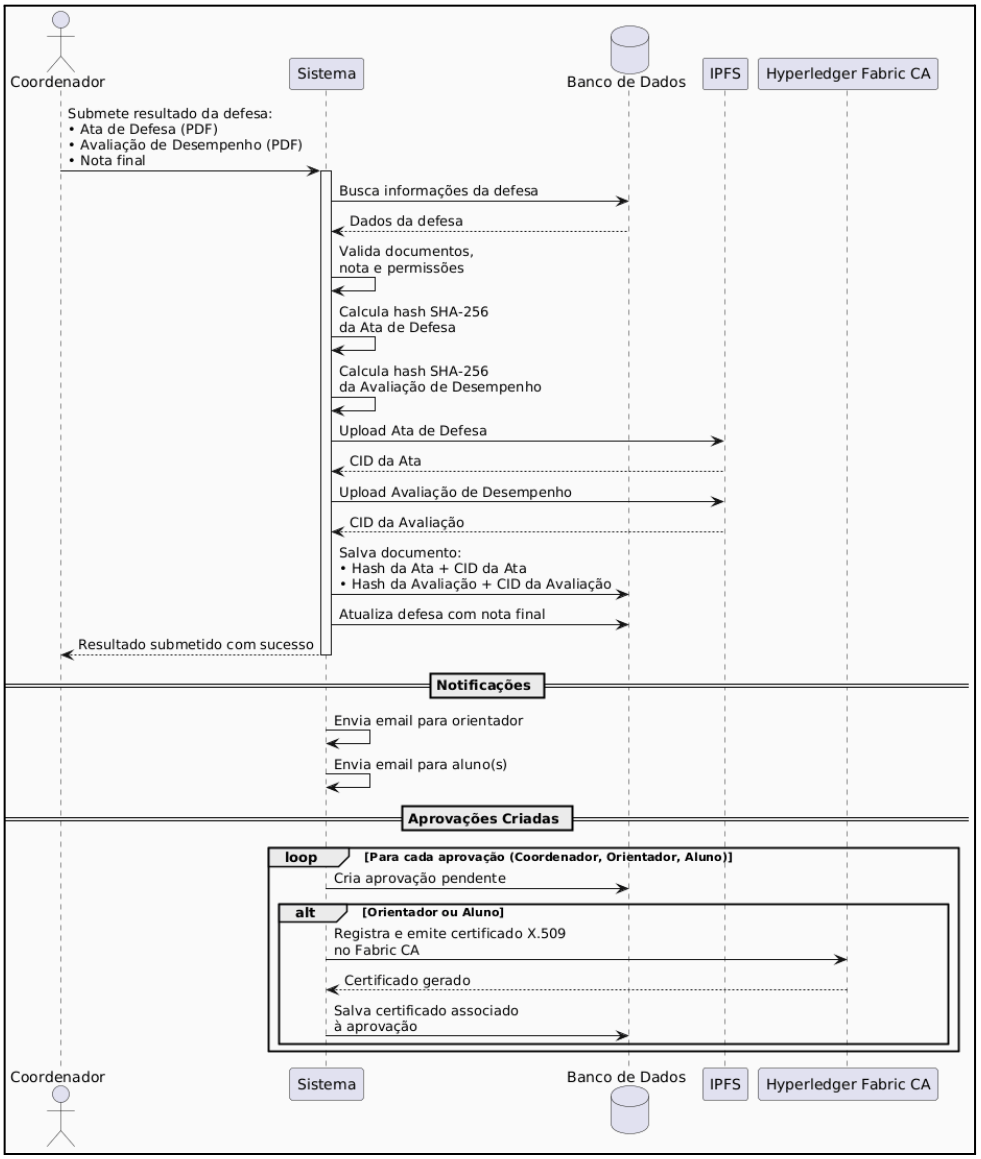
A. Concluir uma defesa do TCC: demonstra o comportamento do sistema durante a conclusão, demonstrando o comportamento do principal evento da submissão da documentação exigida pela portaria e submissão do resultado do TCC (Figura 15). A execução bem-sucedida dessa etapa dá início à Gestão de Aprovação.

B. Gestão de Aprovação: demonstra o comportamento do sistema durante o processo de fluxo de aprovação do módulo “Aprovação Documental”. O fluxo foi dividido em

"Fase 1 - Aprovação Orientador e Aluno" (Figura 16) e "Fase 2 - Aprovação Coordenador" (Figura 17). Uma vez que todos os participantes aprovem, esse documento é preparado com os dados necessários para o registro na *Blockchain*.

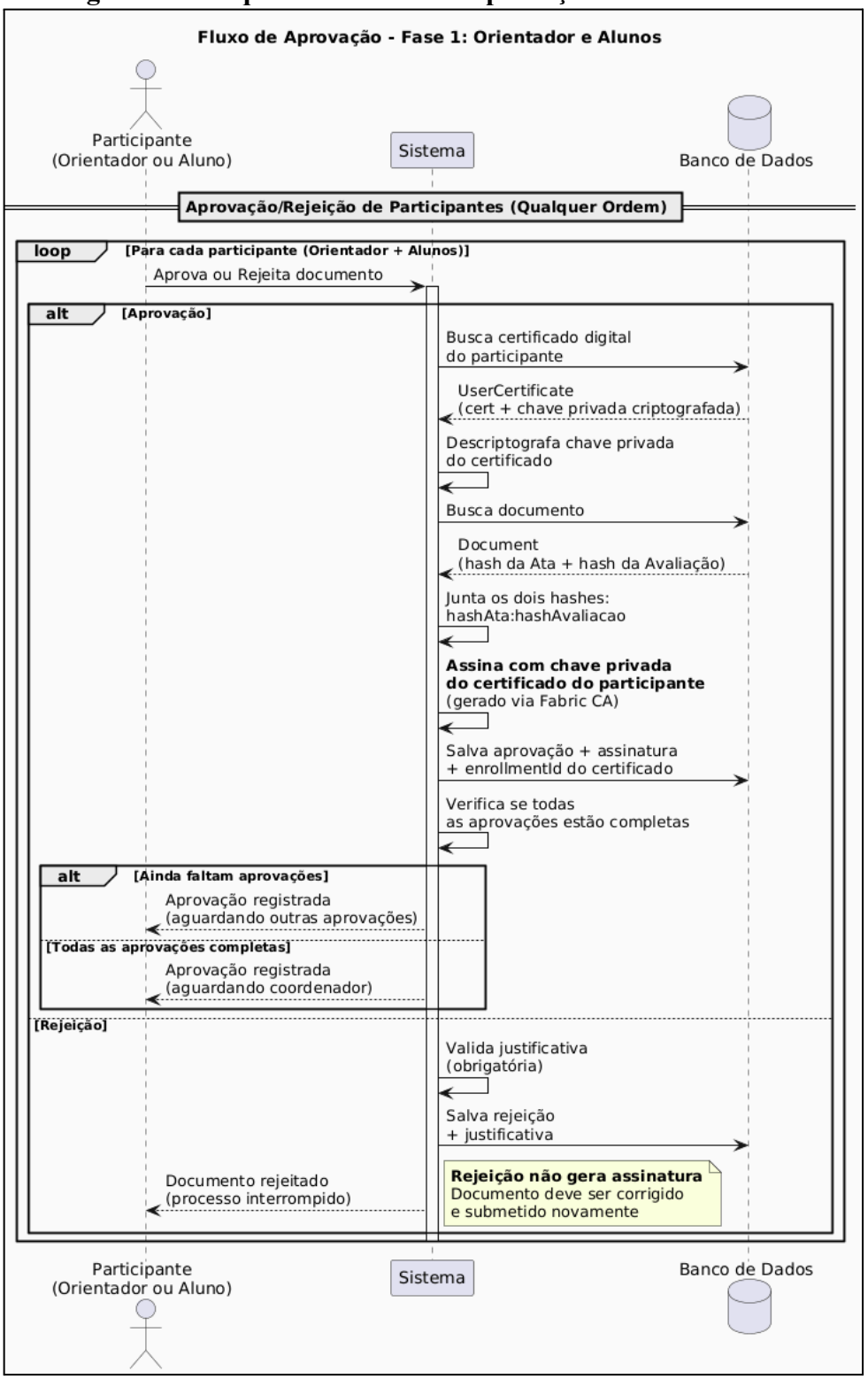
C. Registro na *Blockchain*: detalha o comportamento do processo de *endorsement* e registro na rede *blockchain*, realizado de forma automática, caracterizando o diferencial técnico da solução (Figura 18). Uma vez que esses dados são emitidos, um mecanismo de segurança entra em ação: revogação dos certificados emitidos pela CA ao sistema solicitar aprovações para os participantes.
D. Revogação de Certificados: demonstra o processo de revogação de certificados digitais após o registro definitivo dos dados na blockchain, garantindo que não haja riscos de uso indevido posteriormente. É importante ressaltar que o certificado do coordenador não é revogado, pois possui um caráter permanente (Figura 19). Uma vez que esse documento esteja registrado na ledger, ele estará apto a verificar uma cópia de referência para ser comparada posteriormente com versões armazenadas no sistema centralizado.
E. Consulta e Validação de Autenticidade: descreve o comportamento do sistema quando o usuário solicita a consulta de um documento e a validação de sua autenticidade, por meio da verificação das informações registradas na ledger (Figura 20).

Figura 15 – Diagrama de Sequência - Fluxo de Conclusão de uma Defesa



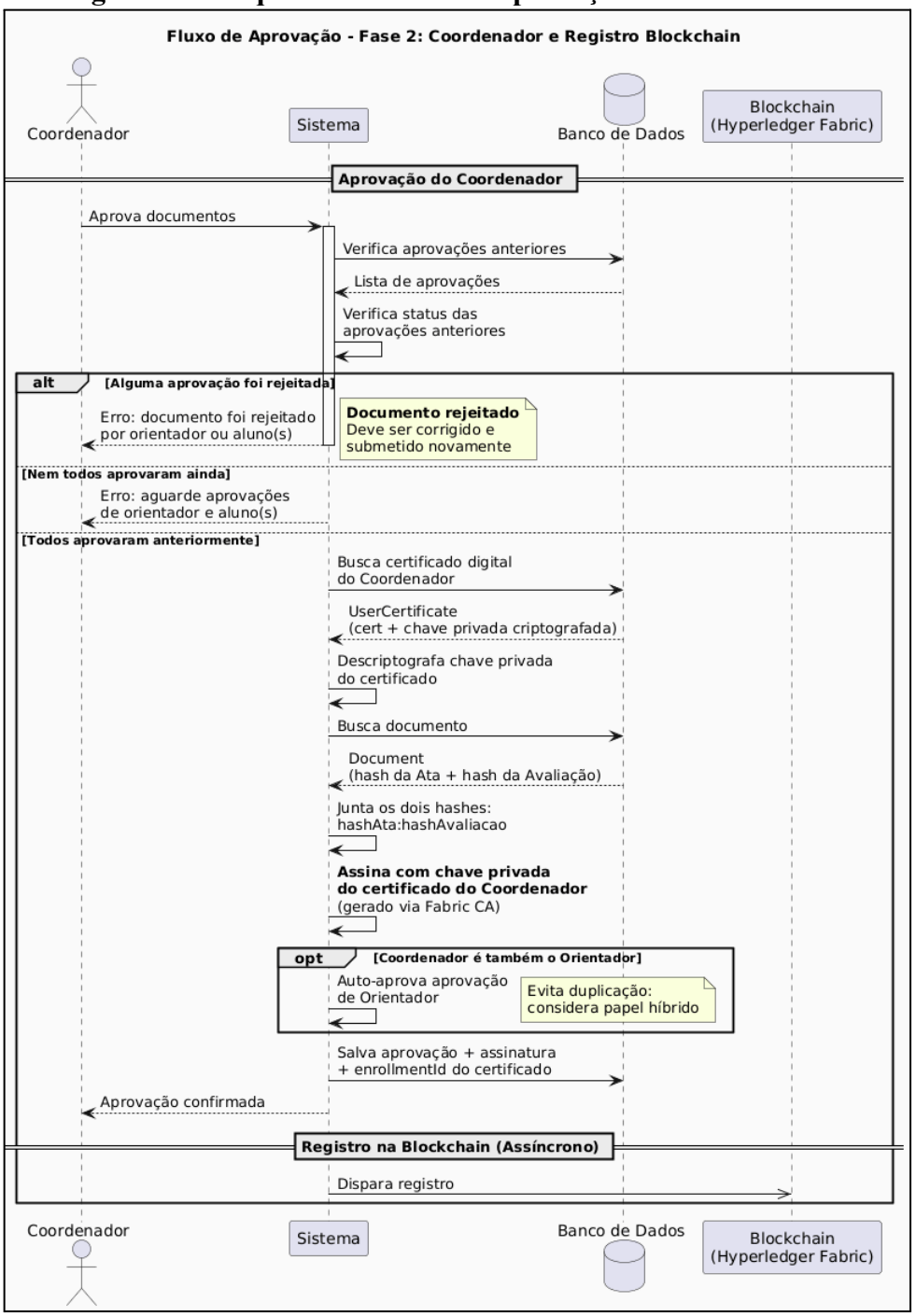
Fonte: Autoria própria.

Figura 16 – Diagrama de Sequência - Fluxo de Aprovação Orientador ou Discentes



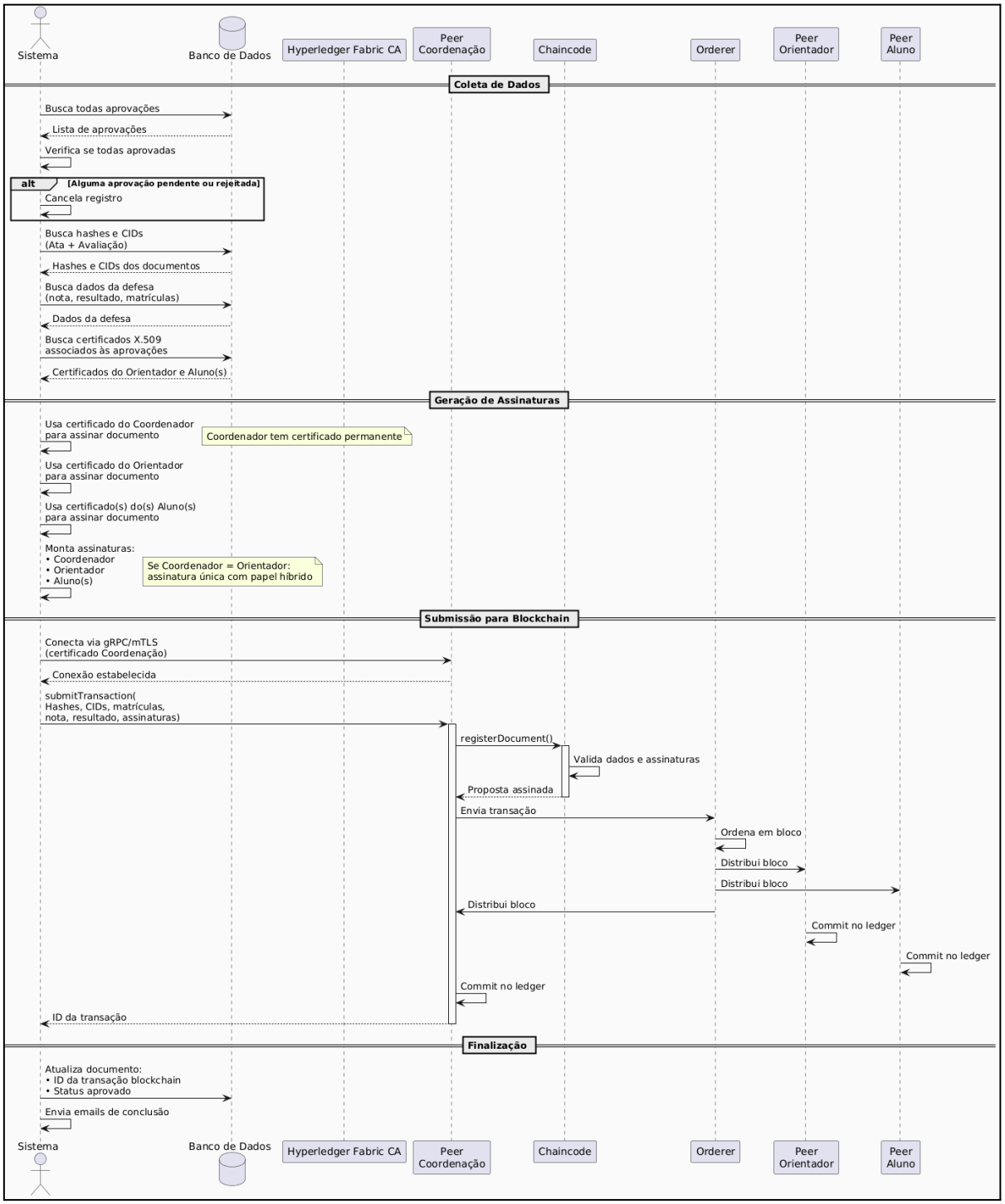
Fonte: Autoria própria.

Figura 17 – Diagrama de Sequência - Fluxo de Aprovação Coordenador



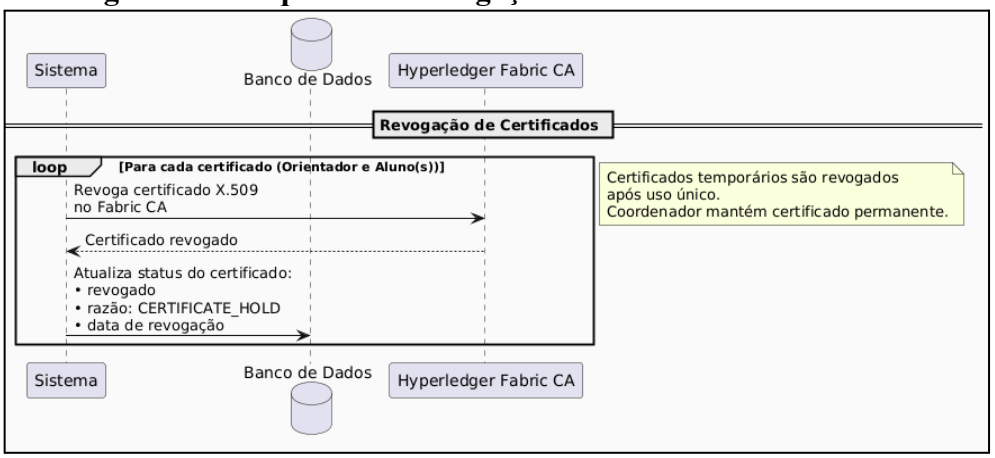
Fonte: Autoria própria.

Figura 18 – Diagrama de Sequência - Registro de Documentos na Blockchain



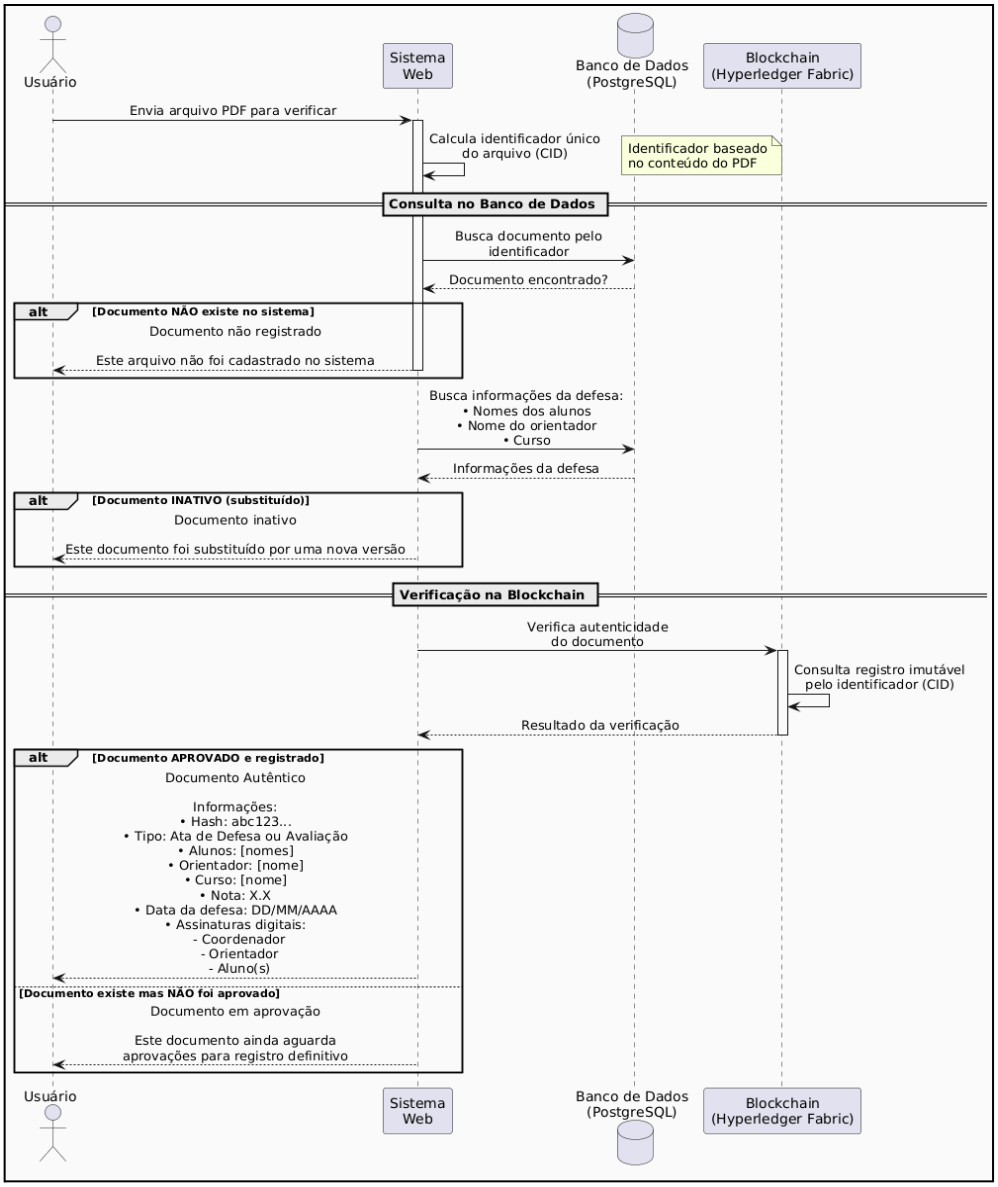
Fonte: Autoria própria.

