FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

DESENVOLVIMENTO DE UMA PLATAFORMA DE PARTILHA DE PROCESSOS CLÍNICOS BASEADA EM *BLOCKCHAIN*

Caso de estudo: **Sistema Nacional de Saúde**.

Autora:

MACAMO, Mónica Olga Ricardo

Supervisor:

Eng. Rúben Moisés Manhiça

Maputo, Setembro de 2022

FACULDADE DE ENGENHARIA

CURSO DE ENGENHARIA INFORMÁTICA

DESENVOLVIMENTO DE UMA PLATAFORMA DE PARTILHA DE PROCESSOS CLÍNICOS BASEADA EM *BLOCKCHAIN*

Caso de estudo: **Sistema Nacional de Saúde**.

Autora:

MACAMO, Mónica Olga Ricardo

Supervisor:

Eng. Rúben Moisés Manhiça

Maputo, Setembro de 2022

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTRÓTECNICA

TERMO DE ENTREGA DE RELATÓRIO DE TRABALHO DE LICENCIATURA

Declaro que a estudante Mónica Olga Ricardo Macamo entregou no dia 14/09/2022, as 03 cópias do relatório do seu Trabalho de Licenciatura com referência **2021EITLD100**, intitulado: **Desenvolvimento de uma Plataforma de Partilha de Processos Clínicos baseada em *Blockchain.***

Maputo, 14 de Setembro de 2022

A Chefe da Secretaria

_____

FACULDADE DE ENGENHARIA

DEPARTAMENTO DE ENGENHARIA ELECTRÓTECNICA

DECLARAÇÃO DE HONRA

Declaro sob compromisso de honra que o presente trabalho é resultado da minha investigação e que foi concebido para ser submetido apenas para a obtenção do grau de Licenciatura em Engenharia Informática na Faculdade de Engenharia da Universidade Eduardo Mondlane.

Maputo, 14 de Setembro de 2022

A Autora

_____

(Mónica Olga Ricardo Macamo)

Dedicatória

Aos meus pais,

Catarina Olga Matusse Macamo e

Ricardo Nhamene Macamo.

Agradecimentos

Em primeiro lugar, agradeço a Deus por ter me permitido e ajudado a chegar até aqui. Ele, com certeza, foi e tem sido o meu catalisador.

Agradeço aos meus pais, Ricardo Macamo e Catarina Macamo por todo o suporte que me deram desde o primeiro dia desta jornada académica, por se alegrarem comigo nos êxitos e me motivarem nas dificuldades.

Agradeço aos meus irmãos por terem me acompanhado durante esta jornada. Ao Salatiel Macamo, por me acordar durante as noites de inverno e verão para que eu pudesse estudar e ao Losdelau Macamo por ter me ajudado em momentos de necessidade. Ao meu Tio Domingos Matusse por ter estado sempre presente e a Josefa Zandamela por, de várias formas, ter me ajudado durante os meus anos na faculdade.

Aos meus colegas, que se tornaram uma família e tornaram os dias na faculdade menos pesados e mais divertidos, José Machanguele, Denise Cossa, Marcos Chichava, Salmento Chitlango, Eurico Mazivila, Edmilson Chelene, Ricardo Manhice, obrigada pelo companheirismo, especialmente ao Delfim Uqueio Jr., que além de colega se tornou o meu melhor amigo de sempre.

Ao corpo docente, especialmente ao meu supervisor Ruben Manhiça, pela paciência e alta disponibilidade sempre. Pelos conhecimentos e experiências compartilhadas ao longo dos últimos anos.

À todos que directa ou indirectamente fizeram parte e contribuíram para o cumprimento desta missão, o meu especial agradecimento.

Epígrafe

Dar sempre o seu melhor é garantia de victória ao final de cada desafio, independentemente do resultado, pois se tem por certo que tudo o que poderia ser feito se fez.

-A autora

Resumo

O Sistema Nacional de Saúde (SNS) é um órgão regido pelo Ministério da Saúde (MISAU), instituído em 1991 pelo Governo de Moçambique, com o objectivo de promover a saúde de todo o cidadão nacional. Para o alcance destes objectivos, uma das ferramentas essenciais que os profissionais de saúde usam para o atendimento aos pacientes é o Processo Clínico (PC), que é, essencialmente, um histórico clínico do paciente durante os diferentes estágios da sua vida. Daí, a importância de possibilitar a construção de um histórico completo, íntegro e acessível por qualquer profissional de saúde de qualquer Unidade Sanitária (US) do SNS sempre que necessário. Para tal, os PC dos pacientes precisam ser compartilhados entre as US do SNS.

A partilha de PC contribui na melhoraria da precisão de diagnósticos e promove o progresso da pesquisa médica. Entretanto, a garantia da privacidade e integridade desta informação e um controlo de acesso refinado são questões cruciais a serem tomadas em conta quando os PC dos pacientes são compartilhados.

Como uma arquitectura distribuída com recursos descentralizados e à prova de adulteração, *blockchain* fornece uma nova maneira de proteger o sistema de compartilhamento de registos clínicos pessoais. Trata-se de um sistema transparente, pois todo participante pode consultar as transacções já realizadas e registadas; confiável, pois a validação se dá por intermédio de métodos de criptografia e consenso entre os membros; e de alta disponibilidade, pois opera em uma rede ponto-a-ponto com uma base de dados distribuída entre os nós da rede. Além disto, suas características ainda provêm os pilares da segurança da informação.

Assim, o presente trabalho culmina com o desenvolvimento de um protótipo baseado em *blockchain*, para a partilha de PC entre as US do SNS, onde os pacientes são inclusos para o controlo de acessos garantido sua privacidade. Como resultados, espera-se alta disponibilidade dos PC de qualquer US, incorruptibilidade, privacidade e autenticidade da informação.

Palavras-chave: SNS, *blockchain*, descentralização, processos clínicos, segurança, privacidade.

Abstract

The National Health System (NHS) is an entity governed by MISAU, created in 1991 by the Government of Mozambique, with the aim of promoting the health of all national citizens. To achieve these goals, one of the healthcare professionals' essential tool is the patient's medical history, which describes patient's clinical history during the different stages of his life. Hence, the importance of enabling the construction of a medical history which is complete, incorruptible and fully accessible by any health professional from any Health Unit (HU) of the NHS whenever necessary. For this, the patient's medical history need to be shared between the HU of the NHS.

The sharing of patient's medical history contributes to improve the accuracy of diagnoses and promotes the progress of the medical research. However, ensuring the privacy and integrity of this information and fine-grained access control are crucial issues to be taken into account when sharing patient's medical history.

As a distributed architecture with decentralized and tamper-proof features, *blockchain* provides a new way to secure the personal medical record sharing system. This is a transparent system, as every participant can consult transactions that have already been carried out and registered; reliable, as validation is through encryption methods and consensus among members; and high availability, as it operates in a peer-to-peer network with a database distributed among the network nodes. In addition, its features still provide the pillars of information security.

Thus, the present work culminates with the development of a blockchain-based prototype, for patient's medical history sharing between the HU of the NHS, where patients are included for access control, guaranteeing their privacy. High availability of the patient's medical history from any HU, incorruptibility, privacy and authenticity of the information are the expected results.

Keywords: NHS, blockchain, decentralization, patient's medical history, security, privacy.

Índice

Lista de figuras

Lista de Tabelas

Lista de abreviaturas e acrónimos

API - *Application Programming Interface*;

ARH - Administração de Recursos Humanos;

EHR - *Electronic Health Record*;

HCM – Hospital Central de Maputo;

HCB – Hospital Central da Beira;

IDE - *Integrated Development Environment*;

MISAU- Ministério da Saúde;

PC – Processo clínico;

SNS – Sistema Nacional de Saúde;

TIC – Tecnologias de Informação e Comunicação;

US – Unidade Sanitária.

Glossário de termos

Afecção – toda a alteração capaz de expressar uma doença; quaisquer sinais de patologia no corpo;

Incorruptível – característica daquilo que não sofre nenhum tipo de alteração;

Interoperabilidade - é a capacidade que um sistema (informatizado ou não) tem de se comunicar de forma transparente (ou o mais próximo disso) com outro sistema (semelhante ou não);

***Ledger* distribuído** - tipo de banco de dados que é compartilhado, replicado e sincronizado entre os membros de uma rede descentralizada. O *ledger* distribuído registra as transações, como a troca de ativos ou dados, entre os participantes na rede;

1. Capítulo I – Introdução

1.1 Contextualização

A qualidade de vida de qualquer indivíduo está directamente ligada a um quadro de saúde controlado. A busca por assistência médica durante o percurso de vida mostra-se um acontecimento incontornável, seja para prevenir, diagnosticar ou tratar determinada enfermidade. Neste contexto, quando um indivíduo, no caso, paciente, dá entrada numa unidade sanitária para o efeito, um registo é sempre feito. Este registo, pode evoluir para um conjunto ordenado de documentos e relatos sobre o estado de saúde do paciente em diferentes etapas de sua vida. De acordo com Morsch (2020) este conjunto ordenado de documentos é denominado processo clínico.

O processo clínico de um paciente reúne informações clínicas relevantes, tais como, exames médicos, diagnósticos, tratamentos efectuados, entre outros registos de processos pelos quais o paciente tenha passado, sem deixar de lado as, igualmente relevantes, informações administrativas do paciente, como o nome, data de nascimento, o número de identificação do paciente, endereço e contacto. Este histórico constitui a base para a tomada das melhores acções e decisões possíveis com relacção à saúde do paciente. Tratando-se, portanto, de uma ferramenta essencial para o trabalho dos profissionais de saúde no que respeita ao cuidado da saúde dos pacientes, é importante que os processos clínicos dos pacientes estejam sempre disponíveis quando e onde forem precisos, tal como defende Morsch (2020).

Em Moçambique, para efeitos de assistência médica e sanitária aos cidadãos, foi instituído, por meio do Ministério da Saúde (MISAU), o Sistema Nacional de Saúde (SNS). Constituído pelo sector público, sector privado com fins lucrativos, sector privado com fins não lucrativos e o comunitário, segundo o MISAU (2007). Cada um destes sectores comporta diversas unidades hospitalares que gerem processos clínicos de vários pacientes que buscam assistência médica.