Figura 19 – Diagrama de Sequência - Revogação de Certificados



Fonte: Autoria própria.

Figura 20 – Diagrama de Sequência - Consulta e Verificação de Autenticidade

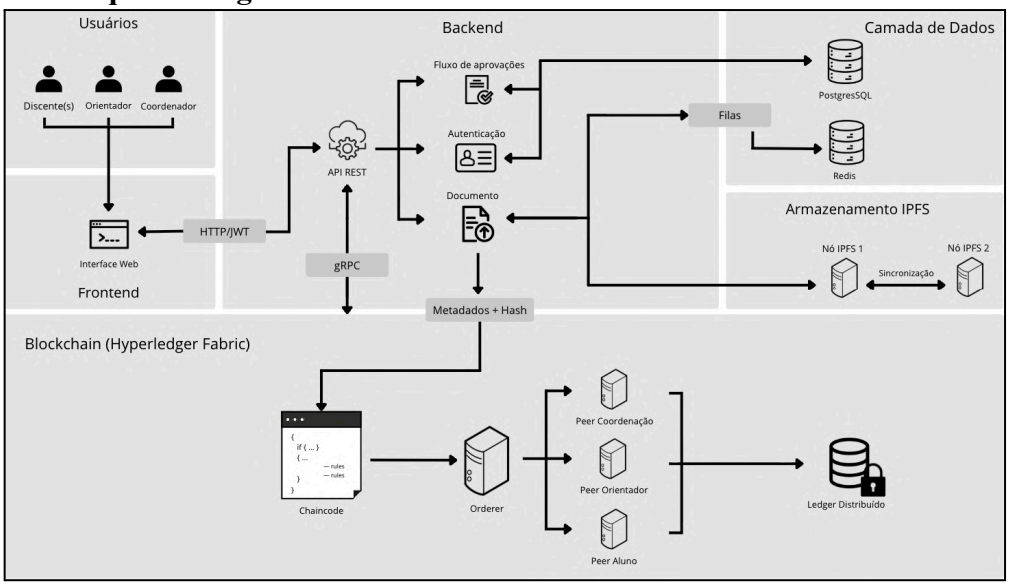


Fonte: Autoria própria.

3.3 ARQUITETURA LÓGICA DA SOLUÇÃO

A solução é organizada em cinco componentes principais: *Blockchain Hyperledger Fabric*[17], API Backend (NestJS), Armazenamento IPFS, Camada de Dados e Frontend (Next.js), que atuam de forma integrada e com responsabilidades (Quadro 6) bem definidas, permitindo uma arquitetura modular e desacoplada, conforme a Figura 21.

Figura 21 – Arquitetura geral do sistema antifraude baseado em blockchain



Fonte: Autoria própria.

Quadro 6 – Responsabilidade dos Componentes da Solução

Componente	Função
Blockchain (Hyperledger Fabric)	Rede permissionada com 3 peers representando cada papel institucional, garantindo a imutabilidade dos registros.
API Backend (NestJS)	Orquestra o fluxo de aprovação, gerencia a autenticação/autorização e integra todos os serviços.
Armazenamento IPFS.	Cluster de 2 nós para armazenamento distribuído de documentos com redundância automática.
Camada de Dados	A camada de dados é responsável por armazenar os registros mutáveis da aplicação, isso inclui todo o gerenciamento de um fluxo centralizado web2-like.
Frontend (Next.js)	Interface web responsiva com dashboards específicos por nível de usuário (aluno, orientador, coordenador, admin).

Fonte: Autoria própria.

A arquitetura híbrida em camadas, com separação de responsabilidades entre o sistema acadêmico centralizado e a rede *blockchain* distribuída, permite manter a usabilidade, o desempenho e a flexibilidade de uma aplicação web tradicional, ao mesmo tempo em que

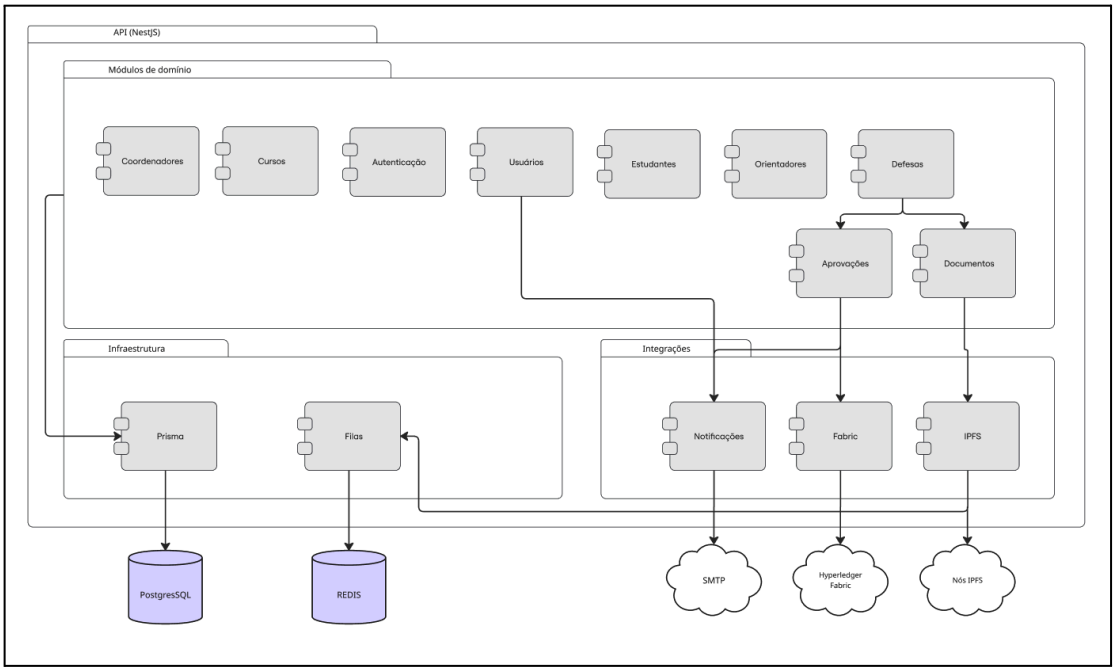
[17] https://hyperledger-fabric.readthedocs.io/en/release-2.5/

incorpora garantias relacionadas à Segurança da Informação, tais como imutabilidade, auditabilidade e verificabilidade dos registros críticos por meio da *blockchain*.

Apesar das vantagens oferecidas pela blockchain, seu uso como repositório principal para todos os dados da aplicação não é adequado para o contexto do problema apresentado neste trabalho. Isso acarretaria limitações de desempenho, maior complexidade operacional e custos, além de dificultar a atualização de informações mutáveis. Assim, os dados dos perfis de usuários, estados intermediários de fluxos de aprovação, são mantidos em um banco de dados relacional centralizado (Apêndice B), enquanto na blockchain serão registrados eventos finais e críticos do processo, como matrículas dos participantes, assinaturas, *hashes* e CIDs dos documentos e nota final; atributos esses que garantam o não repúdio uma vez que estão inseridos no *ledger*.

A *Application Programming Interface* (API) *Backend* (Figura 22 e Figura 56), desenvolvida com o framework NestJS, atua como o principal ponto de orquestração da solução, centralizando regras de negócio, gerenciando a autenticação e autorização de usuários e integrando todos os serviços que compõem a solução. Estruturada nos módulos de domínio: usuários, estudantes, orientadores, coordenadores, cursos, defesas, documentos e aprovações, essa organização favorece o desacoplamento entre responsabilidades, além de facilitar a manutenção e a escalabilidade do sistema, encontrada no Apêndice C.

Figura 22 – Arquitetura modular da API e Organização dos Domínios do Sistema

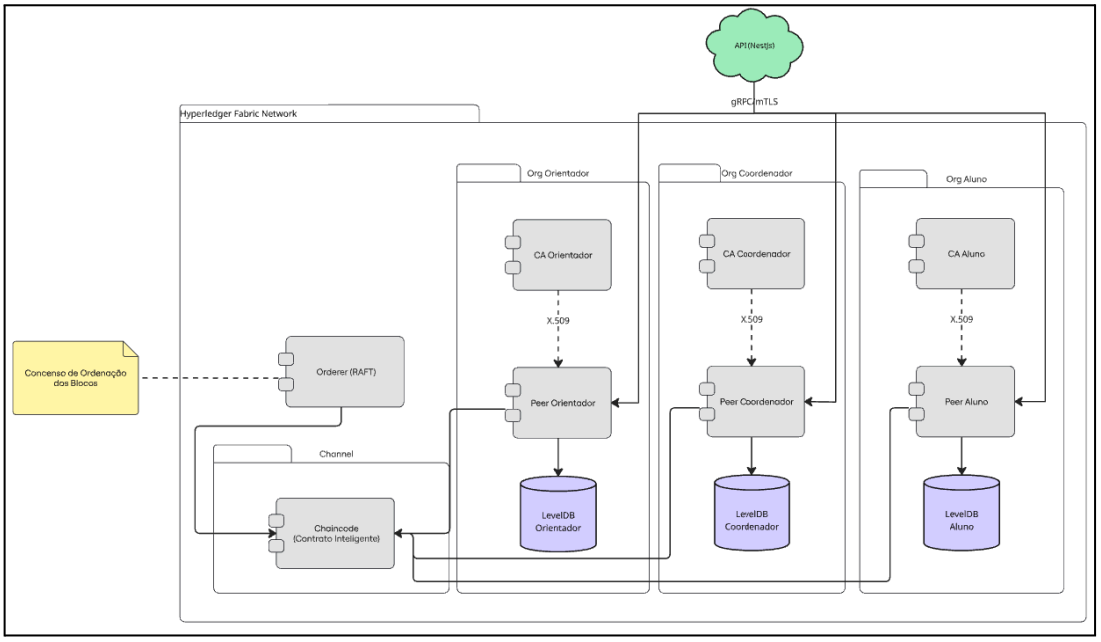


Fonte: Autoria própria.

Quanto à persistência, a API utiliza o Prisma[18] como camada de acesso aos dados dos sistemas, comunicando-se com um banco de dados PostgreSQL[19] por meio da biblioteca Prisma, responsável pelo armazenamento dos dados da aplicação. Para o processamento assíncrono de tarefas, como notificações e integrações externas, é utilizada uma camada de filas baseada em Redis. Além disso, a API também realiza integrações diretas com serviços externos, incluindo envio de notificações via *Simple Mail Transfer Protocol* (SMTP), comunicação segura com a rede *Hyperledger Fabric* e interação com a rede privada IPFS para armazenamento e recuperação de documentos.

Para a camada de blockchain (Figura 23), foi utilizado o *Hyperledger Fabric*, projetada uma rede para representar os papéis institucionais envolvidos no processo de defesa de TCC, sendo criadas as organizações: Aluno, Orientador e Coordenador, com Autoridade Certificadora (CA) própria, responsável pela emissão de certificados digitais X.509, para identificar e autenticar seus participantes. Esse modelo assegura que todas as transações na rede sejam realizadas apenas por entidades previamente autorizadas.

Figura 23 – Arquitetura da rede Hyperledger Fabric utilizada na solução proposta



Fonte: Autoria própria.

Cada organização mantém, ao menos, um peer responsável por executar o *chaincode* (contrato inteligente) e armazenar o estado do *ledger* em bancos LevelDB[20] independentes, permitindo o isolamento lógico entre as organizações, mesmo compartilhando o mesmo canal da rede.

[18] https://www.prisma.io/
[19] https://www.postgresql.org/
[20] https://github.com/google/leveldb

O consenso da rede é realizado por um serviço de ordenação baseado no protocolo RAFT, que é responsável por garantir a organização determinística das transações e a criação consistente dos blocos. O *chaincode* implementa as regras de negócio relacionadas ao *Academic Ledger*, incluindo o registro de eventos acadêmicos e a verificação de integridade por meio de hashes, assegurando que qualquer tentativa de adulteração possa ser detectada.

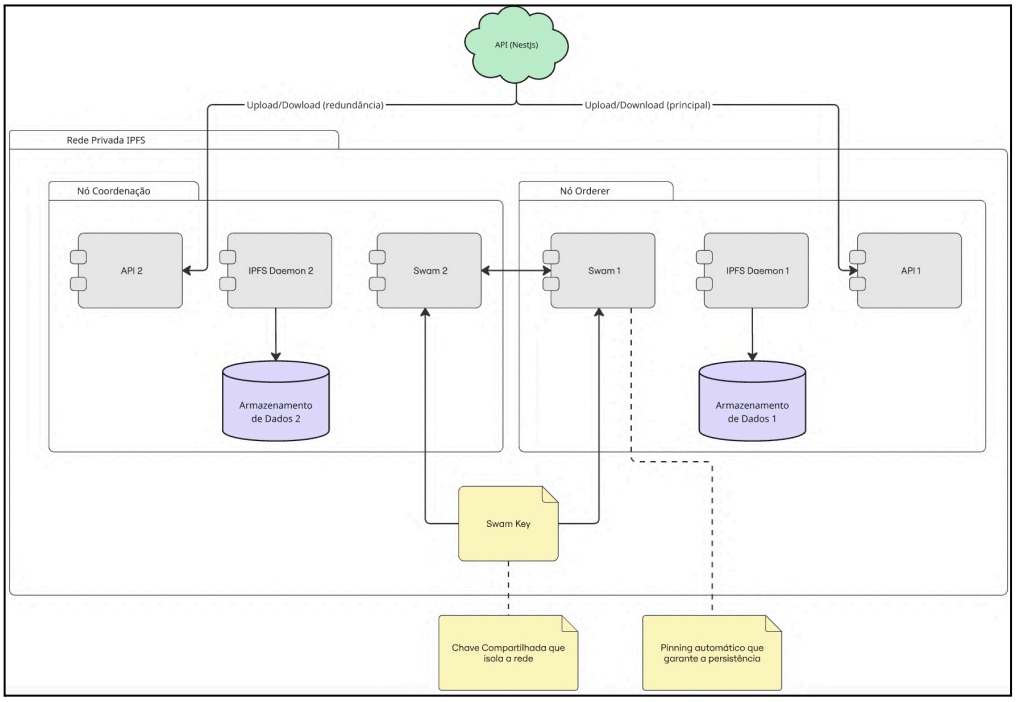
A comunicação entre a API *Backend* e a rede *Hyperledger Fabric* ocorre por meio de gRPC com mTLS, garantindo confidencialidade, autenticidade e integridade nas transações enviadas à blockchain. O acionamento da mesma se dá em momentos específicos, especialmente nas etapas finais e críticas do processo, como a submissão de resultados de defesas, validações formais e registros que exigem imutabilidade e rastreabilidade, assegurando que apenas informações consolidadas e relevantes sejam registradas de forma permanente na rede distribuída.

A rede IPFS privada é outro componente fundamental para o entendimento da solução, ela é responsável pelo armazenamento de documentos e foi projetada para garantir descentralização, redundância e persistência dos arquivos acadêmicos. Diferentemente de uma rede IPFS pública, a utilização de uma *swarm key* restringe a participação apenas aos nós autorizados, impedindo o acesso externo à rede e garantindo o isolamento da infraestrutura de armazenamento. A rede IPFS utilizada na solução é composta por dois nós principais de Ordenação e Coordenação (Figura 24). Cada nó executa um daemon IPFS próprio, associado a armazenamento local persistente, e o mecanismo de pinning automático assegura que os documentos permaneçam disponíveis mesmo em cenários de falha parcial de um dos nós.

Os documentos armazenados no IPFS são identificados por seus hashes de conteúdo (CID), que reforçam a integridade dos arquivos. Esses identificadores são utilizados como referência tanto na camada centralizada da aplicação quanto na *blockchain*, permitindo a verificação cruzada entre os dados armazenados fora da cadeia (off-chain) e os registros imutáveis registrados na blockchain (on-chain).

Embora o IPFS utilize endereçamento por conteúdo, ele não oferece mecanismos nativos de autenticação ou controle de acesso por usuário. No sistema proposto, essas responsabilidades são tratadas na camada da API *Backend*, que atua como intermediária entre os usuários e a rede IPFS, validando autenticação, autorização e permissões antes de permitir qualquer operação de upload ou download. Dessa forma, o IPFS é utilizado exclusivamente como camada de armazenamento distribuído, enquanto a segurança e o controle de acesso são centralizados na aplicação.

Figura 24 – Arquitetura do IPFS com nós distribuídos, replicação e sincronização de dados



Fonte: Autoria própria.

3.4 ARQUITETURA FÍSICA DA SOLUÇÃO

A arquitetura física descreve como os componentes lógicos do sistema são implantados em um ambiente computacional real, evidenciando a distribuição dos serviços, seus pontos de comunicação e decisões práticas de implantação. Essa visão (Figura 25) complementa a arquitetura lógica, sem repetir suas responsabilidades funcionais, focando na organização física e no isolamento entre os componentes.

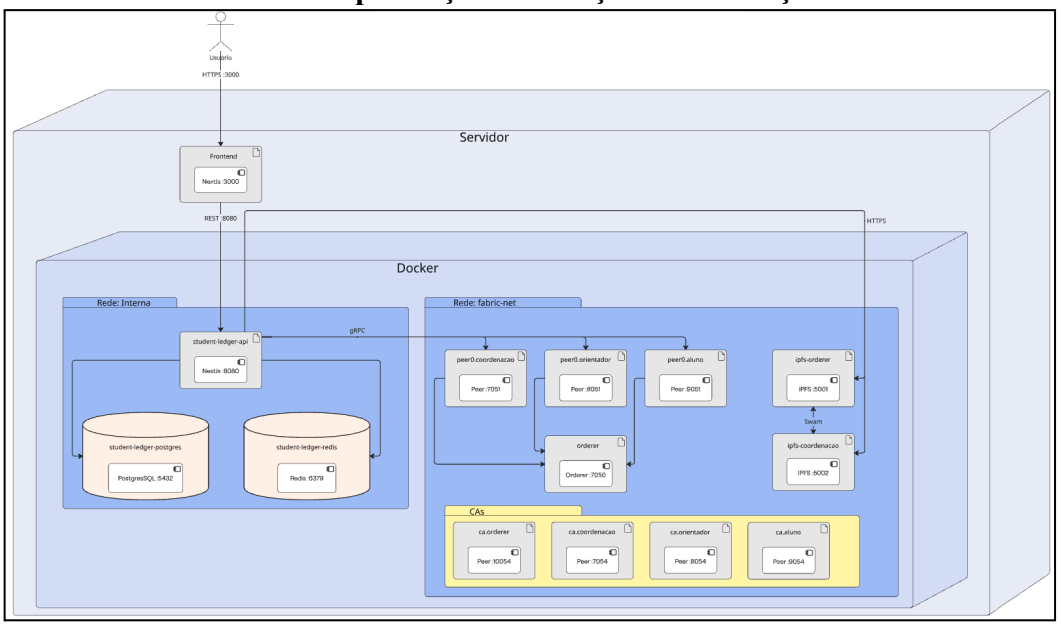
A solução é implantada em um ambiente conteinerizado, no qual a API *backend*, a camada de dados e os serviços distribuídos operam de forma independente, porém integrada. O *frontend* é acessado pelo usuário por meio do protocolo *Hypertext Transfer Protocol Secure* (HTTPS) e se comunica com a API *backend*, que atua como ponto central de orquestração entre os serviços centralizados e distribuídos.

Os serviços da rede *blockchain* no *Hyperledger Fabric*, incluindo o orderer e os peers institucionais, são implantados em contêineres dedicados e organizados em uma rede interna isolada. De forma intencional, dois nós da rede privada IPFS são implantados no mesmo servidor que o peer do coordenador e o serviço de ordenação da blockchain. Essa decisão de co-localização reduz a latência de comunicação entre os serviços distribuídos,

simplifica a gestão da infraestrutura e favorece a persistência e a redundância dos documentos armazenados.

A separação em redes internas permite isolar a comunicação entre a API, o banco de dados e os serviços distribuídos, reforçando aspectos de segurança e modularidade da solução. Essa organização física possibilita que os componentes sejam escalados ou mantidos de forma independente, sem impactar diretamente as demais camadas do sistema.

Figura 25 – Modelo físico de implantação da solução com serviços e contêineres



Fonte: Autoria própria.

3.5 AMBIENTE TECNOLÓGICO DO SISTEMA

A definição das tecnologias utilizadas no desenvolvimento do *Academic Ledger* se propôs a garantir a segurança, inovação e viabilidade tecnológica, sem prejudicar a confiabilidade e simplicidade do sistema, permitindo a manutenção, a escalabilidade e a integração entre os diferentes componentes do sistema na arquitetura lógica e física.

Além disso, também foram considerados aspectos como a curva de aprendizado, a produtividade no desenvolvimento e a ampla utilização dessas tecnologias no mercado, bem como sua constante evolução e alinhamento com práticas contemporâneas de engenharia de software. Dessa forma, o conjunto tecnológico adotado fornece suporte adequado à implementação da solução proposta, sem introduzir complexidades desnecessárias.

Diante disso, o Quadro 7 tem como objetivo apresentar uma visão geral das tecnologias utilizadas no processo de desenvolvimento do *Academic Ledger*.

Quadro 7 – Lista de Tecnologias Utilizadas

Categoria	**Tecnologia**	**Finalidade**
Linguagem de Programação	TypeScript	Linguagem principal para todos os componentes do sistema.
Framework Backend	NestJS	Framework Node.js para construção da API REST.
Framework Frontend	Next.js	Framework React para interface do usuário com SSR.
Blockchain	*Hyperledger Fabric*	Plataforma blockchain permissionada para registro imutável de certificados.
Armazenamento Distribuído	IPFS (Kubo)	Sistema de arquivos distribuído para armazenamento de documentos PDF.
Banco de Dados Relacional	PostgreSQL	Armazenamento de dados estruturados da aplicação.
ORM	Prisma	Mapeamento objeto-relacional e gerenciamento de migrações.
Cache e Filas	Redis	Sistema de cache e broker para filas de processamento assíncrono.
Fila de Tarefas	Bull	Processamento assíncrono de geração de certificados e uploads.
Autenticação	JWT + Passport	Autenticação baseada em tokens com refresh token.
Validação de Formulários	Zod + React Hook Form	Validação de schemas e gerenciamento de formulários.
Estilização	Tailwind CSS	Framework CSS utilitário para estilização responsiva.
Gerenciamento de Estado	Zustand	Gerenciamento de estado global no frontend.
Hash de Integridade	SHA-256	Cálculo de hash para verificação de integridade de documentos.
Comunicação *Blockchain*	gRPC	Protocolo de comunicação com *nodes* do *Hyperledger Fabric*.
Envio de E-mails	Nodemailer	Envio de notificações por e-mail via SMTP.
Documentação da API	Swagger/OpenAPI	Documentação interativa da API REST.
Containerização	Docker + Docker Compose	Containerização e orquestração de serviços.
Controle de Versão	Git	Versionamento de código-fonte.

Fonte: Autoria própria.

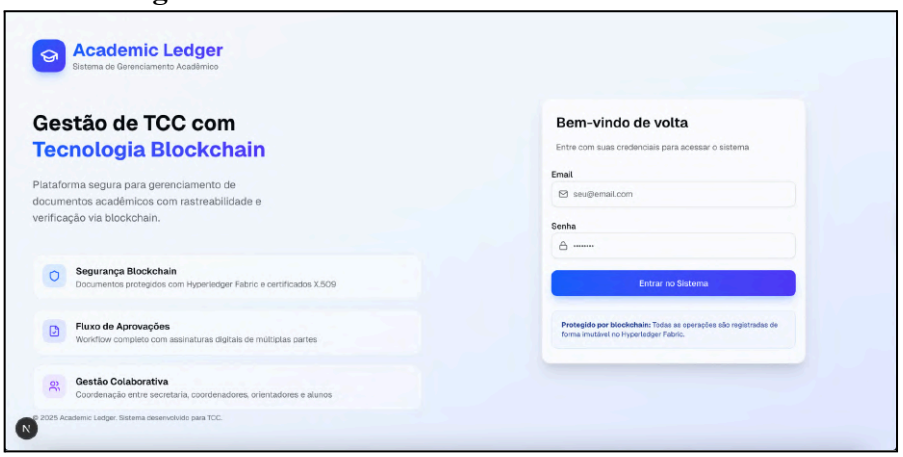
4 RESULTADOS OBTIDOS

Esta seção apresenta os resultados da implementação do *Academic Ledger*, de acordo com as principais funcionalidades desenvolvidas, funcionamento e as respectivas interfaces. Ressalta-se que foram utilizados dados fictícios para exemplificar o uso da ferramenta.

4.1 AUTENTICAÇÃO E DASHBOARDS

Ao acessar o sistema, os usuários deverão realizar o login (Figura 26) informando suas credenciais de acesso válidas. Uma vez autenticados, os usuários terão acesso aos *dashboards* e funcionalidades de acordo com o papel desempenhado no sistema.

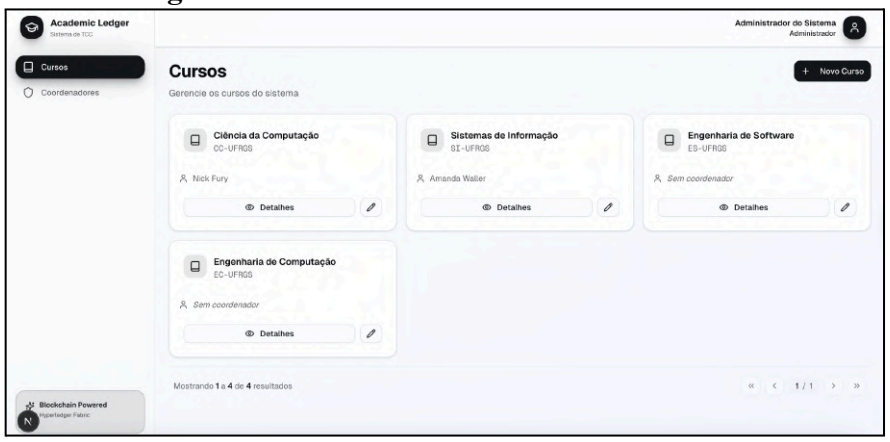
Figura 26 – Tela de Login



Fonte: Autoria própria.

No *dashboard* do usuário "administrador" (Figura 27), é possível visualizar e listar os cursos de graduação cadastrados e seus respectivos cursos já registrados. Além disso, a este usuário é permitido cadastrar um novo curso de graduação e o coordenador.

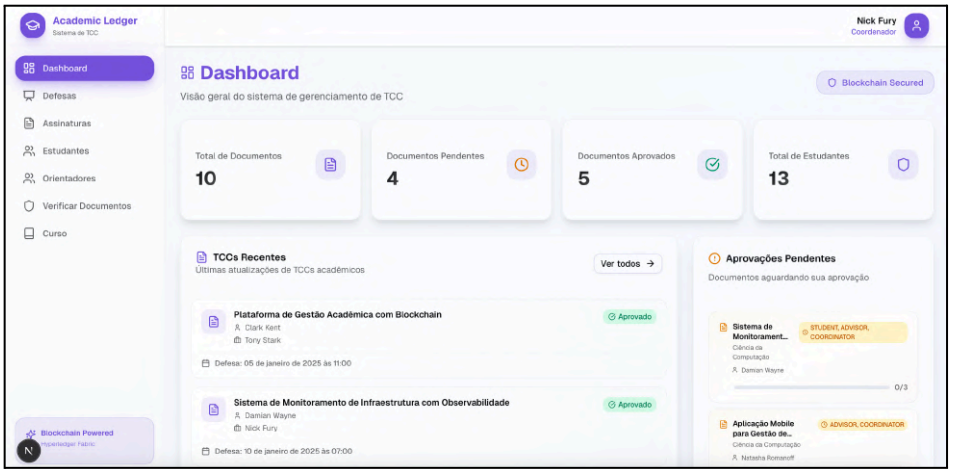
Figura 27 – Tela de listagem de cursos do sistema



Fonte: Autoria própria.

No *dashboard* do usuário “coordenador” (Figura 28), é possível ter uma visão geral dos TCC agendados para o curso vinculado ao coordenador, os documentos pendentes de assinatura, bem como ter acesso ao menu para agendamento de defesas de TCCs, cadastro de discentes, orientadores, verificar informações do curso, e documentos assinados e pendentes.

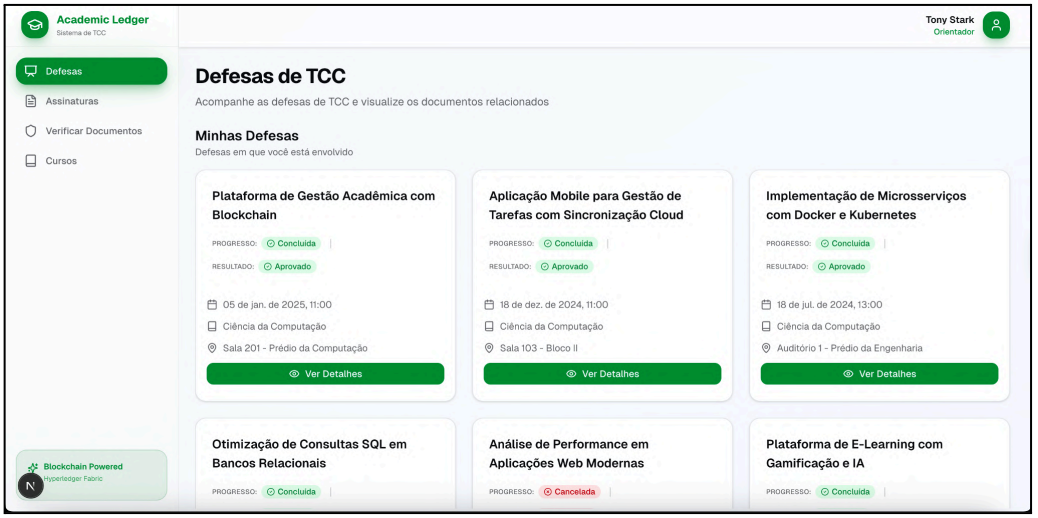
Figura 28 – Tela de dashboard do sistema



Fonte: Autoria própria.

Ao usuário do tipo “orientador” (Figura 29) é permitida a visualização das defesas agendadas sob sua orientação, bem como ter acesso aos cursos e aos documentos pendentes de sua assinatura ou assinados por ele(a).

Figura 29 – Tela de listagem de defesas de TCC



Fonte: Autoria própria.

Por fim, no *dashboard* do aluno (Figura 30), o usuário terá acesso às informações das defesas agendadas e/ou canceladas em seu nome. Além disso, também é permitido acesso à área para visualização dos documentos assinados ou pendentes de assinatura.

Figura 30 – Tela de listagem de defesas de TCC

Fonte: Autoria própria.

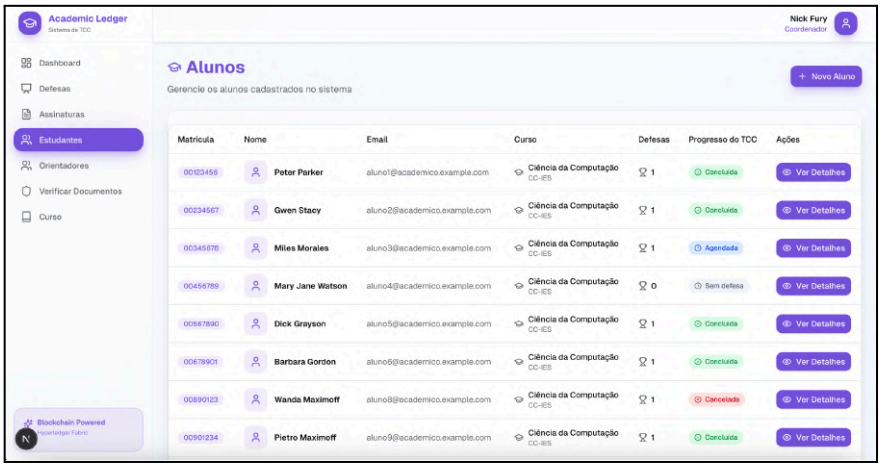
4.2 GERENCIAMENTO DE IDENTIDADES

Dada a limitação de acesso aos dados do Sistema de Informação Acadêmica utilizado pelo IFAL, foram implementadas as funcionalidades para gerenciamento dos usuários do tipo Aluno, Orientador e Coordenador de Curso.

4.2.1 Gestão de Alunos

Ao acessar o módulo de Gerenciamento de Aluno, o usuário visualiza a listagem de alunos (Figura 31), onde são exibidas informações de matrícula, nome, e-mail, curso, quantidade de defesas agendadas e o status (“Concluída”, “Agendada”, “Cancelada” ou “Sem defesa”). Essa visualização permite um acompanhamento rápido e consolidado da situação acadêmica dos estudantes vinculados a um curso de graduação.

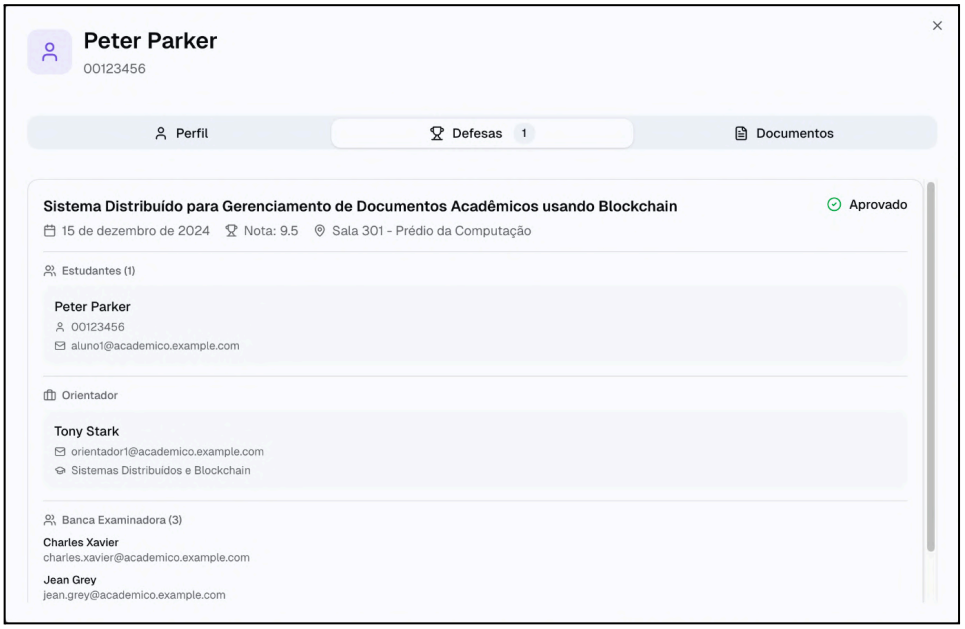
Figura 31 – Tela de Listagem de Discentes



Fonte: Autoria própria.

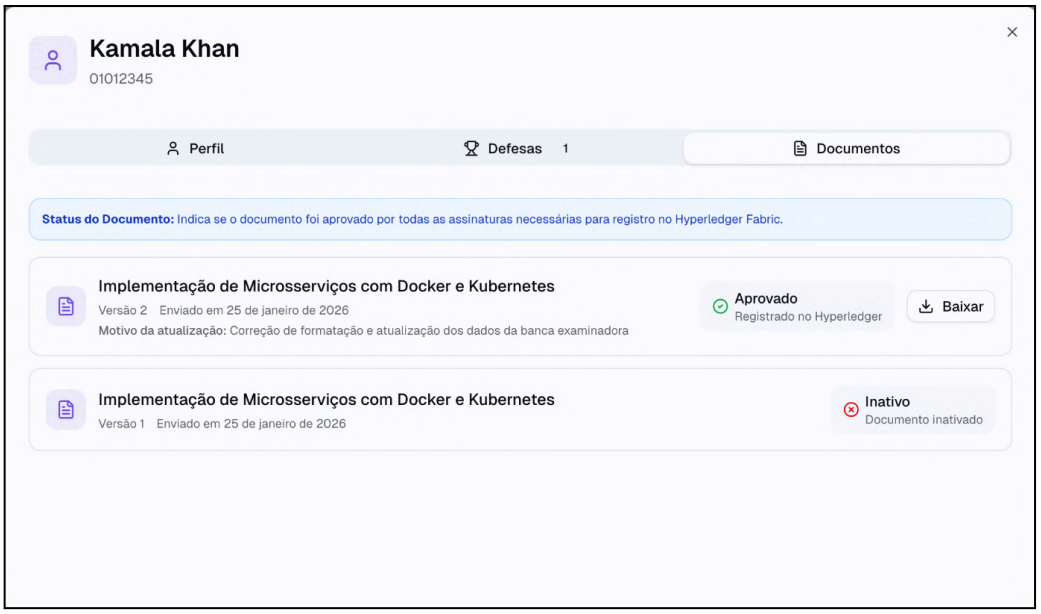
Também é possível realizar o cadastro de novos discentes, consultar e alterar informações cadastrais do discente vinculado ao curso, visualizar as informações das defesas cadastradas (Figura 32), e as informações de versionamento, estado de assinaturas e a indicação de registro dos documentos associados à defesa na blockchain (Figura 33).

Figura 32 – Detalhamento das Defesas de um Discente



Fonte: Autoria própria.

Figura 33 – Histórico de Documentos Submetidos de um Discente

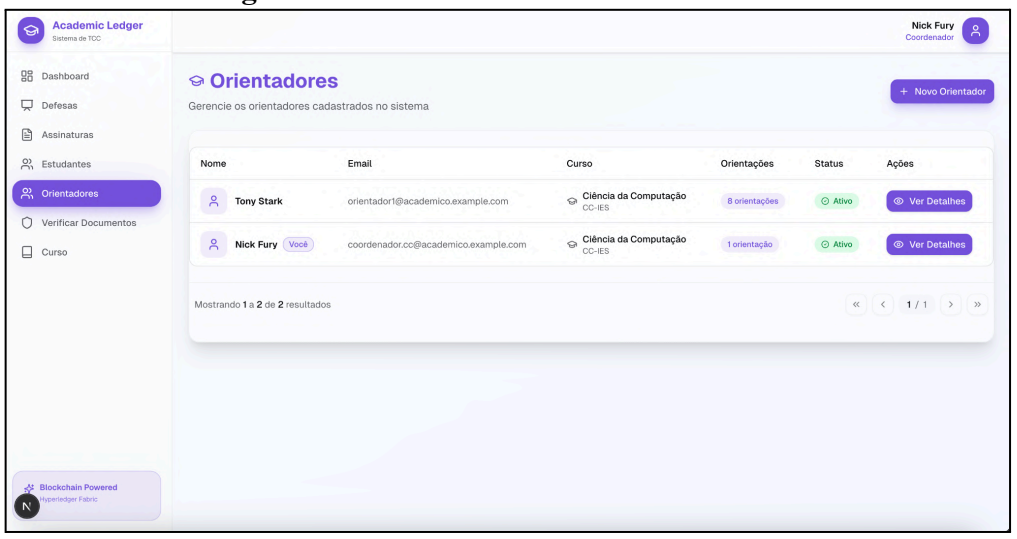


Fonte: Autoria própria.