De acordo com a Lei no 25/91 de 31 de Dezembro de 1991, para efeitos de assistência no SNS, os doentes devem, em regra, ser vistos, em primeira instância, numa unidade sanitária de nível primário. E sempre que, em determinada unidade sanitária, não existam recursos apropriados para o diagnóstico ou tratamento de determinado doente ou doença, o responsável clínico dessa deverá enviar o doente à unidade sanitária que consiga responder à necessidade. Algumas vezes os pacientes também procuram

assistência em diferentes unidades sanitárias de forma independente. Neste processo, segundo Wilson Honwana (2021), chefe do Arquivo Clínico do HCM, os processos clínicos não são partilhados; quando um paciente é transferido de uma unidade sanitária para outra, este leva consigo uma guia de transferência que contém apenas uma parte da sua informação clínica. Este procedimento mostra-se inconveniente em relacção a intervenção médica sobre a saúde do paciente, pois é necessário conhecer as condições do paciente antes de qualquer intervenção, o histórico clínico influencia na conclusão de diagnósticos, prevenção de doenças hereditárias, entre outros. Daí, a importância de se garantir a partilha dos processos clínicos pelas diferentes unidades sanitárias do SNS, promovendo a descentralização e alta disponibilidade da informação, conservando, sempre, a privacidade do paciente e a integridade da informação.

Neste contexto, os avanços da tecnologia têm sido cada vez mais aproveitados. Tecnologias como a *Blockchain* podem ser utilizadas para conseguir que os processos clínicos dos pacientes sejam partilhados a nível das unidades sanitárias que compõem o SNS, respeitando as exigências em torno do tratamento dos mesmos. Segundo afirma Da Silva (2020), *Blockchain* é uma tecnologia de registo descentralizada, incorruptível e criptograficamente segura. Pode-se dizer, também, que *blockchain* actua como um livro de registros distribuído onde somente pessoas autorizadas podem registrar informações. Esses registos são protegidos com o emprego da criptografia, além de só poderem ser feitos com a permissão da maioria dos integrantes da rede.

A partir disso, é possível criar um histórico completo de informações do paciente, que pode ser acedido de qualquer unidade hospitalar do SNS, independentemente de onde o processo clínico tenha sido aberto, com garantia de segurança, desde que esteja devidamente autorizada.

1.2 Motivação

É comum que um paciente precise visitar mais de uma unidade sanitária durante o seu curso de vida. E sempre que se vai observar a saúde, o histórico clínico é imprescindível para possíveis diagnósticos, tratamentos ou prevenção de alguma complicação no futuro. Raras vezes os pacientes podem detalhar o seu histórico clínico, quando o profissional de saúde precisa dele para intervir com diligência. É altamente necessário que os processos clínicos contendo este histórico sejam acessíveis à qualquer unidade sanitária que compõe o SNS ou profissional de saúde devidamente autorizados, independentemente de onde tal informação tenha sido colhida. O facto de um cidadão

mudar, por exemplo, a sua localização geográfica não pode implicar a inacessibilidade do seu histórico clínico, restringindo o acesso ao mesmo quando for preciso em intervenções futuras. Da mesma maneira, se os processos clínicos, além de partilhados forem armazenados de forma distribuída a nível dos hospitais do SNS, as probabilidades de indisponibilidade dos mesmos são, de certa forma, erradicadas.

Segundo Mandlate (2021), em Moçambique, os pacientes dependem de guias de transferências[1] para transportar, e de forma incompleta, os seus históricos clínicos. Se um hospital perde o processo clínico do paciente, o paciente fica sem histórico, tendo de repetir processos ou ser atendido sem informações críticas que podem mudar completamente a sua vida.

Desta forma, com recurso à tecnologia *blockchain* é possível mudar este cenário, fazendo com que os sistemas de gestão de processos clínicos dos hospitais que compõem o SNS actuem em interoperabilidade e descentralizando os processos clínicos dos pacientes.

1.3 Definição do problema

Segundo Rodrigues (2003), os processos clínicos são usados já desde o séc. V a.C., onde os profissionais de saúde registavam todas as informações clínicas dos pacientes em papéis, de forma manuscrita e os outros documentos auxiliares, como exames médicos, também eram anexados em formato físico. Actualmente, o sector da saúde tem sido beneficiado pelo potencial desenvolvimento das TIC, através da implementação de processos clínicos electrónicos. Em várias partes do mundo, os processos clínicos dos pacientes são guardados em formato electrónico, descontinuando o uso do papel.

Em Moçambique, o SNS ainda não descontinuou o uso do papel no tratamento dos processos clínicos dos pacientes, mas já começa a conhecer uma introdução aos sistemas electrónicos de gestão de processos clínicos. Vários pesquisadores, no geral, têm vindo a focar no desenvolvimento de sistemas de gestão de processos clínicos internos para as instituições de saúde, como é o caso de Garife (2016)[2], para acompanhar este desenvolvimento que traz consigo melhorias na conservação dos processos, a acessibilidade e, consequentemente, o tempo de espera dos pacientes nas

[1] É apresentada, no anexo 1, uma imagem ilustrativa de uma guia de transferência em uso no SNS.
[2] Desenvolvimento de um prontuário electrónico do paciente para auxiliar o sistema de saúde em Moçambique.

unidades sanitárias. Entretanto, estes sistemas não se comunicam entre si, fazendo com que os processos clínicos permaneçam centralizados, sendo que, em algum momento, os pacientes precisam visitar unidades sanitárias ou médicos diferentes, seja por mudanças geográficas, importunos ou pelo facto de um tratamento só poder ser complementado em outra unidade hospitalar. Nessas migrações, os processos clínicos precisam acompanhar os pacientes, pois carregam históricos importantes sobre a sua saúde. Isto constitui, ainda, um desafio no contexto Moçambicano, onde a transferência dos processos clínicos dos pacientes de uma unidade sanitária para a outra conhece limitações, pois as informações clínicas dos pacientes são centralizadas, ou seja, as informações clínicas levantadas em determinada unidade hospitalar, a cerca de determinado paciente, permanecem lá e quando este procura assistência em outra unidade hospitalar, o hospital não tem acesso ao histórico outrora composto na outra unidade hospitalar, o máximo que acontece é a emissão de uma guia de transferência, que também não vem com informação completa, ou simplesmente uma narração do paciente, que quase nunca tem capacidade para descrever o seu quadro clínico (uma vez que, este, nunca chega a possuir por completo as informações de suas visitas médicas). Esta realidade traz consigo consequências negativas como:

- Em cada unidade hospitalar por onde passa, o paciente possui um processo clínico, um conjunto de informações que, com a falta de interoperabilidade entre os sistemas de gestão de processos clínicos dos diferentes hospitais, fica disperso e sem relacção, dificultando aquele que é o estudo da evolução da saúde do paciente, tomada de decisões preventivas, diagnósticos em pouco tempo, inclusive, a realização de estudos.
- A repetição dos exames, que constitui um desgaste e custo para o paciente, não só de tempo de atendimento e resolução do seu problema, mas à própria saúde do paciente à medida em que alguns envolvem radiação (como, raio-x) ou são considerados procedimentos invasivos.
- A centralização dos processos clínicos aumenta as probabilidades de perda de informações essenciais dos pacientes.

Portanto, há uma necessidade de se olhar para os processos clínicos como um recurso partilhado entre os provedores de serviços de saúde a nível do SNS, com especial atenção à segurança da informação bem como a privacidade dos pacientes.

1.4 Objectivos

1.4.1 Objectivo Geral

- Propor uma plataforma de partilha de processos clínicos, para o SNS, baseada em *blockchain*, que garanta a descentralização, disponibilidade, integridade, privacidade e autenticidade da informação.

1.4.2 Objectivos específicos

- Descrever o funcionamento actual do Sistema Nacional de Saúde, no que respeita a partilha de Processos Clínicos;
- Identificar as principais técnicas de *blockchain* aplicáveis a processos clínicos;
- Construir um modelo de partilha de processos clínicos baseado em *blockchain*;
- Desenvolver um protótipo funcional para testar o modelo.

1.5 Metodologia

1.5.1 Classificação da metodologia de trabalho

Para o alcance dos objectivos estabelecidos no presente trabalho, as metodologias de trabalho aplicadas são baseadas na classificação que, de acordo com Gil (2002), podem ser: (a) quanto à abordagem, (b) quanto à natureza, (c) quanto aos objectivos e (d) quanto aos procedimentos.

- **Quanto à abordagem**

Segundo Coelho (2019), quanto à abordagem a metodologia de trabalho pode ser classificada em dois grupos, nomeadamente: o quantitativo e o qualitativo. Para estes, a abordagem quantitativa expressa e traduz em valores numéricos os conceitos e os dados para que possam ser analisados, julga que tudo pode ser representado por quantidades numéricas e para tal o processo requer recurso às técnicas estatísticas. Já na abordagem qualitativa, segundo Terence e Escrivão Filho (2006), o pesquisador procura aprofundar-se na compreensão dos fenômenos que estuda, as acções dos indivíduos, grupos ou organizações em seu ambiente e contexto social, interpretando-os segundo determinada perspectiva, sem se preocupar com representatividade numérica, generalizações estatísticas e relações lineares de causa e efeito.

A abordagem utilizada no decurso deste trabalho é classificada como qualitativa, já que é baseado na identificação e compreensão dos comportamentos e acções da

organização em estudo, através de interpretações sem bases necessariamente estatísticas.

- **Quanto à natureza**

Segundo Coelho (2019), quanto à natureza, a pesquisa pode ser básica ou aplicada. A pesquisa básica é aquela que tem como objectivo gerar conhecimentos úteis, envolvendo verdades e interesses universais, sem qualquer aplicação prática prevista, defendem Silveira e Gerhardt (2009). A pesquisa aplicada, por sua vez, visa gerar conhecimentos para aplicações práticas que solucionem problemas.

O trabalho em questão é classificado como uma pesquisa aplicada, uma vez que o objetivo é gerar conhecimentos para aplicações práticas, com vista a solucionar o problema da centralização das informações clínicas dos pacientes e a falta de interoperabilidade entre os sistemas de gestão de processos clínicos, no SNS.