4.2.2 Gestão de Orientadores

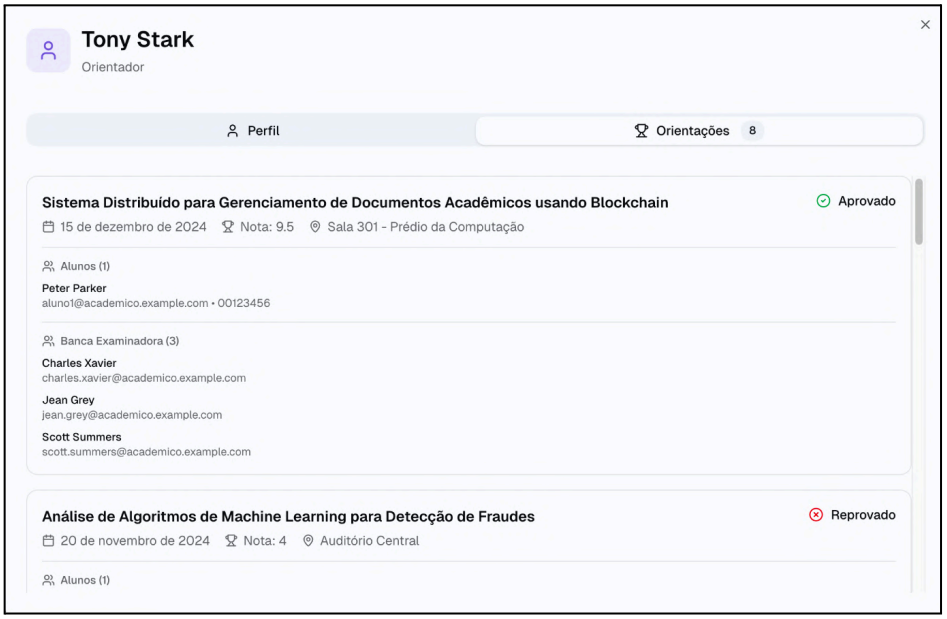
No gerenciamento de orientadores, a coordenação do curso terá acesso à listagem de orientadores vinculados ao curso, às informações pessoais de cada um, à quantidade de orientações agendadas e ao seu status atual (“Ativo” ou “Inativo”), conforme a Figura 34. Além disso, o usuário com perfil de coordenação de curso poderá cadastrar ou alterar docente orientador(a) e, a partir do detalhamento do registro do docente, acessar as informações das orientações agendadas e seus respectivos status (Figura 35).

Figura 34 – Tela de Listagem dos Orientadores



Fonte: Autoria própria.

Figura 35 – Detalhamento da Participação de Defesas de um Orientador

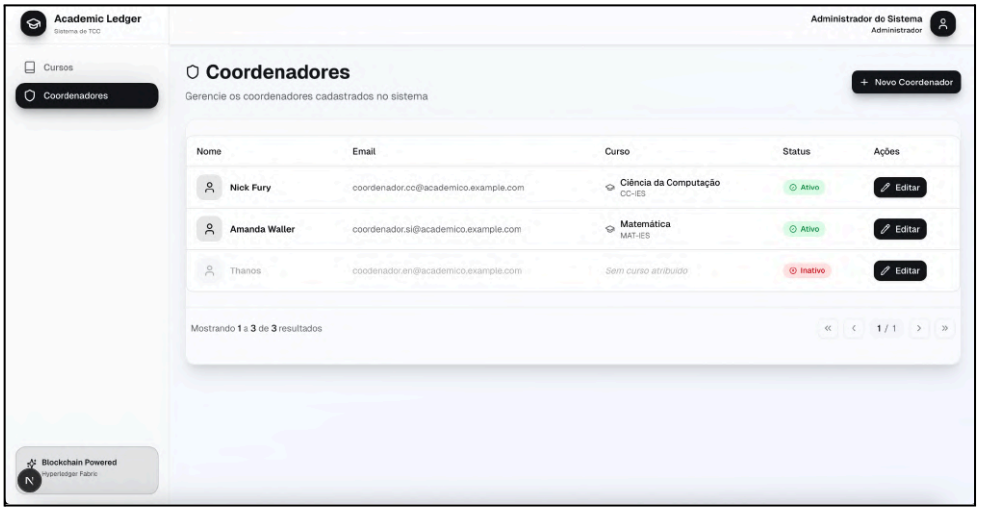


Fonte: Autoria própria.

4.2.3 Gestão de Coordenadores

O gerenciamento de coordenadores é uma funcionalidade restrita ao perfil de administrador do sistema, sendo responsável por manter a estrutura de coordenação de curso organizada e atualizada. Para isso, é permitido o cadastro, a edição e a listagem dos coordenadores de curso, conforme a Figura 36.

Figura 36 – Tela de Listagem de Coordenadores



Fonte: Autoria própria.

Dentre os dados exibidos na listagem dos usuários coordenadores, o *status* é utilizado para informar a atividade ou inatividade no sistema. Não há exclusão de registros de usuários coordenadores, apenas desativação com a remoção automática do vínculo com o curso de graduação e do acesso à plataforma.

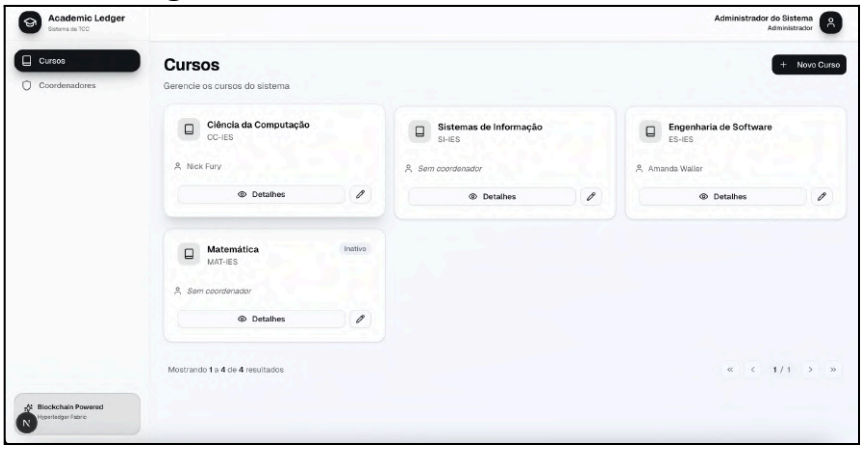
4.3 GESTÃO DE CURSOS

O módulo de gerenciamento de cursos, de acesso exclusivo dos usuários do tipo "Administrador", concentra as informações relacionadas aos cursos de graduação cadastrados no sistema. No dashboard, cada curso é apresentado no formato de cartões individuais, identificado por seu nome, código institucional, status ("ativo" ou "inativo") e coordenador responsável (Figura 37).

A partir dessa visualização, é possível cadastrar novos cursos de graduação, editar os cursos já cadastrados e visualizar as informações cadastrais, tais como: nome, código, coordenador associado e datas de criação e/ou atualização dos registros (Figura 38). Ressalta-se que na edição é permitido alterar o nome e o status do curso, mantendo o código como um identificador fixo imutável. Não há exclusão de cursos de graduação, apenas a

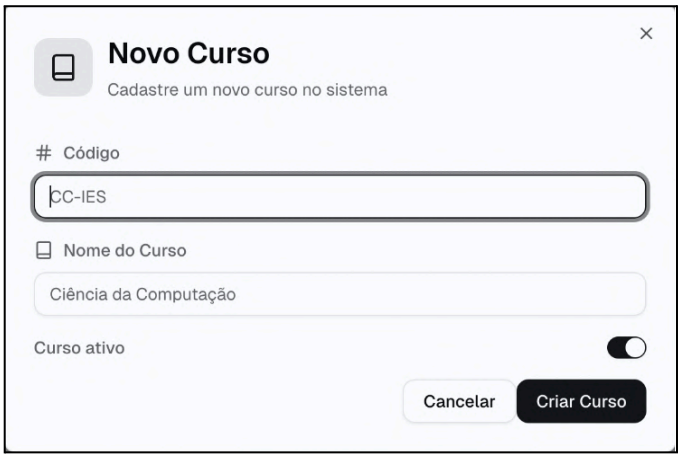
“desativação” que impede seu uso nos demais fluxos do sistema, preservando a integridade das operações acadêmicas (Figura 39).

Figura 37 – Tela de Listagem de Todos os Cursos



Fonte: Autoria própria.

Figura 38 – Interface do Fluxo de Criação de um Curso



Fonte: Autoria própria.

Figura 39 – Interface de Edição de um Curso Específico

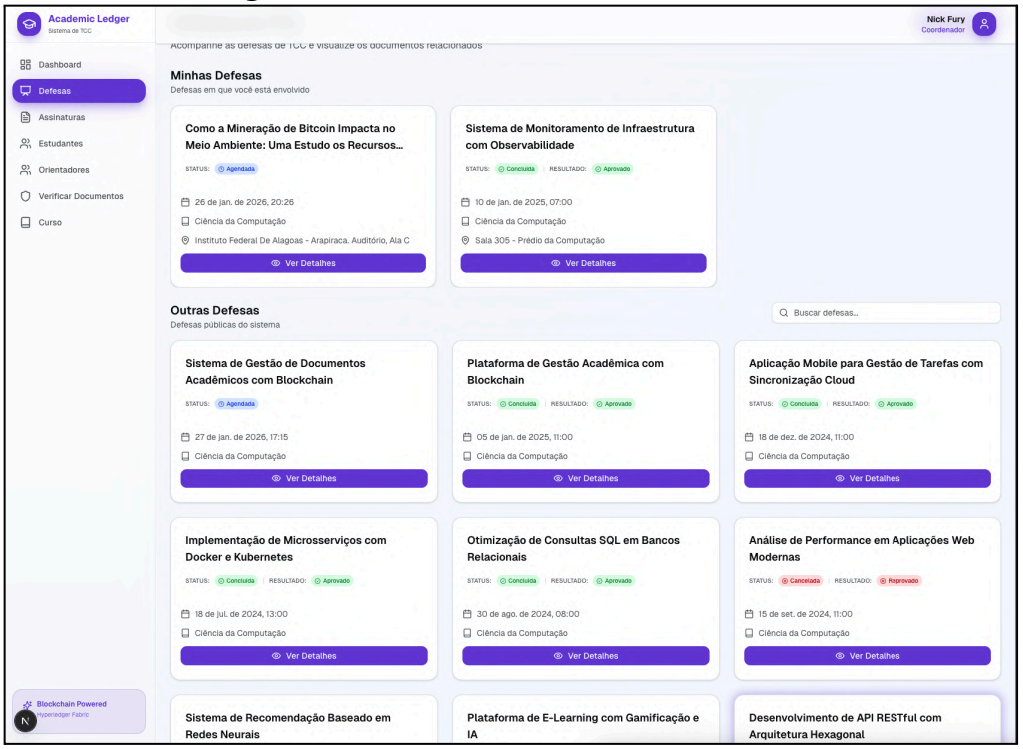
Fonte: Autoria própria.

4.4 GESTÃO DE DEFESAS

O Gerenciamento de Defesas de TCC é responsável pelo agendamento, reagendamento e cancelamento de defesa. Tais ações são realizadas apenas pelos usuários com perfil “Coordenador”.

A interface do módulo de Gerenciamento de Defesas (Figura 40) reúne os registros de TCC agendados organizados em dois blocos principais: o primeiro apresenta as defesas nas quais o usuário está diretamente envolvido, enquanto o segundo exibe as demais defesas públicas disponíveis para consulta. Cada cartão visual da defesa agendada contém as informações do título do trabalho, curso, data e horário, local, status de progresso, e resultado final (“Aprovado” ou “Reprovado”), permitindo uma visualização ágil do andamento das defesas.

Figura 40 – Tela de Listagem de Defesas



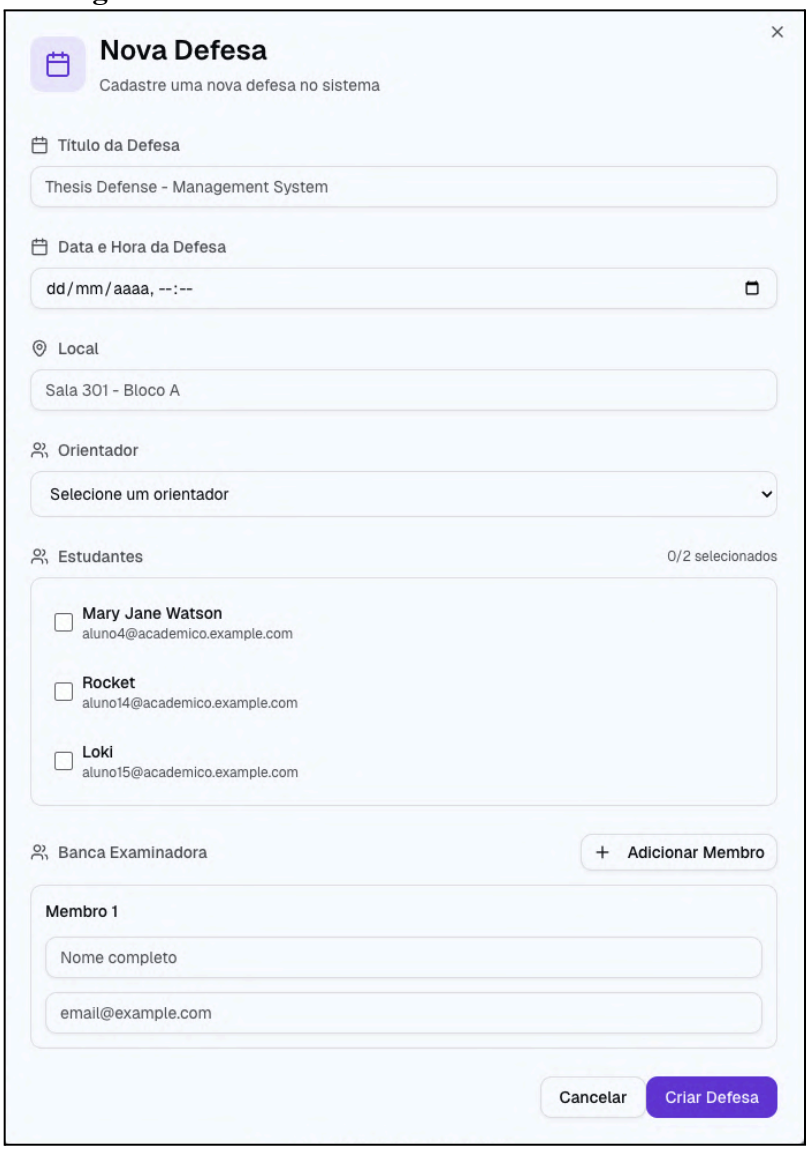
Fonte: Autoria própria.

A partir da listagem das defesas agendadas, o usuário Coordenador pode agendar uma nova defesa de TCC. Para isso, deve ser informado o título do trabalho, data e horário da apresentação, local, orientador responsável, estudantes envolvidos e os membros da banca examinadora. No agendamento, o orientador e os estudantes serão selecionados a partir dos registros previamente cadastrados, conforme a Figura 41.

Também é disponibilizada uma área dedicada à visualização individual das defesas de TCC. Ao clicar em “Ver detalhes”, a solução exibe as informações acadêmicas e

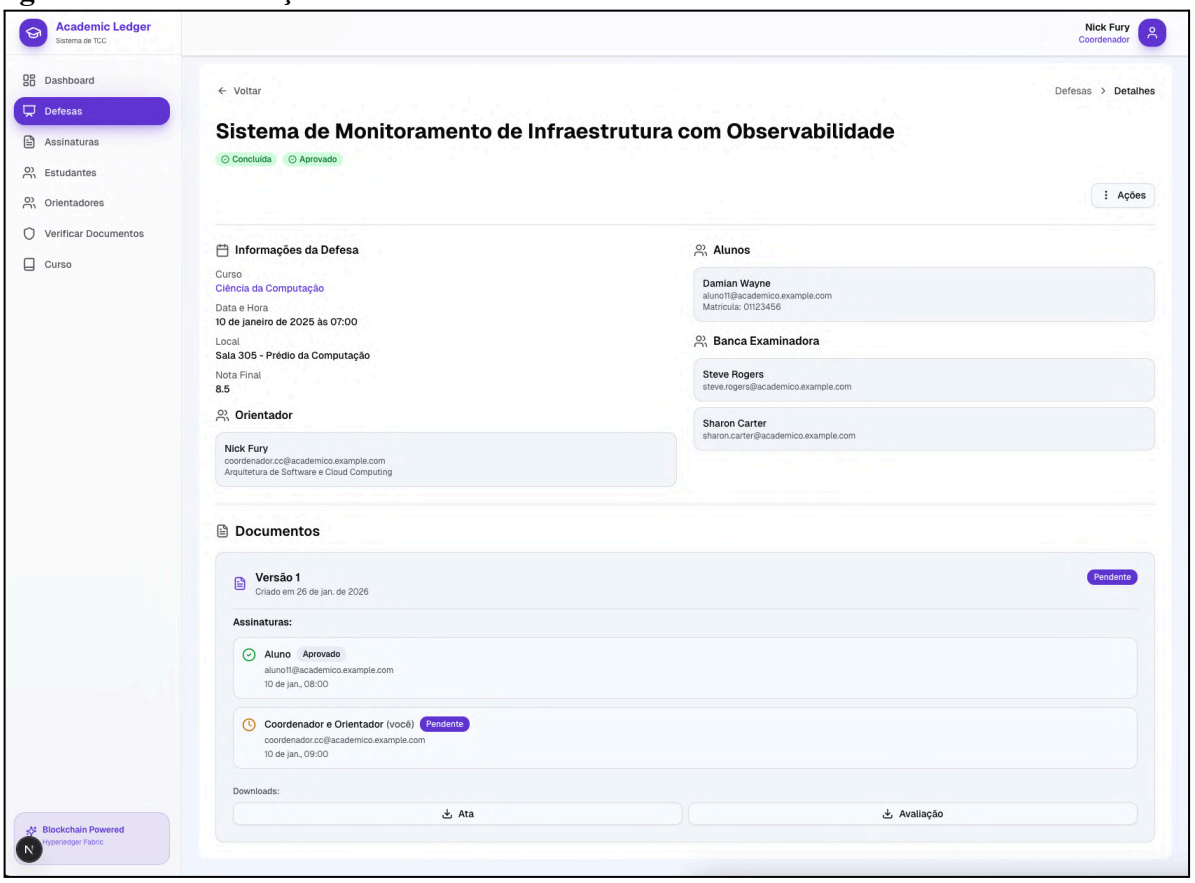
documentais das defesas, apresentando, além dos dados de cadastro, o resultado final do TCC e o versionamento dos documentos “Ata de Defesa” e “Ficha de Avaliação”, exigidos pela portaria 1483, e que devem ser anexados ao registro de TCC durante o processo de “Finalização de TCC”, conforme a Figura 42. Também é possível fazer o download dos documentos anexados ao agendamento.

Figura 41 – Tela de Agendamento de nova Defesa de TCC



Fonte: Autoria própria.

Figura 42 – Visualização Detalhada da Defesa de TCC



Fonte: Autoria própria.

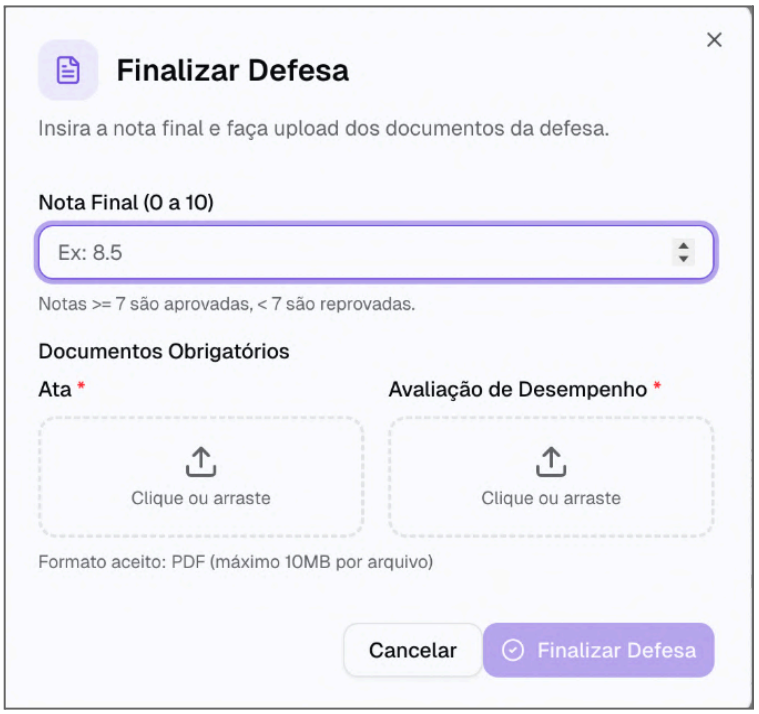
Quanto às funcionalidades de reagendamento ou cancelamento de defesas de TCC, estas estão localizadas no menu “ações” da tela de gerenciamento da defesa. É importante destacar que essas opções estão disponíveis caso o TCC agendado ainda não tenha acontecido. Para o reagendamento ou cancelamento, são necessárias algumas informações obrigatórias: nova data da defesa e também o motivo, em caso de reagendamento; justificativa, em caso de cancelamento, à ação de cancelamento é irreversível, sendo apresentado no resultado da defesa o status “reprovado”, e a mesma não será registrada no ledger do *Hyperledger Fabric*.

Conforme já mencionado, na finalização do TCC faz-se necessário a gestão dos documentos “Ata de Defesa” e “Ficha de Avaliação”, conforme a portaria do IFAL. Na solução, essas documentações devem ser submetidas, pelo usuário Coordenador, por meio da funcionalidade de “Finalizar Defesa”, conforme a Figura 44. A partir desse momento, a defesa passa a constar como concluída no sistema, com seus dados registrados para as etapas seguintes de validação.

Figura 43 – Visualização Detalhada da Defesa de TCC

Fonte: Autoria própria.

Figura 44 – Interface de Conclusão de uma Defesa



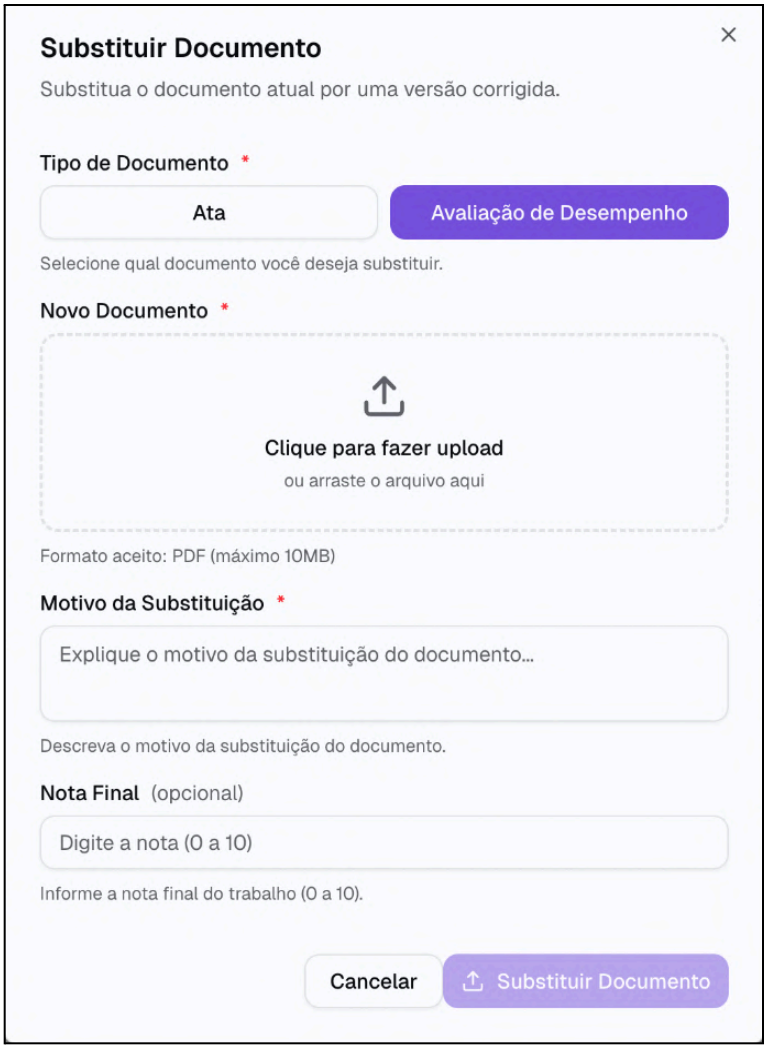
Fonte: Autoria própria.

Ao usuário, é permitida a substituição de documentos já existentes por meio de uma interface específica (Figura 45) para envio de nova versão. Nela, o usuário coordenador indica qual o documento deve ser atualizado, anexa o novo arquivo e descreve o motivo da alteração. Essa informação passa a compor o histórico do documento, registrando o contexto da mudança realizada. Caso o documento substituído não tenha sido enviado à blockchain, a nova submissão substitui a versão anterior no banco de dados. Nessa situação, todas as

aprovações previamente concedidas são invalidadas, exigindo nova validação dos envolvidos, assegurando que a análise recaia sempre sobre o conteúdo atualizado.

Não é permitida a substituição direta de documentação aprovada e registrada na *blockchain*. Nesses casos, o sistema cria automaticamente uma nova versão do documento, preservando a versão anterior de forma imutável. A nova versão do documento passa novamente pelo processo de avaliação e assinatura (de aprovação), sem alterar os registros anteriores. As versões já consolidadas permanecem disponíveis, formando um histórico contínuo das alterações realizadas.

Figura 45 – Interface de Substituição de um Documento de TCC



Fonte: Autoria própria.

4.5 GESTÃO DE APROVAÇÕES

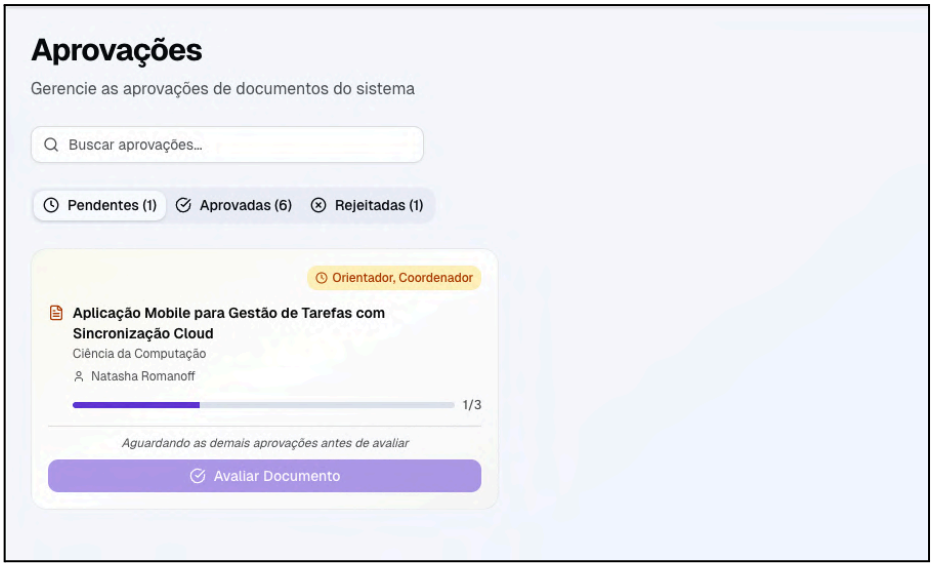
Após uma submissão de documentos, uma solicitação de aprovação de documentos é criada. Essa solicitação é refletida na “Tela de Aprovações”, conforme a Figura

46. A partir dessa visualização, o avaliador consegue identificar com facilidade quais documentos ainda exigem sua avaliação.

Os documentos são classificados em 3 estados principais: “pendente”, “aprovado” e “rejeitado”, os quais representam as etapas do fluxo de validação. Durante esse processo, o estado do documento é atualizado de forma automática mediante as avaliações dos participantes da defesa, no qual o documento foi inserido. Caso ocorra uma rejeição em qualquer etapa, o documento é imediatamente direcionado para a aba de rejeitados, independentemente das aprovações anteriores.

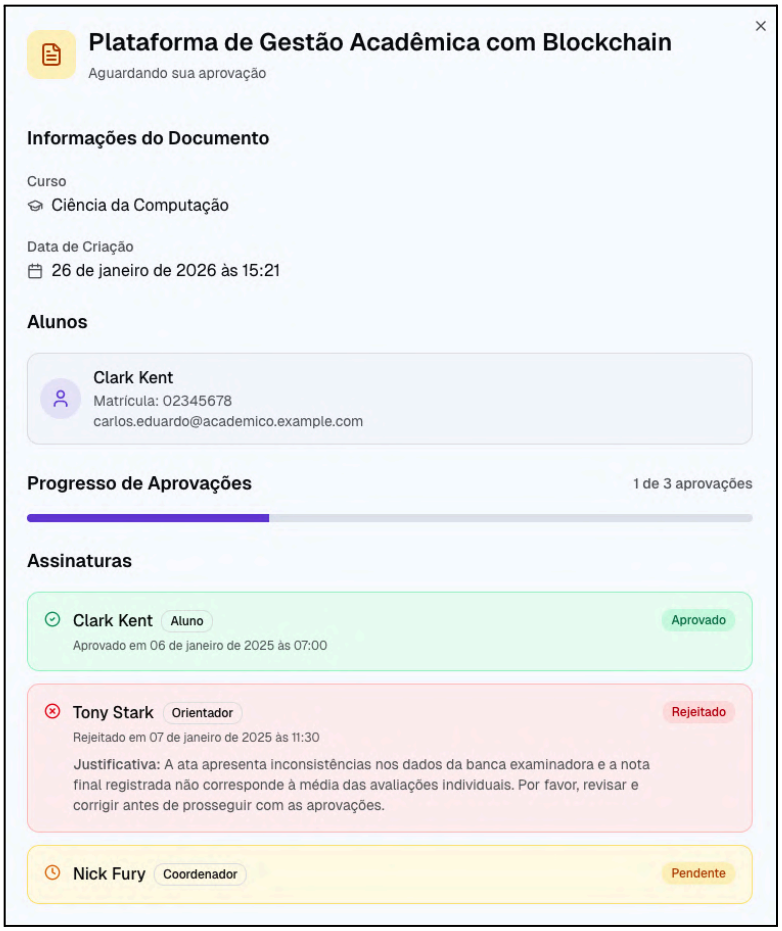
Além da listagem de assinaturas pendentes, o sistema permite a visualização detalhada do processo de aprovação documental, apresentada na Figura 47. Essa interface possibilita o acompanhamento granular. Nessa interface, é possível visualizar informações como o estudante vinculado, o curso, o TCC associado e o histórico de assinaturas, incluindo quem já realizou a validação e o respectivo status de cada participante.

Figura 46 – Visualização de Listagem de Aprovações Pendentes



Fonte: Autoria própria.

Figura 47 – Visualização Detalhada de um Processo de Aprovação Documental

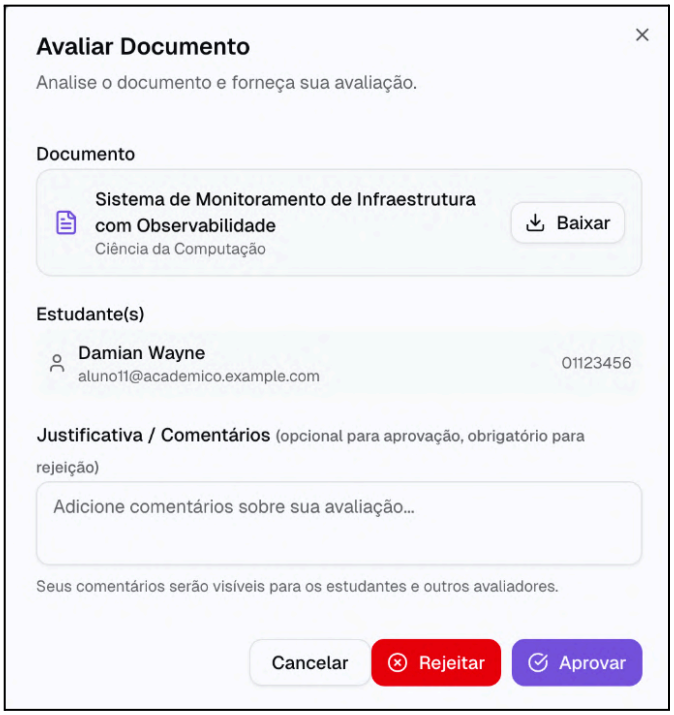


Fonte: Autoria própria.

Na aba dependentes, os avaliadores podem acompanhar o progresso das assinaturas, conforme apresentado na Figura 46. Os orientadores e demais membros da banca podem aprovar o documento a qualquer momento. No entanto, o coordenador, por sua vez, possui uma regra específica: sua ação de aprovação ou rejeição somente é liberada quando ele for o último avaliador restante no fluxo, assegurando que todas as demais validações sejam realizadas previamente.

Para avaliar um documento, o usuário deve acessar esta aprovação pendente. Nesta visão (Figura 48), são exibidas as principais informações do arquivo, sendo possível realizar o download do documento para análise, bem como aprová-lo para posterior registro na blockchain ou rejeitá-lo. Em caso de rejeição, o sistema exige o preenchimento de uma justificativa, a qual fica associada ao documento e pode ser consultada pelos demais participantes do processo.

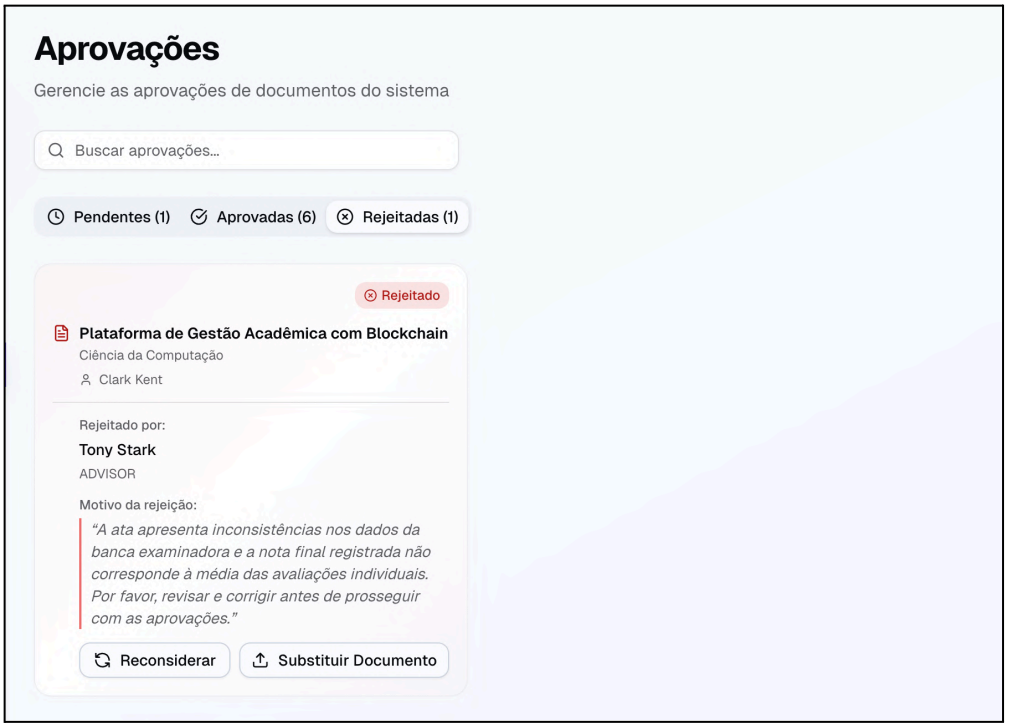
Figura 48 – Interface de Avaliação de um Documento



Fonte: Autoria própria.

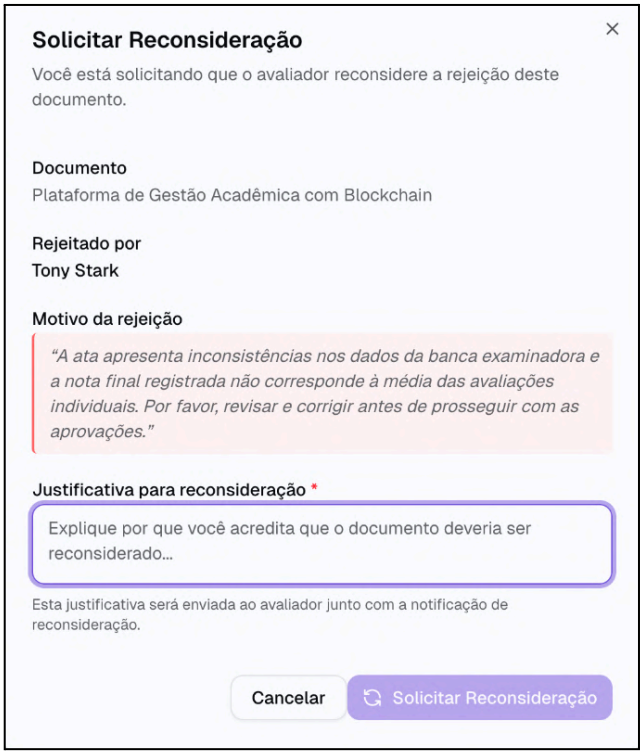
Quando um documento é direcionado para a aba de rejeitados (Figura 50), o coordenador, e apenas ele, deve avaliar se a solicitação de rejeição é válida ou, por algum motivo, o participante que solicitou se encontra equivocado. Neste cenário, é preciso que o coordenador solicite uma reconsideração na avaliação, conforme representado pela Figura 51. Em anexo, o coordenador também deve expor a razão para tal evento, possibilitando que o avaliador reavalie o documento com base nas novas informações apresentadas.

Figura 50 – Listagem de Avaliações Rejeitadas



Fonte: Autoria própria.

Figura 51 – Interface de Solicitação de Reconsideração de uma Avaliação



Fonte: Autoria própria.

Alternativamente, na interface da Figura 45, é possível substituir o documento por uma nova versão corrigida, caso a rejeição pelos participantes seja concedida. O coordenador deve substituir o documento com as devidas correções caso considere o motivo da rejeição

plausível e, assim, o documento passa novamente pelo fluxo de avaliação de todos os participantes envolvidos.

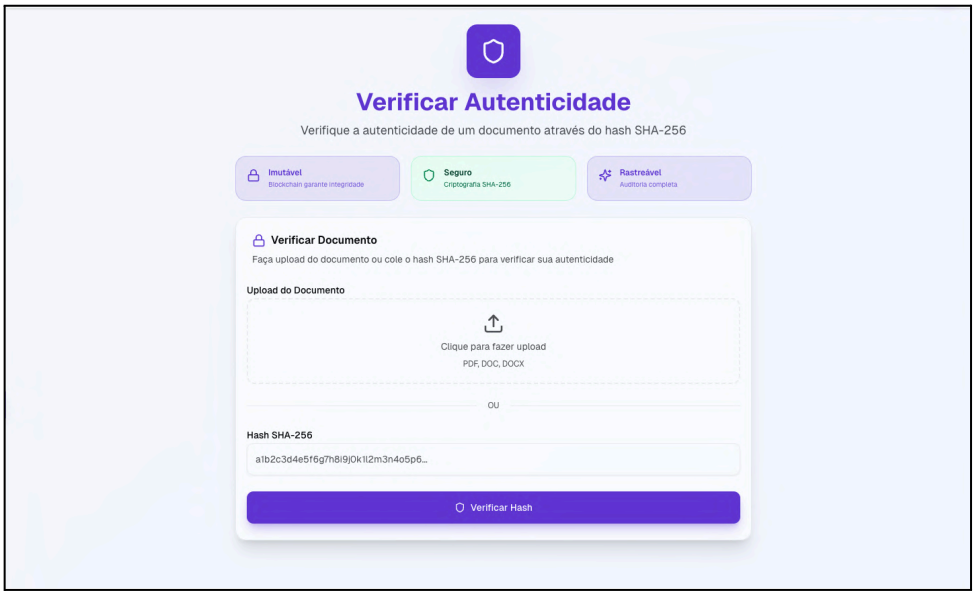
Por fim, após a conclusão de todas as avaliações, o documento é automaticamente transferido para a aba de aprovados, indicando que o processo de validação foi finalizado e que não há mais pendências associadas ao documento.

4.6 CONSULTA E VERIFICAÇÃO DE AUTENTICIDADE

A autenticidade dos documentos é verificada por meio de uma interface na qual o usuário pode confirmar a legitimidade de um documento utilizando o algoritmo SHA-256, garantindo a integridade dos dados, conforme a Figura 52.

Esse processo pode ser realizado de duas formas: upload do documento, permitindo a geração automática do hash; ou inserção manual do hash SHA-256 no local correspondente. Após isso, o usuário deve acionar a verificação para conferir se a cópia inserida corresponde ao documento registrado no processo de uma defesa.

Figura 52 – Tela de Verificação de Autenticidade de um Documento



Fonte: Autoria própria.

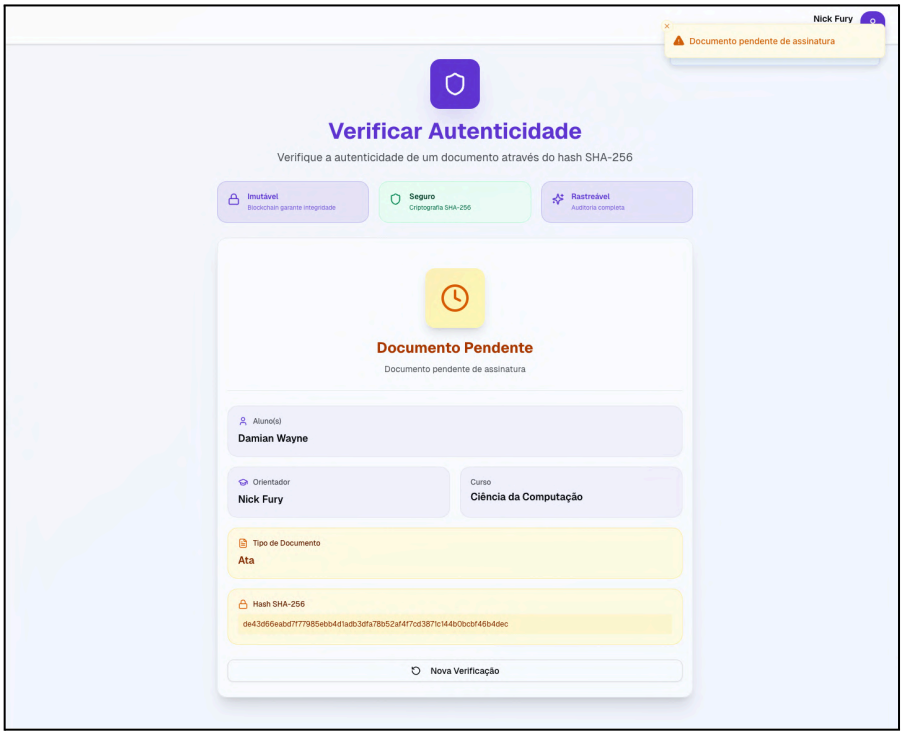
Caso o documento ou *hash* informado não corresponda a nenhum registro existente no sistema, é retornada a mensagem "Documento não encontrado no sistema", indicando que o arquivo não foi registrado ou a cópia inserida sofreu alguma modificação em relação à versão original.