- **Quanto aos objectivos**

Quanto aos objectivos, os trabalhos de pesquisa podem ser classificados de três formas: Pesquisa exploratória, descritiva e explicativa.

O presente trabalho é classificado como uma pesquisa exploratória e descritiva. Exploratória porque visa proporcionar uma maior familiaridade entre a investigadora e o caso em estudo, com recurso a todas a fontes possíveis que tal o permitam, possibilitando a identificação do problema e constrangimentos a serem resolvidos e descritiva porque tem em vista descrever o funcionamento actual do SNS, bem como as técnicas *blockchain* aplicáveis a processos clínicos no mesmo SNS.

- **Quanto aos procedimentos**

Quanto aos procedimentos, a metodologia utilizada durante a realização do presente trabalho é classificada como:

a) **Pesquisa bibliográfica**: pois foi necessária uma revisão bibliográfica, recorrendo aos materiais já publicados, conforme afirmam Gerhardt e Silveira (2009), que a pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas e publicadas por meios escritos e electrónicos como livros, artigos científicos ou páginas *web*.

b) **Estudo de caso**: Segundo Fonseca (2002) citado por Gerhardt e Silveira (2009), um estudo de caso pode ser caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social. Desta forma, a realização deste trabalho consistiu num estudo aprofundado sobre a entidade em questão, o SNS, buscando informações relevantes à cerca, como forma a trazer fundamentos teóricos em torno do caso de estudo.

c) **Pesquisa com Survey**: Segundo Santos (1999) citado por Gerhardt e Silveira (2009), a pesquisa com survey é aquela que busca informação directamente com um grupo de interesse a respeito dos dados que se deseja obter. Durante a realização do presente trabalho, foi preciso entrevistar alguns profissionais de saúde para perceber como o processo decorre e quais limitações/constrangimentos enfrentados.

d) **Pesquisa documental:** segundo Marconi e Lakatos (2003), a característica da pesquisa documental é que a fonte de coleta de dados está restrita a documentos, escritos ou não, constituindo o que se denomina de fontes primárias. Podendo, estas, ser feitas no momento em que o fato ou fenômeno ocorre, ou depois. Para este caso, a pesquisa documental foi utilizada para obter documentos originais, sem tratamento analítico, como a guia de transferência, para ilustrar como se partilham as informações clínicas dos pacientes entre os hospitais do SNS.

e) **Observação participante:** segundo Mann (1970) citado por Marconi e Lakatos (2003), a observação participante é uma tentativa de colocar o observador e o observado lado a lado, tornando o observador um membro do grupo em estudo de modo a permiti-lo vivenciar o que eles vivenciam e trabalhar dentro do sistema de referência deles. Durante a realização do presente trabalho, a pesquisadora tomou o papel de observador participante artificial, já que, apesar de não fazer parte, teve de integrar-se ao grupo dos profissionais da saúde para melhor obter informações e experiências sobre como é feita a partilha de processos clínicos a nível do SNS, actualmente.

- **Técnicas de recolha de dados**

Martins (2019) define coleta de dados como um processo que busca reunir os dados para uso secundário por meio de técnicas específicas. Tais dados são utilizados para

tarefas de pesquisa, planeamento, estudo, desenvolvimento e experimentos. Durante a pesquisa, foram utilizadas as seguintes técnicas:

- **Entrevistas**

Entrevistas, segundo Barbosa (2008), constituem um método flexível de obtenção de informações qualitativas sobre o caso em estudo. Esta técnica requer um bom planeamento prévio e habilidade do entrevistador para seguir um roteiro de questionário, permitindo variações no mesmo, caso necessário. Desta forma, para a coleta dos dados necessários para a concretização do presente trabalho de pesquisa, foi preciso recorrer a entrevistas com algumas entidades profissionais de saúde, mediante questões previamente elaboradas sobre aspectos relevantes para a construção do estudo. As respostas possibilitaram compreender como, na prática, é gerido o processo de partilha de processos clínicos dos pacientes entre as diferentes unidades sanitárias do SNS, bem como identificar os reais constrangimentos enfrentados.

- **Pesquisa bibliográfica**

A pesquisa bibliográfica constitui uma etapa imprescindível em todo o trabalho científico, esta fundamenta o trabalho. Consiste numa pesquisa exaustiva sobre o tema em questão por meio de artigos, livros, jornais, teses, físicos ou digitais, incluindo qualquer documento audiovisual relacionado ao tema em estudo, segundo Costa (2012). Para a elaboração do presente trabalho foi necessário pesquisar e consultar diversas bibliografias relaccionadas ao SNS, como forma a compreender o seu funcionamento, abrindo espaço para a identificação de uma solução que se adeque aos constrangimentos identificados.

1.5.2 Metodologia de desenvolvimento do protótipo da solução proposta

O protótipo da solução proposta será desenvolvido tendo em conta as fases da metodologia de desenvolvimento de software em cascata, segundo Royce (1970). Neste modelo, as actividades do processo de desenvolvimento são estruturadas numa cascata de forma linear e sequencial de forma que uma fase só poderá iniciar quando a anterior tiver terminado. Desta forma, as fases que compõem a metodologia de desenvolvimento em cascata são descritas a seguir:

a) Elicitação de requisitos: onde foram definidos os objetivos, indicadas as funcionalidades e necessidades que o sistema irá responder, tudo baseado nas informações levantadas e refinadas sobre o SNS, através de entrevistas e levantamentos documentais, resultando numa lista de requisitos refinada.

b) Análise: esta fase consistiu na compreensão dos requisitos e das funcionalidades do *software*, bem como os processos de modelação, produzindo uma especificação documentada da descrição completa do comportamento do *software*.

c) Projeto: onde é descrito como o sistema deverá ser implementado através da especificação da sua arquitectura e interface de utilizador

d) Implementação: onde são traduzidas as representações do projeto para uma linguagem de programação resultando em instruções executáveis pelo computador, ou simplesmente, onde acontece a codificação e consequente materialização do protótipo.

e) Testes: onde se são testados os aspectos lógicos do *software*, garantido que as funcionalidades do *software* estejam a funcionar conforme esperado. São testados, também, os aspectos funcionais externos, de modo a identificar erros e garantir que a entrada definida produza os resultados esperados.

f) Implantação e Manutenção: tendo o *software* passado nos testes, é então implantado e entra na fase de manutenção. Todas as modificações efectuadas no sistema após a entrega são consideradas parte da manutenção. Implantação: só vai acontecer caso o teste com alguma amostra população passe)

Nota: para este trabalho, por questões de tempo, será possível ir até a alínea f), pelo que, a última fase será a de testes.

1.5.3 Ferramentas e tecnologias

A solução proposta consiste no desenvolvimento de uma plataforma de partilha de Processos Clínicos entre as diferentes unidades hospitalares que compõem o SNS em Moçambique, baseada na tecnologia *blockchain*, permitindo a partilha completa das informações dos pacientes e consequente descentralização de tais informações. Desta feita, as tecnologias seleccionadas para o desenvolvimento da solução são apresentadas na tabela a seguir.

Tabela 1: Tecnologias empregadas para o desenvolvimento da solução proposta.

Tecnologia/ Ferramenta	**Denominação**	**Descrição**	**Justificativa**
JavaScript	Linguagem de programação	JavaScript é uma linguagem baseada em protótipos, multi-paradigma e dinâmica, suportando estilos de orientação à objectos, imperativos e declarativos (como por exemplo a programação funcional).	É considerada a linguagem mais usada para a *web* e, portanto, com alta disponibilidade de suporte. É uma linguagem intuitiva, próxima da linguagem humana, consequentemente, fácil de usar.
Node.js		O Node.js é uma tecnologia que utiliza o JavaScript como sintaxe. Seu principal uso está na construção de API's.	Seu modelo assíncrono, consome pouquíssimos recursos do *hardware* tornando-o excelente para a tarefa.
React.js	Biblioteca	O React.js é uma biblioteca JavaScript de código aberto com foco em criar interfaces de utilizador em páginas *web*.	Permite que os estados das interfaces de utilizador sejam escritos e modelados de forma declarativa. O que significa que, ao invés de descrever passo-a-passo transacções em interfaces, os desenvolvedores apenas descrevem as interfaces em termos de um estado final.
Visual Studio Code	IDE (Ambiente de Desenvolvimento Integrado)	O Visual Studio Code, aliado à extensão *Blockchain VSCode*, é um ambiente de desenvolvimento que possibilita a construção de aplicações baseadas em *blockchain* através da possibilidade de conexão com ambientes que suportam o desenvolvimento desta tecnologia, permitindo aos desenvolvedores criar e testar as aplicações.	A extensão VSCode acompanha uma galeria de tutoriais fáceis de seguir e focados em manipular *blockchain* nesses casos. A galeria de tutoriais da extensão VSCode é uma boa opção para iniciantes.

1.6 Questão de pesquisa

- Como promover a partilha de processos clínicos de pacientes com garantia de segurança da informação e privacidade dos pacientes?

1.7 Estrutura do trabalho

O presente trabalho está organizado em seis (6) capítulos e duas (2) secções referentes a bibliografia e anexos, cujas descrições dos mesmos encontram-se a seguir:

Capítulo I – Introdução: esta é a parte do trabalho em que, de forma clara e objectiva, se aborda o assunto em estudo, como forma a prover uma contextualização da pesquisa. Constituída por uma contextualização do tema, motivação da pesquisa, definição do problema, definição dos objectivos e metodologias empregada.

Capítulo II – Revisão de Literatura: neste capítulo são apresentados os tópicos relevantes à pesquisa, como base teórica para a construção do modelo de partilha de processos clínicos baseado em *blockchain*, no SNS.

Capítulo III – Caso de estudo: neste capítulo é descrito o modelo de funcionamento actual em relacção a partilha de processos clínicos no SNS, os constrangimentos identificados e a proposta da solução mais adequada ao problema identificado.

Capítulo IV – Desenvolvimento da solução proposta: neste capítulo está patente a modelagem e concepção do protótipo funcional da solução.

Capítulo V – Discussão dos resultados: neste capítulo serão apresentados os resultados da pesquisa realizada.