Caso o arquivo consultado seja localizado no sistema, mas ainda não possua todas as aprovações necessárias, a verificação retorna a mensagem "Documento pendente de Assinatura", indicando que o arquivo foi registrado, porém o processo de assinaturas ainda

não foi concluído, conforme a Figura 53. Como resultado da verificação, são exibidas as informações associadas ao documento, a defesa envolvida, os participantes associados e também o andamento do processo de aprovação dos documentos. Enquanto houver assinaturas pendentes, o documento permanece nesse estado, sinalizando que a autenticação definitiva ainda depende da conclusão do fluxo de avaliações previsto pelo sistema.

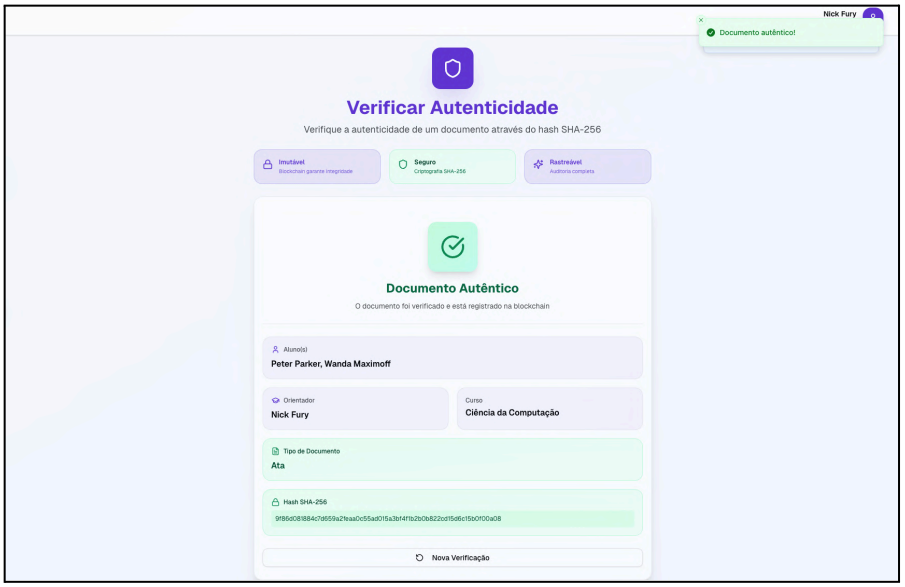
Uma vez que o documento esteja aprovado por todos os participantes envolvidos e ele também esteja escrito na blockchain, será possível conferir a autenticidade da cópia do documento. Em caso de sucesso, a verificação retorna a mensagem “Documento Validado”, indicando que a cópia que foi inserida, é a mesma que está registrada no ledger, conforme a Figura 54.

Figura 53 – Tela de Verificação de Autenticidade de um Documento



Fonte: Autoria própria.

Figura 54 – Tela de Verificação de Autenticidade de um Documento



Fonte: Autoria própria.

4.7 VALIDAÇÃO DA SOLUÇÃO

Com o objetivo de verificar a robustez, a confiabilidade e a adequação da plataforma ao contexto acadêmico, foram realizados testes funcionais, estruturais e de desempenho.

A análise dos resultados, exibidos no Apêndice D, foi baseada no conceito do Trilema da Blockchain, considerando os três pilares que o compõem: segurança, descentralização e escalabilidade. Essa abordagem permitiu avaliar não apenas se o sistema funciona corretamente, mas também quais decisões arquiteturais foram adotadas e quais limitações foram assumidas no projeto.

Os testes foram executados em uma rede blockchain privada baseada no Hyperledger Fabric, composta por três organizações independentes: Coordenação, Orientação e Aluno.

A validação envolveu:

- Testes de integridade criptográfica.
- Testes de controle de acesso e políticas de endosso.
- Testes de tolerância a falhas.
- Testes de desempenho (latência).

Os testes de integridade criptográfica tiveram como objetivo verificar se o sistema impede o registro, a alteração e a validação de documentos que não atendem aos requisitos de segurança da plataforma. A validação realizada no nível do *chaincode* do *Academic Ledger*,

responsável por aplicar as regras de negócio antes da gravação das transações na *blockchain,* demonstraram um resultado satisfatório (Quadro 8).

Inicialmente, foi testada a verificação de um hash inexistente no ledger. Em seguida, tentativas de registro com *hashes* fora do padrão SHA-256 e com CIDs.

Também foram realizados testes de imutabilidade, nos quais um documento válido foi registrado e, posteriormente, uma nova tentativa de registro com a mesma matrícula resultou na criação de uma nova versão, mantendo a versão original preservada no histórico do ledger.

Quadro 8 – Testes de Integridade Criptográfica

Cenário de teste	Entrada avaliada	Resultado esperado	Resultado obtido
Hash inexistente.	Hash SHA-256 não registrado.	Documento não encontrado.	Figura 57.
Hash inválido.	Hash fora do padrão SHA-256.	Rejeição por validação.	Figura 58.
CID inválido.	CID fora do padrão IPFS.	Rejeição por validação.	Figura 59.
Registro de documento válido.	Hash e CID válidos.	Documento registrado na blockchain.	Figura 60.
Tentativa de modificação de documento.	Nova submissão com a mesma matrícula e dados diferentes.	Criação de nova versão do documento.	Figura 61.

Fonte: Autoria própria.

Complementarmente aos testes de segurança da plataforma, foram realizados testes de controle de acesso e validação das políticas de endosso.

Os testes foram sintetizados no Quadro 8 e mostraram que consultas podem ser realizadas a partir de um peer autorizado, enquanto operações de escrita exigem o envio da transação para múltiplos peers, respeitando a política de endosso configurada.

Quadro 9 – Testes de Controle de Acesso e Políticas de Endosso

Cenário de teste	Resultado esperado	Resultado obtido
Query com peer da coordenação.	Resposta válida para operação de consulta.	Figura 62.
Invoke com múltiplos peers.	Envio da transação para os três peers da rede.	Figura 63.
Invoke com peers não permitidos.	Retorno de erro ao tentar submeter uma resposta.	Figura 64.

Fonte: Autoria própria.

Quanto aos testes de tolerância a falhas, o objetivo é verificar se a rede permanece operacional mesmo diante da indisponibilidade de componentes individuais. Os testes foram

conduzidos por meio da interrupção controlada de um *peer* da rede e da posterior execução de consultas ao *HyperLedger Fabric,* no qual obtiveram um resultado satisfatório.

Inicialmente, o peer pertencente à organização Orientador foi intencionalmente interrompido. Em seguida, o peer interrompido foi reiniciado e a rede voltou ao estado normal de operação, mantendo a consistência e a disponibilidade dos dados registrados.

O Quadro 10 apresenta um resumo dos testes de tolerância a falhas realizados e seus respectivos resultados.

Quadro 10 – Testes de Tolerância a Falhas

Cenário de teste	Resultado esperado	Resultado obtido
Parada do peer orientador.	Peer interrompido com sucesso.	Figura 65.
Query com peer offline.	Resposta válida da rede.	Figura 66.
Recuperação do peer orientador.	Peer reiniciado e ativo.	Figura 67.
Query após recuperação.	Rede totalmente funcional.	Figura 68.

Fonte: Autoria própria.

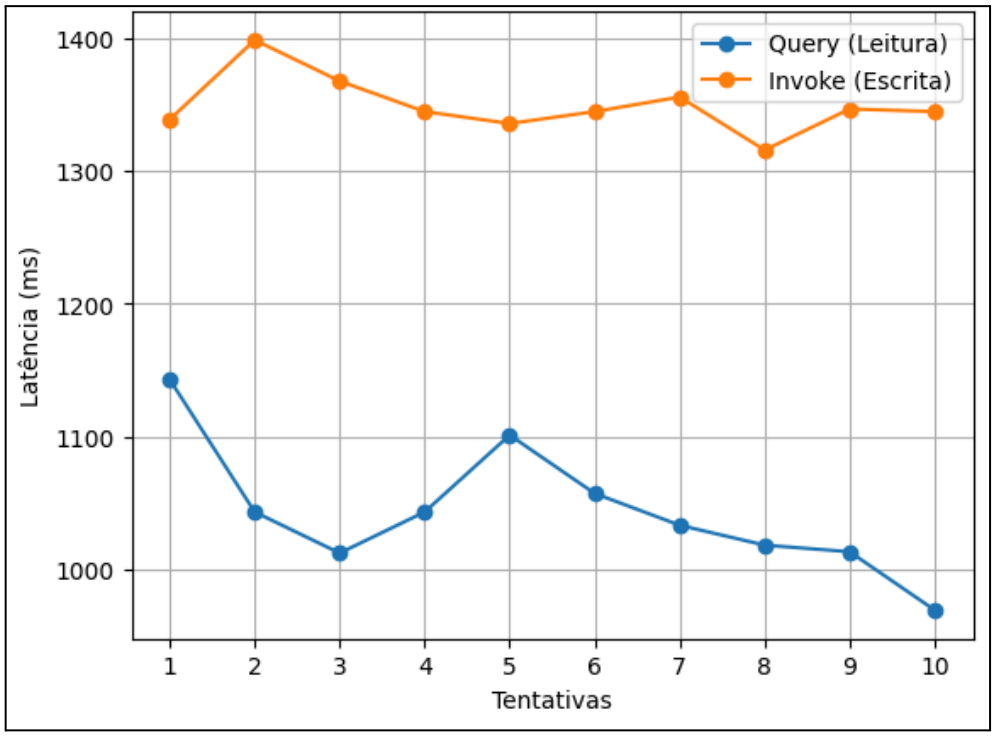
Por fim, para os testes de desempenho, o objetivo foi medir a latência das operações de leitura (*query*) e escrita (*invoke*) executadas no bloco. Os testes foram realizados em ambiente de desenvolvimento local e containerizado, utilizando uma rede *Hyperledger Fabric* com três peers ativos e um nó *orderer*kchain. Este valor não pode ser considerado como satisfatório, pois não foi possível usar parâmetros de uso real.

Inicialmente, foi conduzido um experimento controlado com o objetivo de mensurar o desempenho das operações de leitura e escrita no Ledger da rede blockchain implementada. Para a avaliação das operações de leitura, foram executadas consultas consecutivas a um mesmo conjunto de registros previamente armazenados no Ledger, utilizando a função de consulta disponibilizada pelo chaincode. Essas consultas foram realizadas de forma sequencial, sob as mesmas condições de ambiente, permitindo o cálculo do tempo médio de resposta de cada operação de leitura.

Em seguida, foram realizados testes de escrita por meio da invocação repetida da função responsável pelo registro de documentos no Ledger. Cada invocação correspondeu a uma transação completa, envolvendo as etapas de submissão da proposta, endosso pelos peers, ordenação pelo serviço de ordenação e, por fim, a validação e gravação do bloco na ledger distribuída. O tempo de resposta foi medido desde o envio da requisição até a confirmação da efetivação da transação na rede.

Durante ambos os testes, os tempos de resposta foram registrados individualmente a cada execução, possibilitando a análise da variação da latência ao longo das tentativas. Os valores coletados foram posteriormente consolidados e organizados em gráficos, apresentados na Figura 54, que permite uma visualização comparativa do comportamento das operações de leitura (Figura 68) e de escrita (Figura 69). Essa abordagem possibilita avaliar não apenas a latência média das operações, mas também a estabilidade do sistema e as oscilações de desempenho observadas ao longo das execuções.

Figura 54 – Latência por tentativa das operações de leitura e escrita



Fonte: Autoria própria.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do *Academic Ledger*, protótipo de sistema para a gestão das defesas de Trabalhos de Conclusão de Curso dos cursos de graduação do IFAL, atingiu o objetivo proposto de conceber uma solução tecnológica antifraude baseada em blockchain. A partir da compreensão do problema e da identificação dos requisitos institucionais, foi possível estruturar uma solução voltada à melhoria do controle, da confiabilidade e da rastreabilidade das informações acadêmicas envolvidas no processo de defesa de TCC.

O protótipo desenvolvido possibilitou o gerenciamento integrado de cadastros institucionais, incluindo usuários e seus respectivos papéis, cursos, orientadores, coordenadores e discentes, contribuindo para a organização e padronização das informações. Além disso, foram disponibilizados recursos para o agendamento das defesas, permitindo o controle das datas, etapas e responsáveis, bem como o acompanhamento do andamento de cada processo de forma centralizada.

A solução também incorporou um fluxo de aprovação multiator, no qual coordenador, orientador e discente(s) participam ativamente das etapas de aprovação e validação dos documentos, garantindo maior confiabilidade e transparência ao processo decisório. O controle das etapas de aprovação possibilitou a rastreabilidade das ações executadas ao longo do ciclo de vida dos documentos acadêmicos exigidos pela portaria 1483.

Adicionalmente, foram implementados mecanismos de notificação, responsáveis por informar automaticamente os atores envolvidos sobre pendências, validações, recusas e avanços de etapa, reduzindo falhas de comunicação e tornando o processo mais eficiente. Por meio de uma interface web, o sistema permitiu o acompanhamento do processo de defesa, a visualização do status dos documentos submetidos, do histórico de versões e a verificação da autenticidade dos documentos, sem exposição de informações sensíveis.

Durante o desenvolvimento deste trabalho, foram identificadas algumas limitações que podem ser exploradas em trabalhos futuros, tais como:

a. A implantação da rede *Hyperledger Fabric* em um ambiente distribuído com múltiplas máquinas ou máquinas virtuais (VM), permitindo avaliar aspectos como sincronização do ledger e latência das transações em condições próximas às de produção.
b. Podem ser implementados mecanismos adicionais de proteção das chaves de assinatura armazenadas no banco de dados, utilizando algoritmos criptográficos consolidados e técnicas de gerenciamento seguro de chaves, a

fim de reduzir riscos de acessos não autorizados e vazamento de informações sensíveis.

c. A adoção de ferramentas de monitoramento e observabilidade, como *logs* estruturados e coleta de métricas, para acompanhamento do desempenho, detecção de falhas e suporte a auditorias do sistema.
d. É necessário o aumento da cobertura de testes automatizados, incluindo testes unitários, de integração e testes *End-to-End* (E2E), com o objetivo de aumentar a confiabilidade do sistema e reduzir a ocorrência de regressões.
e. Integração com sistemas acadêmicos institucionais para a coleta automática de dados reais de usuários, como alunos, orientadores e coordenadores, eliminando a necessidade de cadastro manual no sistema.
f. Avaliar a aplicação da solução em um ambiente institucional real, verificando sua viabilidade prática, integração com sistemas existentes e aceitação pelos usuários.

Por fim, o uso do *Hyperledger Fabric* se mostrou adequado, satisfatório e tende às exigências documentais estabelecidas pela Portaria nº 1483/2012 do IFAL, demonstrando ser uma alternativa viável para suprir a lacuna existente na portaria que regulamenta os processos de defesa de TCCs, especialmente no que tange à integridade, auditabilidade, confiabilidade desses artefatos, garantido pelas principais características de uma blockchain. Dessa forma, o trabalho evidencia o potencial do uso de tecnologias blockchain como ferramenta para processos acadêmicos institucionais.

6 REFERÊNCIAS

ALMEIDA, Murilo Henrique dos Santos de; OLIVEIRA, Flávio Henrique Magalhães de. Utilização da tecnologia blockchain para certificação de sistema de gestão de processos e documentos eletrônicos. In: ANAIS da Escola Regional de Redes de Computadores (ERRC), 2022. Disponível em: https://sol.sbc.org.br/index.php/errc/article/view/15182. Acesso em: 14 jan. 2025.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). Perguntas mais frequentes. Brasília, DF: CONARQ, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/perguntas-mais-frequentes. Acesso em: 14 jan. 2026.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais. Brasília, DF: CONARQ, 2012. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_presuncao_autenticidade_completa.pdf

SHARPLES, Mike; DOMINGUE, John.
The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward.
In: Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL), 2016. Disponível em: https://link.springer.com/content/pdf/10.1007/978-3-319-45153-4_48.pdf

HYPERLEDGER FABRIC. Hyperledger Fabric documentation [S. l.]: Hyperledger Foundation, 2025. Disponível em: https://hyperledger-fabric.readthedocs.io/. Acesso em: 14 jan. 2026.

INSTITUTO FEDERAL DE ALAGOAS (IFAL). Portaria nº 1483/GR, de 19 de setembro de 2012. Aprova o Regulamento de Trabalhos de Conclusão de Cursos do IFAL. Maceió: IFAL, 2012. Disponível em: https://www2.ifal.edu.br/o-ifal/pesquisa-pos-graduacao-e-inovacao/legislacao-e-normas/arquivos/portaria-no-1483-gr-2012.pdf

PESSANHA, Grasiella Ribeiro Monteiro; SALES, Diego da Silva; PIMENTA, Fabrícia Pires. *Repositórios Institucionais de Instituições de Ensino e Pesquisa Brasileiras: gestão, direitos autorais e digitalização de trabalhos acadêmicos impressos.* In: Research and Integration: Multidisciplinary Studies. Curitiba, PR: Aurum Editora Ltda, 2025. p. 65–79. DOI: https://doi.org/10.63330/aurumpub.008-007. Disponível em: https://doi.org/10.63330/aurumpub.008-007.

MEDEIROS, Daniel Márcio de. Mecanismo de consenso em uma rede ponto a ponto distribuída para validação e registros de diplomas universitários. 2019. 67 f. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em: https://tede2.pucsp.br/bitstream/handle/22827/2/Daniel%20M%C3%A1rcio%20de%20Medeiros.pdf. Acesso em: 30 jun. 2025.

MILI, Khaled. Blockchain traceability to ensure the veracity of diplomas. International Journal of Intelligent Information Systems, v. 10, n. 4, p. 60–68, 2021. DOI: https://doi.org/10.11648/j.ijiis.20211004.14. Disponível em: https://www.sciencepublishinggroup.com/article/10.11648/j.ijiis.20211004.14. Acesso em: 30 jun. 2025.

RUSTEMI, Avni et al. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification. IEEE Access, v. 11, p. 64679–64693, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3289598.

VANDERLEY NETO, Inaldo Matos. *Fraude acadêmica: um estudo da percepção dos docentes do Departamento de Finanças e Contabilidade da Universidade Federal da Paraíba*. 2021. Trabalho de Conclusão de Curso (Bacharelado em Ciências Contábeis) – Universidade Federal da Paraíba, João Pessoa, 2021. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/21751/1/IMVN28122021.pdf

MACHADO, Beatriz Menezes. *Segurança da informação: abordagem do tema com foco no usuário e seu comportamento informacional seguro.* 2013. 78 f. Monografia (Especialização em Gestão Estratégica da Informação) – Universidade Federal de Minas Gerais, Escola de Ciência da Informação, Belo Horizonte, 2013. Disponível em: https://repositorio.ufmg.br/items/1f5a60c0-1d6e-4ba0-aaa2-42d293c1d49b

ALBUQUERQUE JUNIOR, Antonio Eduardo de; SANTOS, Ernani Marques dos. Adoption of information security measures in public research institutes. *JISTEM – Journal of Information Systems and Technology Management*, v. 12, n. 2, p. 289–316, 2015. Disponível em: https://jistem.tecsi.org/index.php/jistem/article/view/10.4301%252FS1807-17752015000200006.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica (parte 1): conheça os principais algoritmos de cifragem. *Revista Segurança Digital*, Niterói, n. 5, p. 11–15, mar. 2012. Disponível em: https://www.researchgate.net/publication/303367222_Criptografia_simetrica_e_assimetrica_os_principais_algoritmos_de_cifragem

LUDWIG, Lara; REBELATTO, Miguel Grando; SILVA, Sandro José Ribeiro. *O estado da arte das criptografias modernas: uma revisão sistemática da literatura*. Revista Brasileira de Computação Aplicada (RBCA), v. 12, n. 2, p. 46-53, 2020. DOI: 10.5335/rbca.v12i2.10455. Disponível em: https://dx.doi.org/10.5335/rbca.v12i2.10455.