Capítulo VI – Considerações finais: neste capítulo encontra-se uma análise para avaliação do nível de alcance dos objectivos definidos no início do trabalho, apresentação das conclusões a que se tenha chegado e, no caso de alguma deficiência no alcance dos objectivos definidos, são deixadas recomendações para trabalhos futuros que tenham a mesma natureza.

Secção das Bibliografias: nesta secção são apresentadas todas as fontes utilizadas e consultadas durante a pesquisa e redação do relatório.

Secção dos Anexos: nesta secção são apresentados elementos que especificam o sistema e seu processo de construção e outros elementos que tenham contribuído para a concretização do trabalho.

2. Capítulo II – Revisão de Literatura

2.1 O Sistema Nacional de saúde

O Sistema Nacional de Saúde, em Moçambique, foi instituído em 1991, à luz da Constituição da República de 1990, que reestabeleceu o direito à assistência médica e sanitária a todos os cidadãos, por meio do MISAU. Criado com o objectivo de promover a saúde, prevenção de doenças, assistência e reabilitação, associando-se à formação de recursos humanos e pesquisas para seu contínuo desenvolvimento, segundo a Lei n.º 25/91 de 31 de Dezembro.

Desde a instituição do SNS, em 1991, o sector público foi sempre o principal prestador de serviços de saúde a nível nacional. No entanto, reconhecendo, ainda em 1991, com o advento da democratização do país, a sua incapacidade de ser o único provedor de serviços de saúde, integrou ao Sistema as actividades da assistência médica privada, em conformidade com o Decreto-Lei nº 5/75, de 10 de Agosto, nacionalizadas após a independência do Estado. Assim, o SNS é, actualmente, constituído pelos seguintes sectores:

- Público;
- Privado com fins lucrativos;
- Privado com fins não lucrativos;
- Comunitário.

Segundo o MISAU (2007), o SNS está organizado em quatro níveis de prestação de serviços (ou de atenção):

Nível primário - constituído por centros e postos de saúde, cada um deles compreendendo a respectiva área de saúde[3], tem como função executar a estratégia de cuidados de saúde primários. Estas unidades sanitárias constituem o primeiro contacto da população com os Serviços de Saúde. Tendo sob a sua responsabilidade a saúde da população e do ambiente, estas devem assegurar a cobertura sanitária de uma população dentro de uma zona geográfica bem definida pela Área de Saúde.

[3] Área de Saúde - Entende-se por área de saúde a unidade territorial com uma população variando entre 100 000 e 200 000 habitantes, aproximadamente, servidos por um centro ou posto de saúde.

Nível secundário - formado por hospitais distritais, gerais e rurais, tem como função prestar cuidados de saúde secundários e constitui o primeiro nível de referência para os doentes que não encontram resposta nas unidades sanitárias de nível primário.

Nível terciário - composto por hospitais provinciais, constituem uma referência para os doentes que não encontram soluções ao nível dos hospitais distritais, rurais e gerais, bem como dos doentes provenientes de hospitais distritais e centros de saúde que se situem nas imediações do hospital provincial e que não haja hospital rural nem geral para onde possam ser transferidos.

Nível quaternário – constituído por hospitais centrais e especializados, é uma referência para os doentes que não encontram soluções nos níveis abaixo. Neste nível, situam-se, também, os Hospitais Especializados que prestam cuidados muito diferenciados de uma só especialidade.

Em suma, os primeiros dois níveis têm como missão a prestação de cuidados primários e o encaminhamento dos pacientes com condições clínicas mais graves, tais como complicações no parto, traumas, emergências médicas e cirúrgicas, entre outras, para os níveis seguintes. Os dois últimos níveis estão essencialmente destinados à prestação de cuidados mais especializados.

Hospital: segundo o Diploma Ministerial nº 127/2002, é um local de prestação de cuidados clínicos, em regime de internamento e de atendimento em ambulatório a doentes que não encontram solução para os seus problemas de saúde em níveis inferiores. O Hospital oferece sempre a possibilidades de diagnóstico clínico, com apoio laboratorial e de outros exames complementares e constituem sempre um nível de referência. O Hospital oferece, também, a possibilidade de cuidados de urgência aos traumatismos e outras afecções. O hospital tem sempre disponível um médico.

Hospitais distritais, gerais e rurais: um Hospital Rural distingue-se de um Hospital distrital por possuir condições para a realização de intervenções cirúrgicas e dispor de internamento com serviços individualizados para quatro especialidades básicas: Medicina Interna, Pediatria, Cirurgia e Obstetrícia e Ginecologia. Por sua vez, os Hospitais Gerais são semelhantes aos Rurais, o que os diferencia é a localização, os Hospitais Gerais localizam-se, sempre, em zonas urbanas.

Os centros e postos de saúde: estão direccionados a prestação de cuidados primários. Os cuidados primários proporcionam o primeiro nível de contacto do indivíduo, da família e da comunidade com o sistema nacional de saúde, permitindo a aproximação da assistência de saúde o mais possível dos locais onde a população vive e trabalha, e constituem o primeiro elemento de um processo permanente de assistência de saúde. Os cuidados primários têm como objectivo reduzir as altas taxas de mortalidade impostas por doenças transmissíveis, incluindo problemas de saúde associados a mortalidade materna.

Linha hierárquica das unidades sanitárias

O MISAU é o órgão central do Sistema Nacional de Saúde, responsável pela definição das políticas que regem o funcionamento do Sistema Nacional de Saúde.

Cada Província do país tem uma representação do MISAU, que se denomina Direcção Provincial de Saúde (DPS).

Em cada Distrito existe uma representação distrital do Sistema Nacional de Saúde que é o Serviço Distrital de Saúde, Mulher e Acção Social (SDSMAS).

Portanto, as Unidades Sanitárias relacionam-se com o SDSMAS correspondente, o SDSMAS, por sua vez, com a DPS da sua Província e as DPS relacionam-se com o MISAU.

2.2 Abordagens utilizadas para a partilha de processos clínicos

Em Moçambique

Em Moçambique, os processos clínicos não são completamente partilhados entre as unidades sanitárias. Apenas uma parte da informação é partilhada em um documento denominado guia de transferência, para o caso de pacientes que são transferidos de uma unidade sanitária para outra. Ou então, através da requisição de um relatório médico, que também não consta informação detalhada. Os processos clínicos permanecem nas unidades sanitárias em que são criados, apenas em casos muito excepcionais são entregues aos pacientes, uma prática muito recente, com vista a contornar o desafio da perda dos processos clínicos nas unidades sanitárias, mas que não garante qualquer garantia de conservação do mesmo para que possa ser partilhado com outras unidades.

Em outros países, a partilha completa de processos clínicos ao nível dos prestadores de serviços de saúde já é dada a devida importância, a ponto de serem adoptadas tecnologias que permitam esta partilha da melhor maneira dentro do contexto e possibilidades de cada um.

Mecanismos de partilha de processos clínicos em outros países

Bélgica

No final de 2004, o governo belga criou a *BeHealth*, uma plataforma para organizar e coordenar a partilha mútua de informações clínicas electrónicas dos pacientes entre todas as partes integrantes do sistema de saúde. Como uma instituição pública, o principal mandato da plataforma *BeHealth* tem sido para permitir que vários sistemas de troca de dados de saúde floresçam em várias regiões do país, assegurando ao mesmo tempo que todos estarão interligados. Actualmente, restrito a operar a nível local, *BeHealth* está trabalhando na conexão dos cinco centros regionais existentes (um para a Valónia, um para Bruxelas e três na Flandres) através do *«Hub-Metahub»*, projeto (em francês). Por exemplo, em abril de 2012, a rede de saúde da Valónia, o Centro da Valónia, incluiu aproximadamente 30.000 pacientes, 4.000 profissionais de saúde e 17 hospitais. No ano de 2011-2012, quase 900.000 documentos foram partilhados através da rede.

França

A França implementou o Dossiê Médico Pessoal (DMP), acessível aos pacientes por meio de serviços da *Web* e sob a responsabilidade das agências regionais de ARH. Para aceder ao DMP, o profissional de saúde precisa do consentimento do paciente que também pode escolher negar o acesso a determinados profissionais de saúde. O DMP tem sido objecto de polêmica na França com um apelo ao Conselho de Estado para que o declare inconstitucional. O Conselho rejeitou a alegação, porém o governo, posteriormente, instituiu maiores salvaguardas.

Além disso, a França implementou o *Dossier Pharmaceutique*. De acordo com a associação dos farmacêuticos franceses, mais de 25 milhões de *Dossier Pharmaceutic* foram implementados, e 97,6 das farmácias estão conectadas.

Outros países como Israel, Brasil, EUA e Holanda abraçaram soluções para partilha de processos clínicos baseadas em *blockchain*, que são descritas a seguir.

2.2.1 Sistemas baseados em *blockchain*, em uso a nível de outros países

MedRec

Investigadores do MIT Media Lab e do Beth Israel Medical Center propuseram o MedRec, um sistema para gestão de registos baseados em *blockchain*, principalmente para lidar com EHR. O objectivo principal do projecto é gerir a autenticação, a confidencialidade, a responsabilização e a partilha dos dados.

A MedRec não armazena os dados de saúde dos doentes. Apenas armazena a assinatura do registo na *blockchain* e notifica o seu titular, que por sua vez está em controlo absoluto dos locais para onde esse registo pode ir. Esta particularidade transfere o ónus do controlo do registo e das permissões da instituição de saúde para o utente. As permissões são definidas através de um conjunto de *smart contracts* que especificam os termos e condições sob os quais alguém tem acesso remoto aos dados de um EHR.

Baseado no princípio da interoperabilidade, o sistema foi desenhado para permitir o suporte de padrões para a partilha de dados, como o [FHIR ou outros da HL7][4]. No entanto, não está garantida a leitura dos dados, devido a incompatibilidades entre *softwares* de leitura.

OmniPHR

O OmniPHR é um modelo de uma arquitectura distribuída para integrar registos clínicos pessoais, proposto por investigadores da Universidade do Vale do Rio dos Sinos do Brasil. Este modelo foca-se na distribuição e na interoperabilidade dos dados de PHR. Para o seu desenvolvimento, o OmniPHR baseia-se num conjunto de funções tecnológicas, que visam melhorar a sua funcionalidade, além de que já incorpora o padrão openEHR.

Este modelo, introduz uma inovação em relacção aos demais. Suporta uma componente adicional na sua arquitectura primariamente responsável pela interoperabilidade, que é o *translator*. Este componente só é utilizado quando existe um padrão diferente do utilizado no modelo OmniPHR, que neste caso é o openEHR. Se o prestador utilizar um

[4] HL7 e FHIR são padrões de interoperabilidade de dados médicos provem as bases para intercambiar informações entre sistemas.

padrão diferente, quer seja um open standard ou não, o *translator* é activado para converter os blocos de dados quando eles passam por um *ultrapeer*[5]. No entanto, este componente representa um grande desafio para os autores devido à heterogeneidade de padrões que podem ser utilizados.

FHIRChain

A FHIRchain é uma iniciativa nascida na Universidade de Vanderbilt nos EUA e da *Varian Medical Systems*. Os seus autores propõem uma arquitectura baseada em *blockchain* para a partilha de dados que cumpra os requisitos definidos no "*Shared Nationwide Interoperability Roadmap*" do *Office of the National Coordinator for Health Information Technology* (ONC), através do encapsulamento do padrão da *HL7 Fast Healthcare Interoperability Resources (FHIR)*.

A adoção do padrão FHIR em combinação com a tecnologia *blockchain*, a FHIRChain, facilita a partilha de dados sem a necessidade de fazer *uploads* ou *downloads* de dados, através da troca de *pointers* na *blockchain* que referenciam dados armazenados em bases de dados isoladas. Esta particularidade pode revelar-se vantajosa para superar problemas de rede existentes em áreas rurais, por exemplo.

GuardTime

A GuardTime é uma empresa de segurança de dados holandesa que, em parceria com o governo da Estónia desenvolveu uma *framework* baseada em *blockchain*. Neste sistema, a tecnologia *blockchain* é utilizada para assegurar a integridade dos EHR armazenados, assim como registar todos os acessos ao sistema. Cada pessoa na Estónia, que tenha visitado um médico, tem o seu registo electrónico *online*. Este registo contém notas, resultados de testes, prescrições médicas electrónicas, imagiologia e também um ficheiro que acompanha os acessos aos dados. Assim, os clínicos podem aceder aos registos electrónicos dos doentes onde quer que estejam e, consequentemente, agir de maneira informada de modo a tomarem as melhores decisões. Com efeito, em 2017, eram cerca de um milhão de registos clínicos armazenados através deste sistema. Concluindo-se que o caso da Estónia é a prova de

[5] Utilizadores que direccionam requisições de busca e respostas para utilizadores conectados a eles, em vez de agirem como cliente e servidor como os demais.

que é possível operar os sistemas de informação de uma infraestrutura pública de saúde baseada em *blockchain*.

2.3 A tecnologia *Blockchain*

Segundo Boiani (2018), *Blockchain* é uma estrutura de dados onde os registos são guardados em uma sequência de blocos interligados. Esta sequência forma um *ledger* distribuído, o que significa que é replicada em várias máquinas, chamadas de nós, que se comunicam entre si. Os nós formam uma rede ponto a ponto em que cada actualização do *ledger* deve ser aceita pela rede usando um protocolo de consenso. O protocolo de consenso garante que todos tenham a mesma visão sobre o estado do sistema.

A *Blockchain* foi introduzida em 2008, como a tecnologia base de uma criptomoeda denominada *Bitcoin*, com o objectivo principal de permitir a troca de valores monetários digitais entre pares sem a mediação de uma autoridade central terceirizada e melhorar a segurança das transacções financeiras. Contudo, ao longo do tempo foi se mostrando útil para diferentes aplicações como é o caso do sector da saúde, promovendo a segurança em termos de como as informações dos pacientes são conservadas e compartilhadas entre as diferentes entidades interessadas.

No contexto dos registos clínicos, conforme afirma Yuhong & Zhang (2018), um sistema de *blockchain* pode ser considerado como uma base de dados distribuída[6], criptográfica e virtualmente incorruptível onde informações médicas críticas podem ser guardadas. O sistema é mantido por uma rede de computadores, ou seja, acessível a qualquer pessoa que execute o *software*. *Blockchain* opera como um sistema pseudo-anónimo que vela, ainda, pela questão de privacidade, uma vez que todas as transações são expostas ao público, e à prova de falsificação no que concerne a integridade da informação. O controle de acesso de registos de saúde de pacientes diferentes, em instituições e agentes de saúde diferentes, estaria devidamente acautelado.

Portanto, além da descentralização, a *blockchain*, ainda, assegura os pilares da segurança da informação. A seguir, são apresentadas as principais características da tecnologia *blockchain*.

[6] "Um *banco de dados distribuídos* é uma colecção de dados pertencentes logicamente a um sistema, mas distribuídos sobre vários sítios de uma rede de computadores". (Hopper, 1995)

2.3.1 Características de uma *blockchain*

a) Descentralização da informação

Segundo Rocha & De Paula (2019), a descentralização da informação refere-se à dispersão da informação, evitando que uma entidade central tenha o poder sobre ela. Na *Blockchain*, a descentralização deve ser observada por dois lados:

- **quem detém o poder de realizar alguma acção sobre uma informação:** no caso da informação estiver centralizada em uma entidade, no sentido de apenas ela ter o poder de realizar qualquer acção sobre essa informação. Note-se que diversas instituições funcionam dessa forma. Por exemplo, os processos clínicos têm os seus respectivos titulares, entretanto apenas a unidade sanitária onde os mesmos tenham sido abertos tem o poder de manipular a informação lá presente.
- **quem possui fisicamente a informação:** quando a informação está unicamente sob posse de uma entidade. Na linha do exemplo dos processos clínicos, estes estariam armazenados em infra-estruturas próprias de determinada unidade sanitária, onde entidades externas não têm acesso.

A *blockchain* visa que as informações não estejam centralizadas nem da perspectiva do poder para realizar alguma acção, nem da perspectiva do armazenamento físico.

No primeiro caso, os participantes decidem, em conjunto, sobre qualquer alteração sobre as informações. Para tal, os participantes precisam consentir sobre a validade da modificação que se pretende realizar. No segundo caso, cada um dos participantes possui uma réplica da informação armazenada consigo, em sua máquina, evitando a centralização física da mesma.

b) Disponibilidade

A disponibilidade da informação está estritamente relaccionada à descentralização. A partir do momento em que a informação se encontra distribuída pelos computadores dos participantes, ela torna-se disponível para ser utilizada independentemente da falha de um ou outro computador.

O conceito utilizado para garantir a disponibilidade da informação na *blockchain* é a replicação da informação. Neste sentido, a mesma informação precisa estar replicada e distribuída em vários pontos. A *blockchain* realiza a replicação utilizando a rede *peer-to-peer* (uma arquitectura de redes de computadores onde cada um dos pontos ou nós da

rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central). Além da replicação, caso novas informações sejam inseridas, é necessário que todas as réplicas sejam sincronizadas.

c) Privacidade

A privacidade permite que todas as operações na *blockchain*, denominadas transacções, sejam realizadas de forma anónima, evitando que terceiros saibam, exactamente, que entidade as protagonizou. Para tal, são utilizadas técnicas de criptografia, que permitem que uma entidade (no mundo real) seja identificada (na *blockchain*) somente através de um identificador. Nesse sentido, um terceiro, mesmo tendo acesso a toda a *blockchain*, apenas poderá visualizar as operações feitas identificadas por números, sem saber quem é a pessoa ou instituição por trás deles.

d) Integridade

A integridade da informação constitui um dos pilares da segurança da informação, e garante que a informação não seja corrompida, ou seja, que não sofra alterações não autorizadas ou impróprias. Neste sentido, a *blockchain* utiliza o conceito de cadeia, que permite criar um enlace entre as informações. Para a criação desses enlaces, na *blockchain*, cada elo corresponde a um bloco de informações. Este bloco é criado com um identificador único e nele são inseridas as operações (transações) realizadas pelos utilizadores. O elo entre dois blocos é realizado fazendo com que um bloco contenha o identificador do bloco anterior, formando assim o enlace.

e) Imutabilidade

A imutabilidade na *blockchain, s*egundo Rocha & De Paula (2019), diz respeito a propriedade de as informações (sejam elas as transações contidas em um bloco, ou as informações do cabeçalho do bloco) não poderem ser alteradas a partir do momento em que são inseridas na cadeia. Existem, contudo, informações que variam com o tempo. No caso de um processo clínico, por exemplo, com o tempo ele vai sendo actualizado e para permitir estas modificações, a *blockchain* cria um novo bloco, inserindo essa alteração como uma nova transação. Note-se que, com isso, a cadeia possuirá todas as modificações realizadas na informação, formando um histórico completo, e não somente o último estado dela.

f) Auditabilidade

A auditabilidade na *blockchain* permite verificar, por qualquer um que possua a cadeia, que todas as informações contidas nela são válidas. Para tal, é preciso verificar que tanto os blocos quanto as transações são válidas. No primeiro caso, é necessário validar que cada bloco aponte para o bloco anterior, até chegar ao primeiro bloco gerado, seguindo o enlace explicado na integridade de blocos. Já no segundo caso, é necessário verificar se todas as transações de uma determinada pessoa ou instituição (pelo anonimato, será mostrado, apenas, um identificador) apresentam coerência, no contexto da utilização da *blockchain*.

2.3.2 Estrutura básica de uma *Blockchain*

Conforme mencionado, a *blockchain* é composta por uma cadeia interligada de blocos e os blocos, por sua vez, divididos em duas partes: cabeçalho e transacção.

O cabeçalho consiste em diversos metadados que identificam unicamente o bloco. A lista de transacções identifica as transacções realizadas e contidas nesse bloco. Note-se que o conceito de transacção é bem geral, podendo ser tanto as informações de um movimento financeiro quanto às informações de um processo clínico do paciente.

A seguir, são apresentados os principais campos que compõem o cabeçalho de um bloco:

Previous Block Hash: apontador para o cabeçalho do bloco anterior;

Merkle Root: número único que determina as transacções que existem no bloco;

Timestamp: data e hora aproximada da criação do bloco;

Difficulty Target: nível de dificuldade na criação do bloco;

Nonce: número que determina como foi criado o bloco.