CARMO, Dalton Gonçalves do. *Digitalização de substituição no contexto da gestão arquivística de documentos: uma análise dos riscos à autenticidade e confiabilidade documental.* 2023. Dissertação (Mestrado em Ciências da Informação) — Universidade Federal de Minas Gerais, Belo Horizonte, 2023. Disponível em: https://repositorio.ufmg.br/server/api/core/bitstreams/176161a6-d989-45da-83b8-49dc36e9bf52/content.

MAZIEIRO, Carlos A. *Criptografia simétrica*. In: Segurança Computacional. Capítulo 2. Curitiba: Departamento de Informática, Universidade Federal do Paraná, 2019. Disponível em: https://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=sc%3Aseg-texto-02.pdf. Acesso em: __ jan. 2026.

MAZIEIRO, Carlos A. Funções hash criptográficas. In: Segurança Computacional. Curitiba: Departamento de Informática, Universidade Federal do Paraná, 2019. Capítulo 3. Disponível em: https://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=sc:seg-texto-03.pdf. Acesso em: 14 jan. 2026.

CHEAPSSLSECURITY. What is the SHA-2 / SHA-256 hashing algorithm. Disponível em: https://cheapsslsecurity.com/p/what-is-the-sha-2-sha256-hashing-algorithm/. Acesso em: 14 jan. 2026.

WANG, Y.; ZHANG, Y.; LI, J.; ZHOU, Y. An IPFS-based secure storage and sharing scheme for blockchain. *IEEE Access*, v. 10, p. 53015–53027, 2022. DOI: 10.1109/ACCESS.2022.3177641. Disponível em: https://ieeexplore.ieee.org/document/9794296. Acesso em: 14 jan. 2026.

FREITAS, Allan Edgard Silva; RODRIGUES, Luiz Antonio; DUARTE JR., Elias Procópio. *vCubeChain: Uma Blockchain Permissionada Escalável*. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 41., 2023, Brasília/DF. Anais… Porto Alegre: Sociedade Brasileira de Computação, 2023. p. 127-140. ISSN 2177-9384. DOI: https://doi.org/10.5753/sbrc.2023.394.

FERREIRA, Maria et al. *Construindo aplicações baseadas em blockchain com o Hyperledger FireFly*. Porto Alegre: Sociedade Brasileira de Computação, 2024. Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/download/152/651/1171?inline=1

HYPERLEDGER FABRIC. *Hyperledger Fabric documentation*. [S. l.]: Linux Foundation, 2025. Disponível em: https://hyperledger-fabric.readthedocs.io/. Acesso em: 19 jan. 2026.

WEN, Feng; WANG, Zhuo; QU, Leda; HUANG, Haixin; HU, Xiaojie. Enhancing secure multi-group data sharing through integration of IPFS and Hyperledger Fabric. PeerJ Computer Science, v. 10, e1962, 2024. DOI: 10.7717/peerj-cs.1962. Disponível em: https://peerj.com/articles/cs-1962/. Acesso em: 14 jan. 2026.

IPFS. *A practical explainer on IPFS gateways*. IPFS Blog, 9 jun. 2022. Disponível em: https://blog.ipfs.tech/2022-06-09-practical-explainer-ipfs-gateways-1/. Acesso em: 14 jan. 2026.

IPFS. Kubo (go-ipfs). Disponível em: https://docs.ipfs.tech/install/command-line/. Acesso em: 14 jan. 2026.

IBM. Blockchain basics: Hyperledger Fabric. IBM Developer, [s. l.], [s. d.]. Disponível em: <https://developer.ibm.com/articles/blockchain-basics-hyperledger-fabric/\>. Acesso em: 8 fev. 2026.

ANDROULAKI, Elli et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference (EuroSys '18)*, ACM, 2018. Disponível em: https://dl.acm.org/doi/epdf/10.1145/3190508.3190538

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. Rio de Janeiro: Elsevier, 2014.

APÊNDICE A - REQUISITOS DA SOLUÇÃO

Quadro 11 – Requisitos Funcionais

Identificador	Contexto	Requisito	Depende de
RF001	Autenticação	O sistema deve permitir autenticação por e-mail e senha válidos.	RN001, RN002
RF002	Autenticação	O sistema deve permitir o encerramento da sessão autenticada (logout).	RN005
RF003	Usuário	O sistema deve permitir a alteração de senha do usuário autenticado.	RN001
RF004	Usuário	O sistema deve permitir o cadastro de coordenadores.	RN006, RN009, RN042
RF005	Usuário	O sistema deve permitir o cadastro de discentes e orientadores.	RN006, RN009, RN043
RF006	Usuário	O sistema deve permitir a edição de dados de discentes e orientadores.	RN006, RN007, RN010, RN043
RF007	Usuário	O sistema deve permitir a listagem de discentes e orientadores com paginação.	RN010
RF008	Defesa	O sistema deve permitir a visualização do histórico de defesas.	
RF009	Curso	O sistema deve permitir o cadastro de novos cursos.	RN008, RN042
RF010	Curso	O sistema deve permitir a visualização dos cursos cadastrados.	RN008
RF011	Curso	O sistema deve permitir a edição dos dados de um curso.	RN010
RF012	Usuário	O sistema deve permitir a listagem de discentes vinculados a um curso.	RN010
RF013	Usuário	O sistema deve permitir a listagem de orientadores vinculados a um curso.	RN010
RF014	Defesa	O sistema deve permitir o agendamento de defesas de TCC.	RN010, RN013, RN014
RF015	Defesa	O sistema deve permitir a listagem de defesas com filtros e paginação.	RN010, RN013, RN014
RF016	Defesa	O sistema deve permitir a visualização dos detalhes de uma defesa.	RN044
RF017	Defesa	O sistema deve permitir o reagendamento de defesas.	RN010, RN019, RN020
RF018	Defesa	O sistema deve permitir o cancelamento de defesas.	RN010, RN019, RN020
RF019	Defesa	O sistema deve permitir a submissão do resultado de uma defesa.	RN010, RN015, RN016, RN017, RN018.

RF020	Documento	O sistema deve permitir o upload de documentos PDF ao submeter o resultado da defesa.	RN021, RN022, RN023, RN024, RN040, RN041
RF021	Documento	O sistema deve permitir a visualização do histórico de versões de documentos.	RN021, RN022
RF022	Documento	O sistema deve permitir o download de documentos.	RN044
RF023	Documento	O sistema deve permitir a criação de novas versões de documentos.	RN033, RN034
RF024	Documento	O sistema deve suportar versionamento automático.	RN034
RF025	Documento	O sistema deve calcular os hashes SHA-256 dos documentos ao fazer upload.	
RF026	Documento	O sistema deve manter histórico completo de todas as versões de documentos.	
RF027	Aprovação	O sistema deve permitir a aprovação ou rejeição de documentos.	RN025, RN026, RN027, RN028
RF028	Aprovação	O sistema deve permitir a reconsideração de uma rejeição.	RN029, RN030, RN031
RF029	Aprovação	O sistema deve permitir o envio de lembretes para aprovadores pendentes.	RN045
RF030	Aprovação	O sistema deve permitir a listagem das aprovações pendentes de um usuário.	RN046
RF031	Verificação	O sistema deve permitir a verificação de autenticidade de documento por upload de arquivo.	RN021, RN024
RF032	Verificação	O sistema deve permitir a verificação de autenticidade de documento por hash SHA-256.	RN024
RF033	Blockchain	O sistema deve permitir a verificação de documentos por CID registrado na blockchain.	RN035
RF034	Blockchain	O sistema deve permitir a consulta de uma versão específica de documento na blockchain.	RN035, RN037
RF035	Blockchain	O sistema deve permitir a consulta do histórico completo de versões de um documento na blockchain.	RN035, RN037
RF036	Blockchain	O sistema deve permitir a consulta da quantidade de versões de um documento na blockchain.	RN035
RF037	Blockchain	O sistema deve permitir a consulta dos documentos aprovados mais recentes registrados na blockchain.	RN035, RN036
RF038	Blockchain	O sistema deve registrar as assinaturas digitais de todos os aprovadores junto com os hashes dos documentos na blockchain.	RN035, RN036, RN037

RF039	Blockchain	O sistema deve emitir evento de documento registrado após registro na blockchain.	
RF040	Blockchain	O sistema deve manter documentos imutáveis após registro na blockchain.	RN037

RF041	Autenticação	O sistema deve validar credenciais contra o banco de dados.	RN001
RF042	Autenticação	O sistema deve gerar token JWT de acesso após autenticação bem-sucedida.	RN003
RF043	Autenticação	O sistema deve redirecionar o usuário para a tela apropriada conforme seu papel.	
RF044	Usuário	O sistema deve gerar senha temporária ao cadastrar novo usuário.	RN001
RF045	Notificação	O sistema deve enviar credenciais por e-mail ao cadastrar novo usuário.	
RF046	Aprovação	O sistema deve resetar aprovações ao criar nova versão de documento.	RN033
RF047	Aprovação	O sistema deve criar aprovações automaticamente ao submeter resultado (coordenador, orientador e cada discente).	RN025
RF048	Aprovação	O sistema deve resetar a aprovação do integrante ao desconsiderar uma rejeição.	RN031
RF049	Aprovação	O sistema deve autoaprovar a aprovação do orientador se o coordenador for o orientador.	RN032
RF050	Certificado	O sistema deve gerar certificado digital individual via Fabric CA ao criar uma solicitação de assinatura.	
RF051	Certificado	O sistema deve armazenar certificados digitais de forma criptografada no banco de dados.	
RF052	Certificado	O sistema deve revogar certificados digitais após submissão do documento à blockchain.	RN038
RF053	Verificação	O sistema deve calcular o hash do arquivo enviado e comparar com a blockchain na validação.	
RF054	Verificação	O sistema deve retornar informações do documento na verificação de autenticidade.	
RF055	IPFS	O sistema deve fazer upload dos documentos para o IPFS.	RN039, RN040, RN041
RF056	IPFS	O sistema deve armazenar o CID (Content Identifier) do IPFS.	
RF057	IPFS	O sistema deve fazer download de arquivos do IPFS.	
RF058	IPFS	O sistema deve enfileirar o upload se o IPFS estiver offline.	RN039

RF059	IPFS	O sistema deve fazer pinning automático de documentos no IPFS.	RN040
RF060	Notificação	O sistema deve enviar e-mail ao agendar defesa.	RN041
RF061	Notificação	O sistema deve enviar e-mail ao cancelar defesa.	
RF062	Notificação	O sistema deve enviar e-mail ao reagendar defesa.	
RF063	Notificação	O sistema deve enviar e-mail com o resultado da defesa.	
RF064	Notificação	O sistema deve enviar e-mail solicitando aprovação de documento.	
RF065	Notificação	O sistema deve enviar e-mail confirmando a aprovação do documento.	
RF066	Notificação	O sistema deve enviar e-mail informando a rejeição de documento.	
RF067	Notificação	O sistema deve enviar e-mail quando a rejeição for desconsiderada.	

Fonte: Autoria própria.

Quadro 12 – Regras de Negócio

Identificador	Descrição
RN001	A senha deve ter no mínimo 8 caracteres, incluindo pelo menos uma letra maiúscula, uma minúscula, um dígito e um caractere especial.
RN002	O sistema deve exigir troca de senha no primeiro acesso.
RN005	O sistema deve revogar o token após a ação.
RN006	O e-mail do usuário deve ser único no sistema.
RN007	A matrícula do discente deve ser única no sistema.
RN008	O código do curso deve ser único no sistema.
RN009	Cada curso pode ter no máximo um coordenador ativo por vez.
RN010	O coordenador só pode gerenciar discentes, orientadores e defesas do seu próprio curso.
RN011	Não é possível ativar um coordenador sem vinculá-lo a um curso.
RN012	Não é possível atribuir um coordenador inativo a um curso.
RN013	Uma defesa deve ter no mínimo 1 e no máximo 2 discentes.
RN014	Um discente não pode ter mais de uma defesa ativa simultaneamente.
RN015	O resultado da defesa só pode ser submetido após a data da defesa.
RN016	O resultado da defesa só pode ser submetido se o status for “Agendado”.
RN017	Nota maior ou igual a 7 resulta em “Aprovado”; abaixo de 7, “Reprovado”.
RN018	A nota da defesa deve estar entre 0 e 10.
RN019	Não é possível cancelar ou reagendar uma defesa já concluída.

RN020	O cancelamento e o reagendamento de defesa exigem justificativa.

RN021	Os documentos enviados devem ser PDFs válidos.
RN022	Cada arquivo de documento deve ter no máximo 10 MB.
RN023	A submissão de resultado exige obrigatoriamente a ata e a avaliação de desempenho.
RN024	O *hash* SHA-256 de um documento deve ser único no sistema.
RN025	Ao submeter resultado, o sistema deve criar aprovações para o coordenador, o orientador e cada discente da defesa.
RN026	O coordenador só pode aprovar após o orientador e todos os discentes terem aprovado.
RN027	O coordenador não pode rejeitar documentos, apenas orientadores e discentes.
RN028	A rejeição de documento exige justificativa.
RN029	Somente o coordenador pode desconsiderar uma rejeição.
RN030	O coordenador não pode desconsiderar sua própria rejeição.
RN031	Ao desconsiderar uma rejeição, a aprovação do integrante deve ser resetada para “Pendentes”.
RN032	Se o coordenador for o orientador da defesa, a aprovação do orientador deve ser automaticamente aprovada.
RN033	Ao criar nova versão de documento, todas as aprovações devem ser resetadas.
RN034	Nova versão de documento incrementa o número da versão em 1.
RN035	O registro na blockchain exige que todas as aprovações estejam com status “Aprovado”.
RN036	O registro na blockchain exige a contagem correta de aprovações: 2 (Orientador(a) e Coordenador(a)) + número de discentes.
RN037	Documentos são imutáveis após registro na blockchain.
RN038	Após registro na blockchain, os certificados digitais de orientador e discentes devem ser revogados.
RN040	Se o IPFS estiver offline, o upload deve ser enfileirado para retry.

RN041	Documentos devem ter pinning automático no IPFS.
RN042	Apenas administradores podem cadastrar coordenadores e cursos.
RN043	Apenas coordenadores podem cadastrar e editar discentes e orientadores do seu curso.
RN044	Apenas participantes da defesa podem executar essa ação.
RN045	Apenas o coordenador pode enviar um lembrete solicitando uma aprovação.
RN046	A listagem de assinaturas só deve trazer defesas nas quais o usuário é o participante.

Fonte: Autoria própria.

Quadro 13 – Requisitos Não Funcionais

Identificador	Requisito	**Descrição**
RNF001	Segurança	O sistema deve utilizar JWT com expiração de 15 minutos para access token.
RNF002	Segurança	O sistema deve utilizar refresh token com validade de 7 dias

		armazenado em HTTP-only cookie.
RNF003	Segurança	O sistema deve utilizar bcrypt para hash de senhas.
RNF005	Segurança	O sistema deve validar todas as entradas com whitelist (rejeitar propriedades não definidas).
RNF006	Segurança	O sistema deve utilizar rede IPFS privada com chave de swarm compartilhada.
RNF007	Segurança	O sistema deve desabilitar o gateway HTTP público do IPFS.
RNF008	Desempenho	O sistema deve suportar paginação com máximo de 100 itens por página.
RNF009	Desempenho	O sistema deve utilizar filas assíncronas (Bull/Redis) para processamento de uploads.
RNF010	Desempenho	O sistema deve processar uploads IPFS em background sem bloquear requisições HTTP.
RNF011	Disponibilidade	O sistema deve manter redundância entre 2 nós IPFS.
RNF012	Disponibilidade	O sistema deve verificar a saúde dos nós IPFS.
RNF013	Disponibilidade	O sistema deve implementar retry automático para envio de e-mails.
RNF014	Disponibilidade	O sistema deve fazer pinning automático de documentos em ambos os nós IPFS.
RNF016	Escalabilidade	O sistema deve utilizar autenticação baseada em tokens JWT, sem armazenar sessões em memória no servidor.
RNF017	Escalabilidade	O sistema deve utilizar Redis centralizado para filas.
RNF018	Usabilidade	O sistema deve ter interface responsiva.
RNF019	Usabilidade	O sistema deve fornecer feedback visual durante operações.
RNF020	Usabilidade	O sistema deve seguir padrões de acessibilidade.
RNF021	Usabilidade	O sistema deve aplicar temas visuais diferenciados por papel do usuário.
RNF022	Manutenibilidade	O sistema deve fornecer documentação de API via Swagger/OpenAPI.
RNF023	Manutenibilidade	O sistema deve utilizar arquitetura em camadas.
RNF024	Manutenibilidade	O sistema deve utilizar migrations versionadas para o banco de dados.
RNF025	Interoperabilidade	O sistema deve expor API REST com formato JSON.
RNF026	Interoperabilidade	O sistema deve suportar upload de arquivos via multipart/form-data.
RNF027	Interoperabilidade	O sistema deve integrar-se com *Hyperledger Fabric* via gRPC com mTLS.
RNF028	Interoperabilidade	O sistema deve suportar CIDv0 e CIDv1 do IPFS.

Fonte: Autoria própria.

APÊNDICE B: DIAGRAMA DE ENTIDADE E RELACIONAMENTO

O banco de dados utilizado neste trabalho foi desenvolvido com base no modelo apresentado na Figura 55, sendo implementado em um sistema gerenciador de banco de dados relacional PostgreSQL.

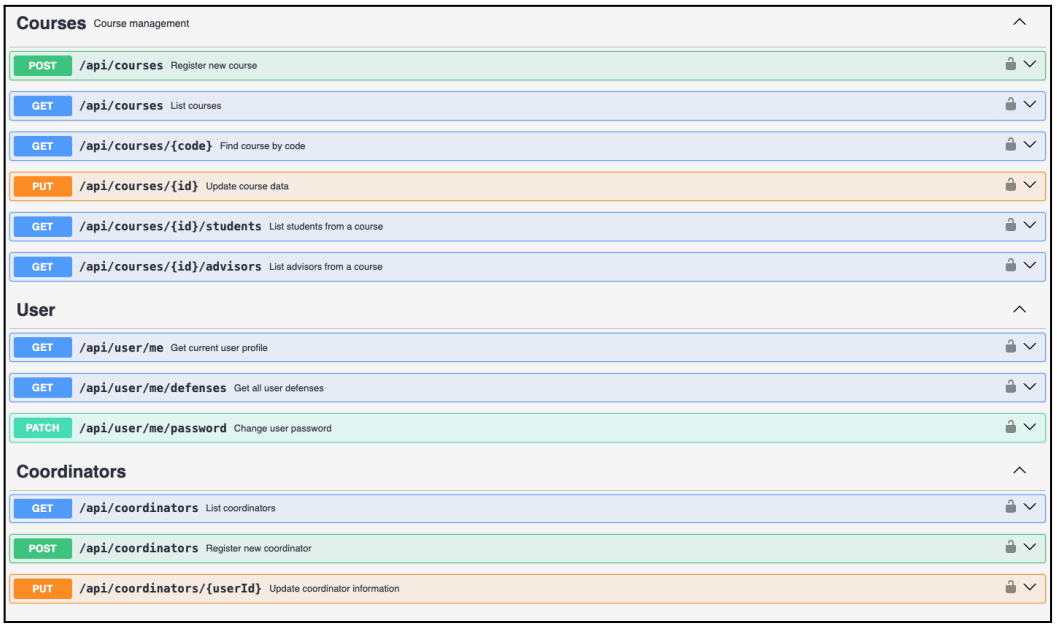
Figura 55 – Esquema de Banco de Dados

Fonte: Autoria própria.

APÊNDICE C: ENDPOINTS API

Os endpoints da API foram organizados considerando os diferentes perfis de usuários e as ações realizadas em cada etapa do sistema antifraude acadêmico. Essa definição evitou a necessidade de tratamentos complexos no frontend e ajudou a manter a implementação do protótipo mais simples durante o desenvolvimento.

Figura 56 – Visualização dos Endpoints da API do Swagger/OpenApi



Fonte: Autoria própria.

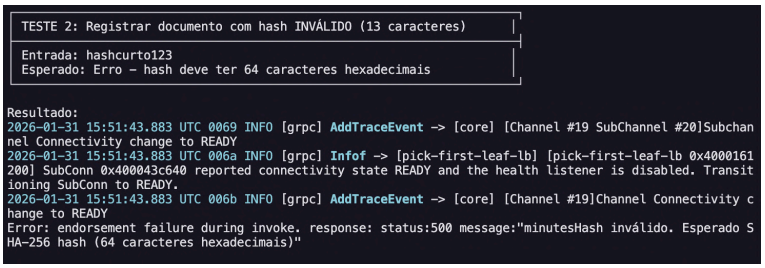
APÊNDICE D: TESTES DE VALIDAÇÃO NO HYPERLEDGER

Os testes realizados neste trabalho foram executados por meio de comandos em terminal, utilizando as ferramentas de linha de comando do Hyperledger Fabric e scripts auxiliares desenvolvidos para interação com o chaincode. Este apêndice apresenta os registros das execuções realizadas, servindo como evidência prática dos testes descritos ao longo do trabalho.