Suponha-se o seguinte cenário, de acordo com Rocha & De Paula (2019):

Uma médica atende um paciente, às 08:00h, e regista os resultados dessa consulta em um processo clínico. Para que ambos possam visualizar essa informação, será necessário, também, que algum computador armazene o processo clínico.

No mesmo dia, às 19:30h, o paciente se consulta uma segunda vez com a mesma médica. Após o atendimento, ela regista as informações no processo clínico do paciente, gerando um novo bloco que, por sua vez, contém uma nova transacção. Na figura a seguir, pode-se observar algumas informações do cabeçalho gerado pelo sistema para o bloco 2, do segundo atendimento.

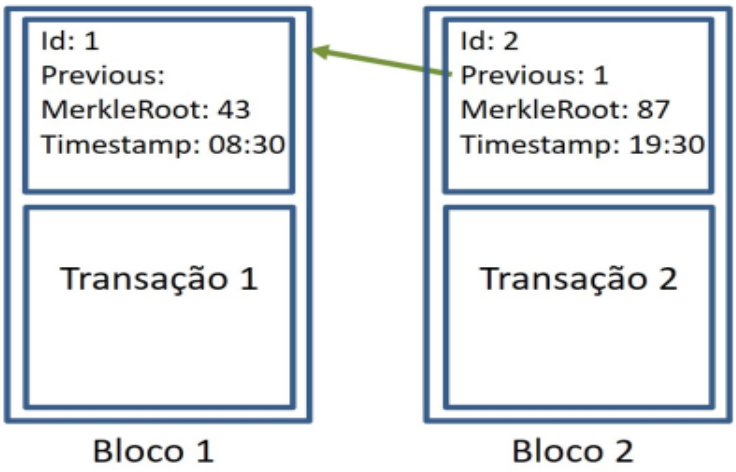


Figura A: Cadeia de Blocos com cabeçalho.

Fonte: Rocha & De Paula (2019)

No bloco 2, o valor do *Previous Block Hash* corresponde ao identificador do bloco 1. Além disso, o sistema gera um valor que determina as transacções que existem no bloco (*Merkle Root*) e a hora em que o bloco foi criado, isto é, às 19.30 (*timestamp*).

O *Previous Block Hash* do bloco 1 vai apontar para um bloco inicial denominado bloco génesis. O bloco génesis é o primeiro bloco de uma cadeia de blocos e todos os computadores que façam uso da *blockchain* devem conhecê-lo. Portanto, incluindo o bloco génesis, a cadeia do cenário suposto é apresentada na seguinte disposição:

Figura B: Cadeia de Blocos com génesis.

Fonte: Rocha & De Paula (2019)

Bloco

Um bloco é a unidade básica de dados de uma rede *blockchain*. Se caracteriza por ser uma estrutura de dados responsável por armazenar informações sobre um conjunto de transacções.

Transacções e cadeia de transacções

Em cada bloco são inseridas as transacções realizadas pelos utilizadores do sistema. Uma transacção pode ser observada como um evento que ocorreu no sistema. No cenário anteriormente suposto, da consulta médica, o evento seria a inserção de um registo no processo clínico electrónico do paciente e a permissão de visualização do processo clínico.

De forma geral, uma transacção é composta por um identificador único da transacção e dois módulos: entradas e saídas. A entrada representa o identificador do utilizador que protagoniza a transacção e a saída representa o identificador do utilizador que recebe a transacção. A título de exemplo, a figura a seguir ilustra como seria a transacção de uma transferência financeira de 5 unidades de uma pessoa com identificador ID1 para outra com identificador ID2.

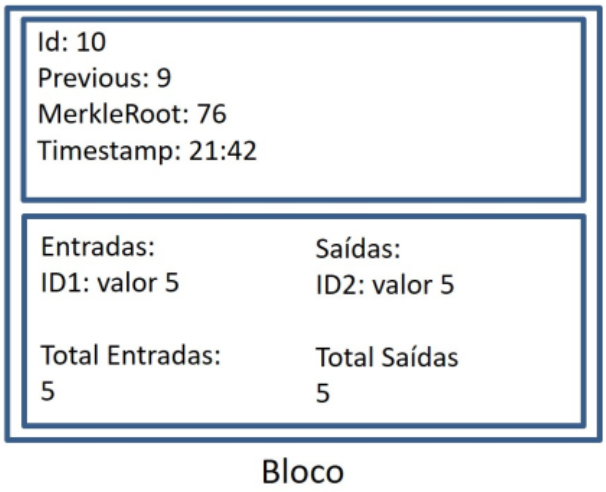


Figura C: Transacção

Fonte: Rocha & De Paula (2019)

Para garantir que ID1 realmente tinha posse do item transferido, o procedimento é semelhante ao dos cabeçalhos, as transacções devem apontar para uma transacção válida, isto é, que já exista em algum bloco da cadeia. Assim, no caso de alguém quiser verificar se ID1 possui ou não o item, basta verificar todas as transacções realizadas por tal identificador por meio dos apontadores das transacções.

Nó

A *blockchain* é constituída por nós que formam os pares interligados. Um nó de rede física é um dispositivo electrónico activo que está ligado a uma rede, e é capaz de enviar, receber ou transmitir informações através de um canal de comunicação.

Rede peer-to-peer

Segundo Tanenbaum (2010), em uma rede *peer-to-peer*, os nós agem como clientes e servidores para os outros nós da rede. Quando comparado ao modelo cliente/servidor, onde só há um servidor recebendo e processando requisições, no modelo *peer-to-peer* os nós compartilham responsabilidades de servir a outros nós. Assim, não há um ponto de controle único. É importante notar que para que essa troca de informações ocorra, os nós têm de concordar com um conjunto de regras previamente definidas para a comunicação.

Chave primária e chave pública

Para garantir a segurança da informação partilhada, a *blockchain* tem como recurso a criptografia. A criptografia, conforme define Pereira (2016), é um conjunto de técnicas empregada para cifrar mensagens, as quais são decifradas por meio de uma chave. Assim, apenas o emissor e o receptor da informação têm acesso ao conteúdo enviado. Pessoas terceirizadas conseguem, apenas, ver códigos aleatórios sem a possibilidade de visualizar o real conteúdo.

Dentro da criptografia, existem duas alternativas: a simétrica e a assimétrica. Na simétrica, faz-se uso do mesmo código tanto para a codificação quanto para a decodificação, assim, origem e destino precisam partilhar o mesmo código. Na assimétrica, são utilizados dois códigos diferentes, um para a codificação e outro para a decodificação. Portanto, para transferências seguras, a *blockchain* faz uso da criptografia assimétrica, onde existem duas chaves, a pública e a privada, que estão relaccionadas entre si.

Segundo Rocha & De Paula (2019), a chave privada permite identificar unicamente o emissor da mensagem, já que é a única pessoa que deverá ter posse dela (o que significa que essa chave não deve ser partilhada com ninguém). Por outro lado, o receptor da mensagem poderá verificar que essa mensagem realmente corresponde ao emissor, dado que a única forma de decriptá-lo é utilizando a chave pública correspondente a essa chave privada.

Função *Hash*

Segundo Mironov (2005) citado por Rocha & De Paula (2019), função *hash* é um algoritmo de compactação da informação, caracterizado por evitar conflitos, ser determinístico e de uma via.

A característica de evitar conflitos está relaccionada ao facto de diferentes textos não poderem ter como resultado o mesmo código. O determinismo está relaccionado à propriedade de a compactação de um texto inicial ter sempre como resultado o mesmo código e a característica de uma via, garante que o texto original não seja sugestivo a partir do código do texto compactado.

Portanto, o mecanismo utilizado pela *blockchain* para compactar a informação chama-se *hash*, e permite compactar um texto de tamanho qualquer em outro de tamanho fixo.

Para a implementação da compactação são utilizados alguns algoritmos, tais como o MD (2,4 e 5), SHA (1 e 2), RIPEMD, PANAMA e TIGER.

2.3.3 Tipos de *blockchain*

Segundo Buterin (2015), existem dois tipos de *blockchain*: permissionadas e não permissionadas. Nas *Blockchain* não permissionadas, qualquer membro pode executar alguma modificação e auditar a cadeia. Nas permissionadas, apenas os membros autorizados podem executar operações na cadeia. É comum associar a *blockchain* não permissionada à *blockchain* pública e a *blockhain* permissionada às instâncias privadas, federadas ou em consórcio.

***Blockchain* não permissionada** - segundo Rocha & De Paula (2019), *blockchain* não permissionada, permite que qualquer entidade possa entrar e sair do sistema a qualquer momento. Ao entrar, a entidade transforma-se em um membro que pode realizar modificações e auditorias na cadeia inteira de blocos. Portanto, pela potencial possibilidade de cada membro possuir a cadeia de blocos, neste tipo de *blockchain* predomina uma total descentralização da informação. Exemplos deles são *Bitcoin* e *Ethereum*.

***Blockchain* permissionada** - na *blockchain* permissionada, somente algumas entidades são transformadas em membros do sistema e, então, tem permissão para realizar operações na cadeia. Dessa forma, algumas podem ler os blocos, outras escrever e outras auditar. Para permitir a identificação e autorização dos membros, torna-se necessária a criação de responsáveis por gerir as permissões. Neste tipo de *blockchain* existem entidades que realizam o papel de autorizadores. Segundo Spruit & Brinkhuis (2018), este tipo de *blockchain* opera, no entanto, em ambientes onde os participantes têm identidades verificadas e são convidados a participar, aceitando direitos de acesso de utilizadores específicos. Isso pode ser útil para aplicativos de negócios com o requisito de nós identificados devido a razões legais e de conformidade. Exemplos de *Blockchain* permissionada são as plataformas *Hyperledger Fabric* e *Corda*.

Rocha & De Paula (2019) afirmam, ainda, que as aplicações *blockchain* que requerem identificação de usuários, tendem a ser construídas usando infraestrutura permissionada. Por outro lado, estruturas não permissionadas tendem a oferecer maior anonimato. Outra questão importante para a escolha de tipo de *blockchain* é a criação e

manutenção da infraestrutura que suporta a rede de nós. Uma *blockchain* privada normalmente é de responsabilidade de uma instituição que a mantém operacional; nesse sentido, as *blockchain* públicas ou federadas concentram menos o poder de decisão sobre a rede.

2.3.4 Mecanismo de Consenso

O consenso tem em vista que os computadores cheguem a um acordo sobre um determinado estado ou valor. Alves, Nasser, & Laigner (2018), define mecanismo de consenso como um conceito de computação distribuída usado na *blockchain* para prover um acordo na definição de uma versão única do bloco que será enviada para todos os nós da rede sem a necessidade de uma autoridade central.

A seguir, são apresentados dois dos mecanismos de consenso mais utilizados na tecnologia *blockchain*: *Proof of Work (PoW)* e *Proof of Stake (PoS)*.

- **Mecanismo de consenso via *Proof of Work (PoW)*:** neste tipo de consenso, todos os computadores podem ser passíveis por realizarem o processo de consenso, diferente do Paxos onde somente alguns são os escolhidos. Para comportar os possíveis milhares de computadores, a escolha de um líder não é a mais adequada, haja vista que esse líder talvez não será capaz de lidar com todas as mensagens advindas de todos os computadores. Assim, será necessário criar um processo que não dependa somente de um computador.

  Funcionamento:

  Essencialmente, o processo começa com um computador (denominado minerador) obtendo de outro computador a cadeia de todos os blocos, com suas respectivas transacções, que existe até esse momento. Suponha-se uma cadeia de 100 blocos. Em posse desse histórico, o minerador, que será denominado de M1, deve verificar que cada uma das transacções é válida e que cada bloco é válido.

  Tendo realizado as validações, o minerador M1 obterá novas transacções que foram realizadas pelos clientes (e que não existem em nenhum bloco anterior), criando um novo bloco com essas transacções.

  Na criação do bloco é necessário preencher as informações do cabeçalho do mesmo. Primeiro, o campo '*timestamp'* corresponde à hora do computador do minerador, por exemplo, 12/02/2019 13:30. A seguir, o campo '*Previous Block*

Hash' deverá apontar para o bloco 100, calculado através do *hash* desse bloco 100.

- **Mecanismo de consenso *Proof of Stake (PoS)***: diferente do mecanismo *proof of work*, em *blockchains* que adoptam a *Proof of Stake*, não há mineradores, mas sim validadores. O algoritmo *Proof of Stake* usa um processo de eleição pseudo-aleatório para seleccionar um nó para ser o validador do próximo bloco, com base numa combinação de factores que podem incluir o tempo de participação na rede, a aleatoriedade e a riqueza do nó (quantidade de criptomoedas investidas).

  No método de selecção aleatório de blocos, os validadores são seleccionados procurando nós com uma combinação do menor valor de *hash* e maior tempo de participação e, como o tempo das participações é público, o próximo constructor, geralmente, pode ser previsto por outros nós.

  Quando um nó é escolhido para construir o próximo bloco, ele verifica se as transacções no bloco são válidas, assina o bloco e o adiciona à *blockchain*. Como recompensa, o nó recebe as taxas de transacção associadas às transacções no bloco.

Proof of Work* VS *Proof of Stake

Tabela 2: Mecanismos de consenso

	Proof of Work	*Proof of Stake*
Vantagem	-Fácil de implementar; -Método testado e consolidado, que mantém redes descentralizadas e seguras há muitos anos; -Não é necessário investir em criptomoedas para começar.	-Se torna mais fácil criar um bloco ou, sem muito investimento, se juntar ao grupo; -Maior escalabilidade; -Exige muito menos energia eléctrica para funcionar.
Desvantagem	-Alto consumo de energia eléctrica; -Necessidade de investimento em equipamentos de alta performance para minerar. -Conglomerados de mineração podem ser criados levando à centralização de esforços.	-É um método mais recente e, portanto, menos testado e consolidado.

2.3.5 Contractos inteligentes

*S*egundo Rocha & De Paula (2019), um contracto inteligente é análogo a um contracto em papel firmado por pessoas. No contracto em papel, são definidas as regras que estabelecem as responsabilidades e comunicação entre as partes que a assinaram. Na *blockchain*, a diferença é que o contracto é digital, porém são mantidos os mesmos preceitos do contracto em papel.

No contexto da computação, as regras que estabelecem as responsabilidades que devem ser tomadas pelas partes envolvidas são denominadas de regras de negócio ou funcionalidades do sistema. Uma regra de negócio, nesse contexto, contém uma sequência lógica de passos que são transformados e implementados em um código executável por meio de alguma linguagem de programação.

Segundo Alves, Nasser, & Laigner (2018), um contrato inteligente pode ser entendido como um agente autónomo armazenado na *blockchain*, enviado da mesma forma que uma transacção. Assim, ele deve ser aprovado pelos nós da rede de acordo com o seu mecanismo de consenso. Uma vez criado, o contrato inteligente é identificado por um endereço para que possa ser chamado por outros sistemas, utilizadores e até mesmo por outros contratos inteligentes. Os contratos inteligentes não podem ser modificados em execução, o máximo que pode acontecer é parar o contrato caso uma função *kill* tenha sido programada.

Exemplo de aplicação de um contrato inteligente:

1. Uma das partes cria o contrato inteligente para transferência de um bem mediante pagamento de um valor;
2. O contrato é enviado para a rede e em seguida é utilizado pelas partes para realizar o pagamento do valor acordado e transferir o bem para o solicitante.
3. Qualquer pessoa poderá reutilizar o contrato se as cláusulas atenderem às necessidades do utilizador.

2.3.6 Resumo do funcionamento da *blockchain*

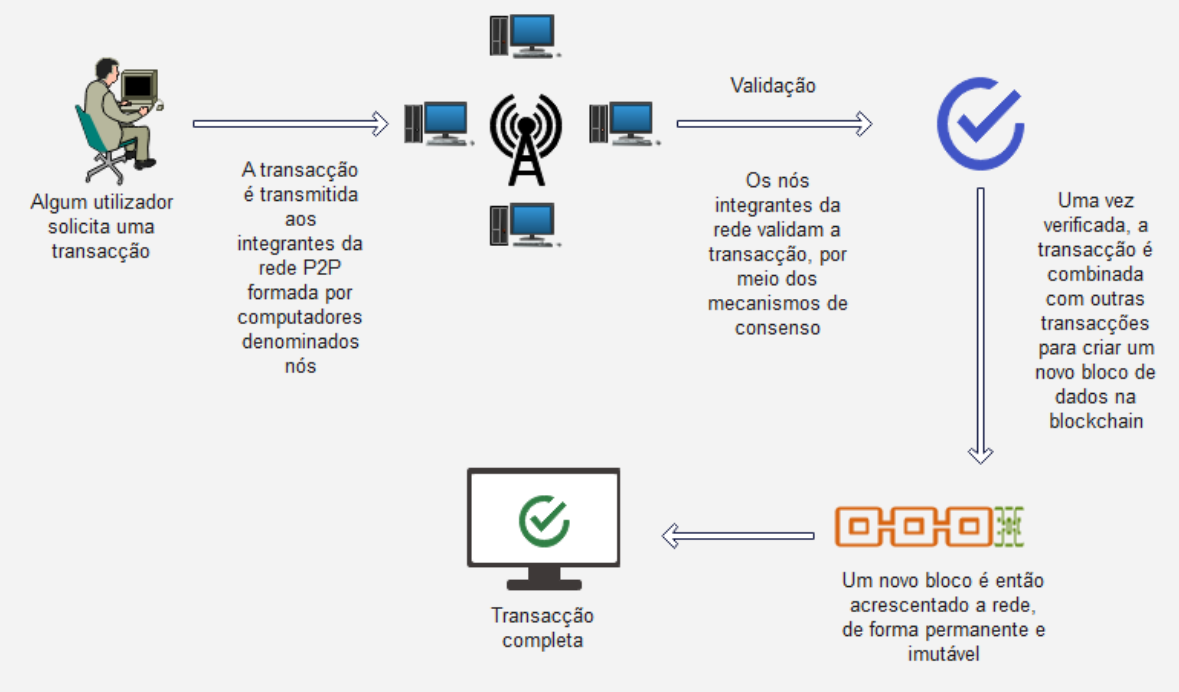


Figura D: Resumo do funcionamento da *blockchain*

2.3.7 Desafios da utilização da *blockchain* em relacção à partilha de processos clínicos e respectivas formas de mitigação

Segundo afirma da Silva (2020), apesar das oportunidades que a *blockchain* disponibiliza para a interoperabilidade, ainda existem algumas barreiras que podem comprometer a sua funcionalidade.

1. Segundo White (2018) citado por Silva (2020), a criptografia de chaves públicas e privadas pode ser eficaz para gerir as identidades digitais na partilha de dados. Permite uma fácil autenticação da identidade dos profissionais de saúde e dos doentes, uma vez que só necessitam de fornecer a sua chave privada. No entanto, as chaves privadas são mais difíceis de relembrar que as *passwords* convencionais, o que pode comprometer a sua usabilidade em casos de extravio. Já que, um recurso digital na *Blockchain* só pode ser manipulado usando a chave privada que o gerou, a perda dessa chave privada leva a perda permanente do recurso. Para a mitigação deste problema, é possível anexar as chaves privadas a cartões de identificação físicos facilitando este processo.

2. O segundo desafio relacciona-se com a escalabilidade do sistema. O tamanho, o volume de dados e o mecanismo de consenso na rede comprometem significativamente a escalabilidade. Por exemplo, uma ressonância magnética pode exigir 200 *megabytes* de espaço. Dada a natureza distribuída da *blockchain* não é exequível armazenar dados deste tipo *on-chain*. Este problema pode ser facilmente resolvido com o armazenamento destes dados *off-chain*. Por outro lado, o mecanismo de consenso na rede pode limitar bastante o volume de transações na rede. Para a resolução deste obstáculo é apontada a utilização de *blockchain*s permissionadas, ou mecanismos de consenso alternativos.

Contudo, a *blockchain* não é de todo imbatível ou totalmente isento de ataques. Aliás, todo sistema de informação está sujeito a ataques de segurança. Entre os ataques mais comuns estão a tentativa de quebra de senhas (quebra de segredos criptográficos) ou ataques de disponibilidade (DDOS, *Distributed Denial of Service*, em inglês). *Blockchain*, por sua natureza distribuída, pode estar exposta a ataques adicionais. Portanto, um dos ataques ao qual a *blockchain* estaria exposta é o ataque conhecido por 51%.