Figura 57 – Verificar Hash Inexistente na Blockchain

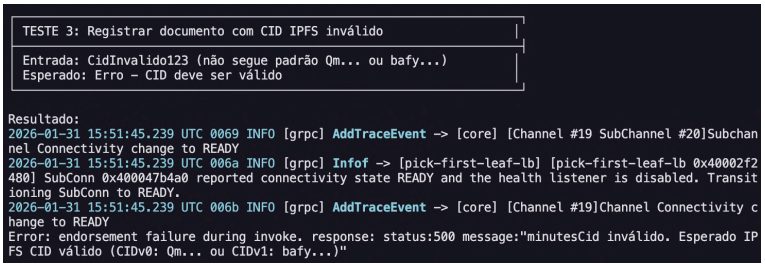
Fonte: Autoria própria.

Figura 58 – Registrar Documento com Hash Inválido



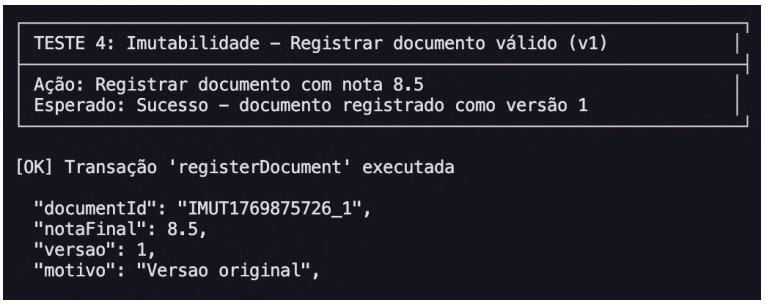
Fonte: Autoria própria.

Figura 59 – Registrar Documento com CID IPFS Inválido



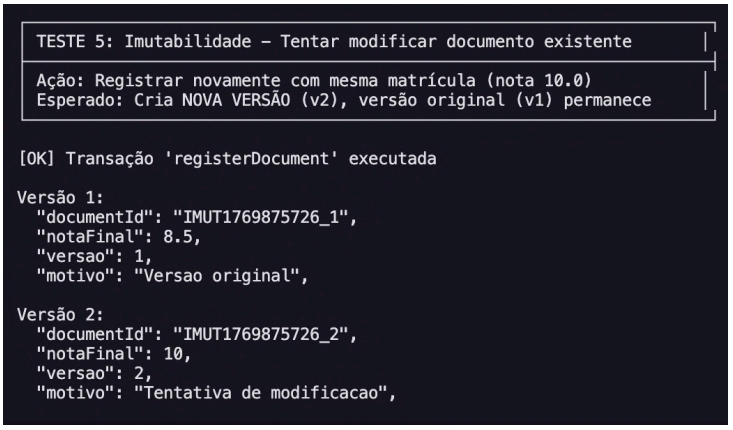
Fonte: Autoria própria.

Figura 60 – Registro de um Documento Válido



Fonte: Autoria própria.

Figura 61 – Tentativa de Modificação de um Documento Existente

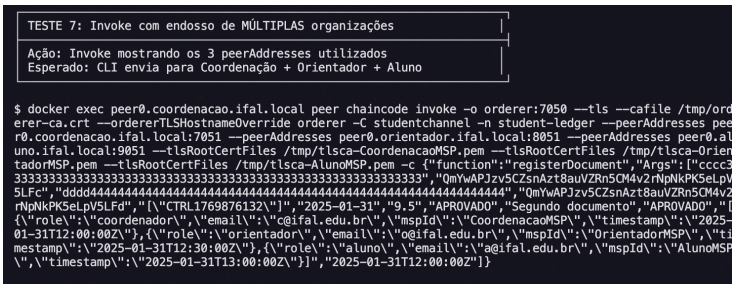


Fonte: Autoria própria.

Figura 62 – Busca com Endossamento de Pelo Menos um Peer

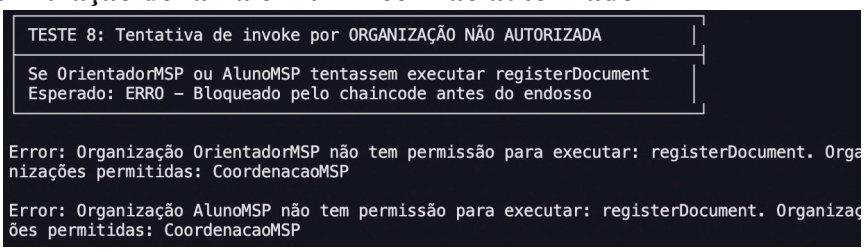
Fonte: Autoria própria.

Figura 63 – Endosso de Todos os Peers no Mecanismo de Consenso



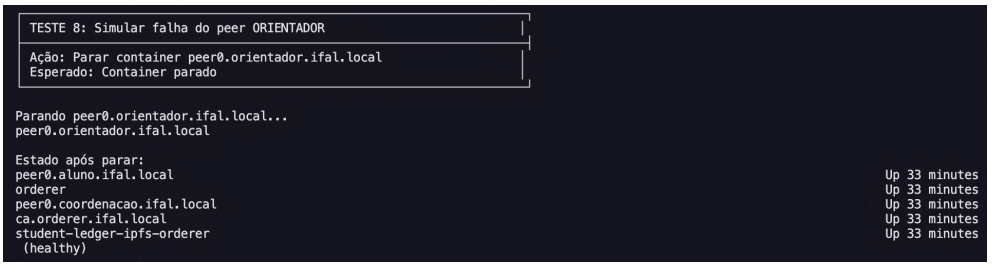
Fonte: Autoria própria.

Figura 64 – Simulação de falha em um Peer não autorizado



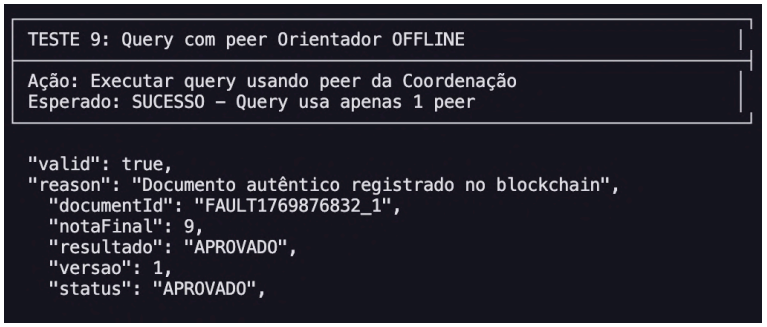
Fonte: Autoria própria.

Figura 65 – Simulação de falha em um Peer



Fonte: Autoria própria.

Figura 66 – Busca de dados com um Peer Desconectado

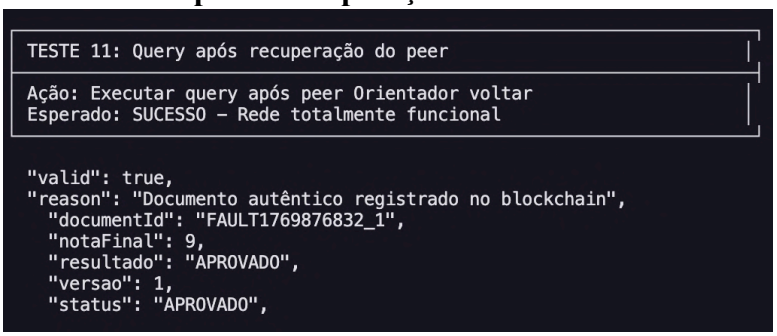


Fonte: Autoria própria.

Figura 67 – Simulação do Retorno de um Peer

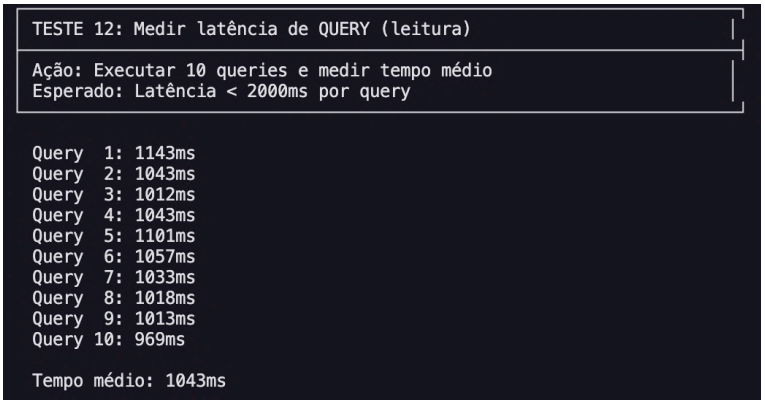
Fonte: Autoria própria.

Figura 68 – Busca de Dados Após a Recuperação de um Peer



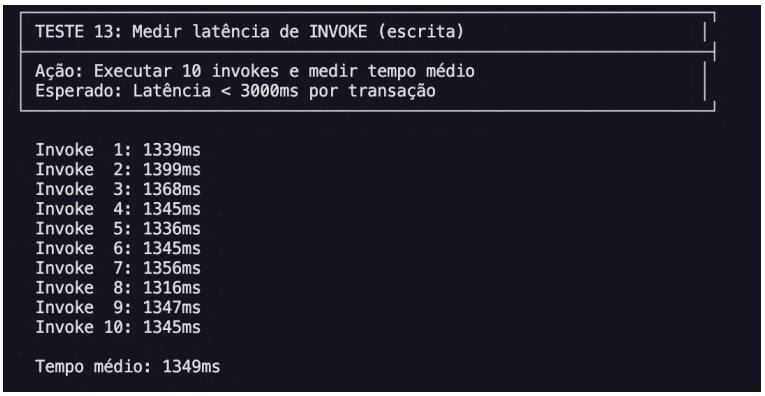
Fonte: Autoria própria.

Figura 69 – Latência de Leitura na Rede



Fonte: Autoria própria.

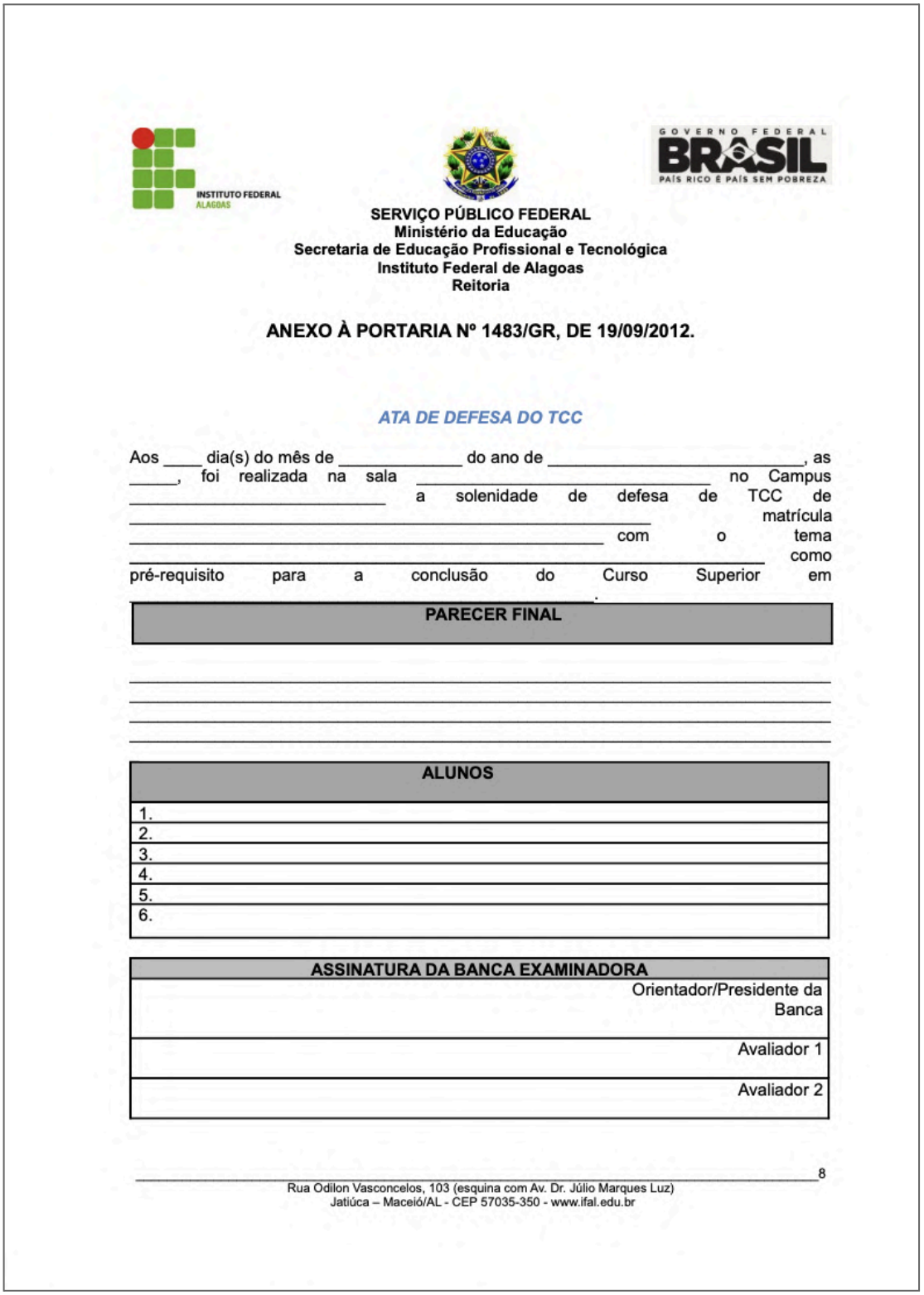
Figura 70 – Latência de Escrita na Rede



Fonte: Autoria própria.

ANEXO I - ATA DE DEFESA DE TCC

Figura 71 – Documento da Ata de Defesa do TCC, exigida pela Portaria nº 1483/GR, de 19 de setembro de 2012



INSTITUTO FEDERAL
ALAGOAS

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA

SERVIÇO PÚBLICO FEDERAL
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Alagoas
Reitoria

ANEXO À PORTARIA Nº 1483/GR, DE 19/09/2012.

ATA DE DEFESA DO TCC

Aos ____ dia(s) do mês de _____ do ano de _____, as _____, foi realizada na sala _____ no Campus _____ a solenidade de defesa de TCC de matrícula _____ com o tema _____ como pré-requisito para a conclusão do Curso Superior em _____.

PARECER FINAL

ALUNOS
1.
2.
3.
4.
5.
6.

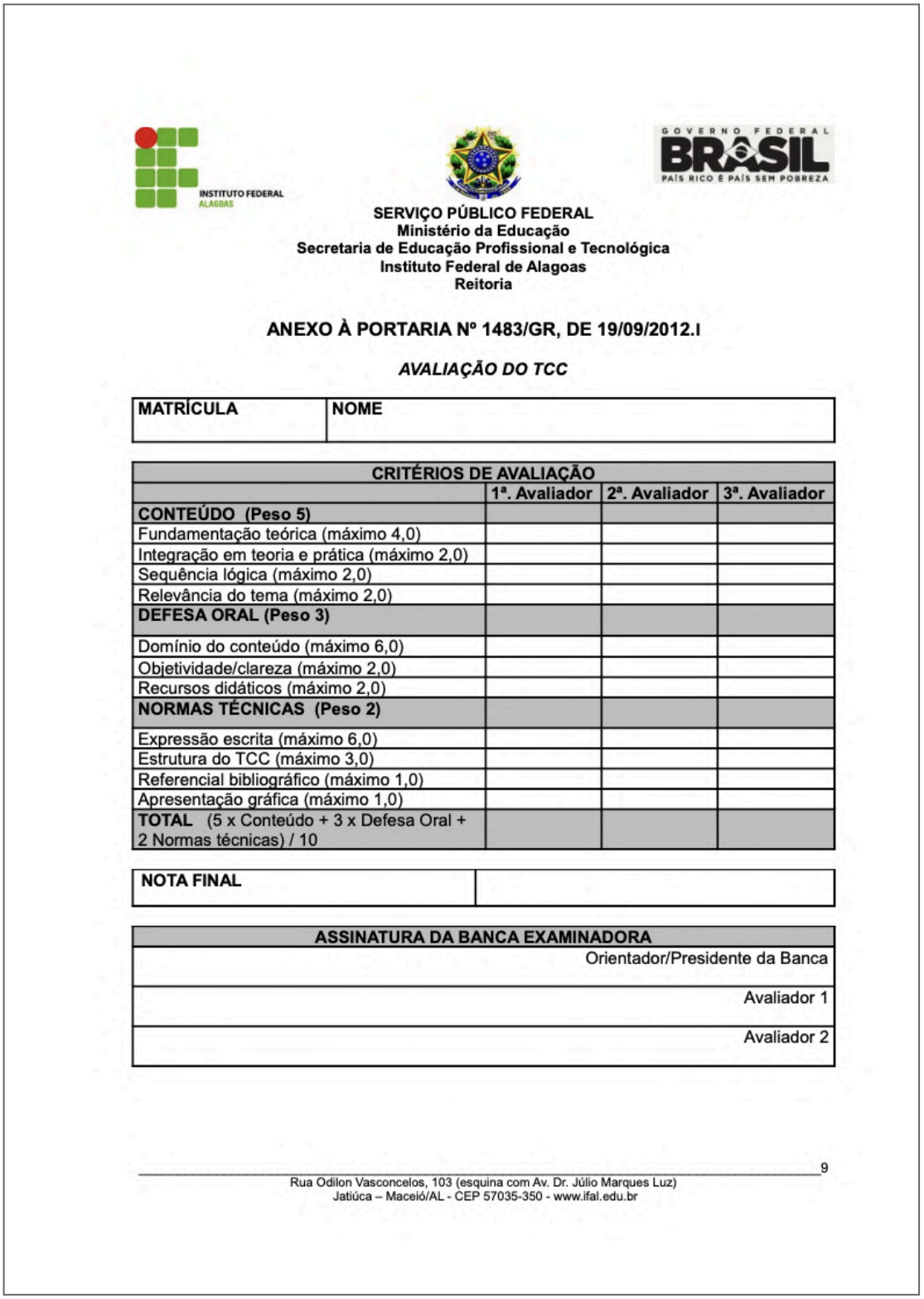
ASSINATURA DA BANCA EXAMINADORA
Orientador/Presidente da Banca
Avaliador 1
Avaliador 2

Rua Odilon Vasconcelos, 103 (esquina com Av. Dr. Júlio Marques Luz)
Jatiúca – Maceió/AL - CEP 57035-350 - www.ifal.edu.br

Fonte: Instituto Federal de Alagoas (2012).

ANEXO II - FICHA DE AVALIAÇÃO DE TCC

Figura 72 – Documento da Avaliação do TCC, exigido pela Portaria nº 1483/GR, de 19 de setembro de 2012



INSTITUTO FEDERAL
ALAGOAS

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA

SERVIÇO PÚBLICO FEDERAL
Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Alagoas
Reitoria

ANEXO À PORTARIA Nº 1483/GR, DE 19/09/2012.I

AVALIAÇÃO DO TCC

MATRÍCULA	**NOME**

CRITÉRIOS DE AVALIAÇÃO			
	1ª. Avaliador	**2ª. Avaliador**	**3ª. Avaliador**
CONTEÚDO (Peso 5)			
Fundamentação teórica (máximo 4,0)			
Integração em teoria e prática (máximo 2,0)			
Sequência lógica (máximo 2,0)			
Relevância do tema (máximo 2,0)			
DEFESA ORAL (Peso 3)			
Domínio do conteúdo (máximo 6,0)			
Objetividade/clareza (máximo 2,0)			
Recursos didáticos (máximo 2,0)			
NORMAS TÉCNICAS (Peso 2)			
Expressão escrita (máximo 6,0)			
Estrutura do TCC (máximo 3,0)			
Referencial bibliográfico (máximo 1,0)			
Apresentação gráfica (máximo 1,0)			
TOTAL (5 x Conteúdo + 3 x Defesa Oral + 2 Normas técnicas) / 10			

NOTA FINAL	

ASSINATURA DA BANCA EXAMINADORA
Orientador/Presidente da Banca
Avaliador 1
Avaliador 2

9

Rua Odilon Vasconcelos, 103 (esquina com Av. Dr. Júlio Marques Luz)
Jatiúca – Maceió/AL - CEP 57035-350 - www.ifal.edu.br

Fonte: Instituto Federal de Alagoas (2012).