Principal vulnerabilidade de segurança da *Blockchain*

Ataque de 51%: chama-se ataque de 51% quando uma única entidade (ou um arranjo de membros actuando como uma única entidade) detém uma fatia expressiva, ou a maioria, do poder computacional. Em uma rede *Bitcoin*, por exemplo, se uma mesma entidade detivesse a maioria do poder computacional, essa entidade poderia influenciar ou manipular a formação da cadeia de blocos. Em outras palavras, poderia influenciar a formação da cadeia mais longa de blocos para permitir, maliciosamente, o cancelamento de transacções ou de decisões de consenso.

Base de dados *off-chain* – IPFS

Conforme mencionado anteriormente, a tecnologia *blockchain* é ideal para um sistema de armazenamento descentralizado, em que os registos podem ser facilmente compartilhados entre os pares da rede. No entanto, a *blockchain* tem limitações em termos de capacidade de armazenamento, quando o conteúdo dos processos clínicos tende a demandar grande espaço de armazenamento (já que pode ter imagens, além de outros registos). Como forma de superar esta limitação, há necessidade de se recorrer a uma base de dados externa, fora da cadeia, com uma estrutura ponto-a-ponto.

Segundo Kumar & Marchang (2020), IPFS (*InterPlanetary File System*, em português Sistema de Ficheiros Interplanetário) é uma estrutura ponto a ponto (P2P), de armazenamento distribuído, em que grandes volumes de informações podem, facilmente, ser armazenados. IPFS armazena ficheiros com seu *content-addressed hash* em uma tabela de *hash* distribuída (DHT) enquanto remove os ficheiros duplicados usando o histórico de controle de versão. IPFS também cria, localmente, um *hash* de ficheiros com alta frequência de solicitação, para garantir acesso rápido na vez seguinte. Além disso, o IPFS é um sistema de armazenamento em bloco, endereçado ao conteúdo, com recursos como alto rendimento, segurança com mapeamento *hash* de transacções e acesso concorrente a transacções pelos pares na rede.

Portanto, em vez de armazenar o processo clínico completo de um paciente na rede *blockchain*, apenas o *hash* endereçado ao conteúdo dos dados são armazenados. O IPFS tem um mecanismo de controle de versão, em que cada relatório é emparelhado com seu valor de *hash* na DHT. Para aceder ao processo clínico de um paciente, o par poderá usar o valor do *hash* correspondente ao processo clínico.

Portanto, no armazenamento *off-chain*, o processo clínico é armazenado no IPFS por um dos pontos da rede, e em resposta a isso, ele recebe o *contente-addressed hash* (*hash* do conteúdo endereçado) e este *hash* pode ser usado no futuro para extrair este processo clínico da rede IPFS.

2.3.8 Utilização da *Blockchain* para a partilha de processos clínicos

Pela sua robustez, *blockchain* é mundialmente reconhecida como a tecnologia mais indicada para contextos em que a segurança é vital. Além do sector financeiro, o sector da saúde tende a adoptar esta tecnologia pela sensibilidade dos seus objectos. O estudo *Healthcare Rallies for Blockchain*, realizado pela IBM, aponta que até 2020 cerca de 56% dos gestores de saúde adoptaram a tecnologia para optimizar a troca de informações dentro das organizações, demonstrando uma intenção real de investimentos em tecnologia de segurança neste sector.

Os processos clínicos de pacientes são objectos sensíveis pois tangem a saúde do paciente e, consequentemente, a sua vida. Estes precisam estar continuamente disponíveis e acessíveis, salvaguardando sempre a privacidade do paciente pois os processos clínicos são de caracter confidencial. *Blockchain* agrega naturalmente as características que respondem a necessidade.

Situações em que se pode utilizar *blockchain*

Claramente, não se deve recorrer a *blockchain* apenas como tendência tecnológica. Existem diversas opções de soluções para resolver um problema; é importante que se analise a viabilidade e necessidade. Galdino (2017), apresenta um conjunto de questões a serem colocadas para decidir a viabilidade de se recorrer a *blockchain* para responder a necessidade do problema.

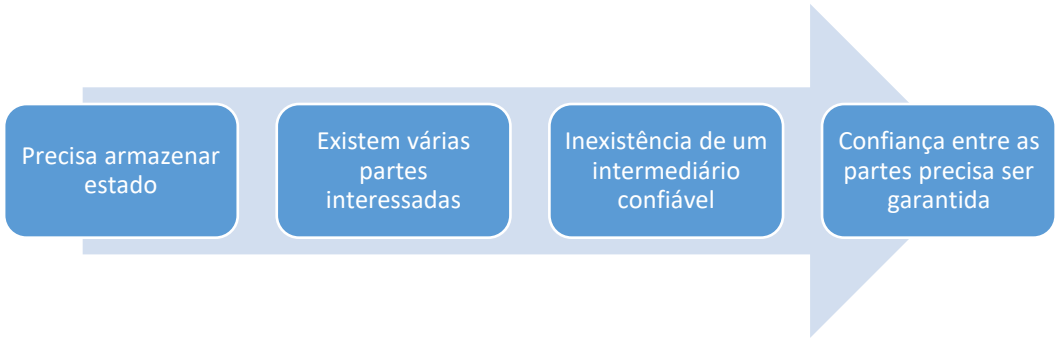


Figura E: Em que situação utilizar *blockchain*?

Portanto, o primeiro aspecto é: é preciso armazenar estado? Isto significa que os dados envolvidos no processo realmente precisam ser guardados numa base de dados. Se seus dados forem transitórios ou só tiverem utilidade por um determinado período de tempo, já se pode considerar que *Blockchain* não será necessário. Mas, se for preciso guardar a informação perpetuamente, segue-se para a próxima questão:

Existem várias partes interessadas? O que *Blockchain* oferece que é a imutabilidade dos dados fará sentido quando mais de uma parte interessada também precisar das mesmas informações. Se for apenas uma parte, a solução envolvendo uma base de dados relacional e outras ferramentas será mais apropriada. Se, contudo, houver mais de uma parte interessada e todas precisarem dos mesmos dados, *Blockchain* pode ser de facto uma opção e, avalia-se, então, a terceira questão:

Na verdade, a solução tem em vista a eliminação de qualquer dependência de intermediários nesta actividade. O facto de todos os blocos e transacções serem validados por todos os nós dificulta que registos incorretos sejam inseridos na *Blockchain*. Se a maioria dos nós do sistema estiverem trabalhando para o bem da rede, então apenas registos corretos serão inseridos. Assim, a confiança não está em um nó, mas na rede de nós como um todo; a confiança está no comportamento colectivo, reforçando ainda mais a confiança. Esta última questão acaba respondendo à questão

que viria a seguir: necessidade de garantia de confiança entre as partes. Se a resposta for sim, sem dúvidas *blockchain* é a mais adequada.

As outras alternativas, reúnem algumas das principais propriedades da *blockchain*, mas não possuem o mecanismo de consenso que elimina completamento a necessidade de um intermediário. Daí que, conclui-se que a *blockchain* tem mais vantagem em relacção as outras opções.

Porque a *blockchain* ficou conhecida pelas *bitcoins*, baseadas na tecnologia *ethereum*, esta também ficou conhecida pelos desafios de consumo de energia e de processamento de pequenas quantidades de transacções por segundo, em relacção as outras tecnologias. No entanto, para amenizar estes desafios sobre cenários diferentes de criptomoedas, foi criado em 2015, o projeto *Hyperledger*, e seu *software Hyperledger Fabric*, de código aberto. Segundo Conceição, Rocha, et.al (2019), por ser permissionada, *Hyperledger Fabric* não exige consumo de energia excessivo, como o *Ethereum* do *Bitcoin* e a capacidade de processamento de transacções também elevada.

3. Capítulo III – Caso de estudo: Sistema Nacional de Saúde

3.1 Modelo actual da transferência de processos clínicos no SNS.

3.1.1 Descrição

No SNS, os processos clínicos dos pacientes não são partilhados entre as unidades sanitárias. Existem dois mecanismos actualmente utilizados para partilha de informação clínica de pacientes: através de guias de transferência e relatório médico.

Guia de transferência é um documento preenchido na unidade sanitária de onde o paciente vai ser transferido. Neste documento não constam todos os detalhes presentes no processo clínico, apenas as informações clínicas relaccionadas à finalidade da transferência. Já o relatório médico é apenas um resumo feito pelo médico em caso de solicitação do paciente para fins diversos.

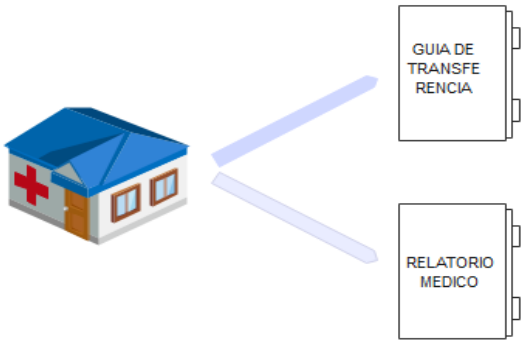


Figura F: Mecanismos utilizados para partilha de informação clínica de pacientes

3.1.2 Constrangimentos

Do modelo actual de transferência de processos clínicos no SNS, foram notados alguns constrangimentos descritos a seguir:

- Monopólio da informação clínica dos pacientes: o processo clínico permanece na unidade sanitária em que tiver sido aberto. As outras entidades prestadoras de serviços de saúde não têm acesso completo aos processos clínicos produzidos na unidade protagonista, tampouco os pacientes titulares dos mesmos processos. O que, por sua vez, constrange a eficiência na assistência e controlo da saúde do paciente.
- Informação clínica do paciente espalhada por diversas instituições de saúde: no modelo actual, não existe possibilidade de se adicionar cada exame, diagnóstico ou observação sobre a saúde do paciente em um mesmo documento, construindo um histórico completo e consistente ao longo da vida do paciente. A cada unidade sanitária que o paciente visita os registos são feitos de forma independente, dispersando a informação e de forma desconexa, fazendo escapar, possivelmente, algumas notas importantes a serem tomadas em conta sobre o histórico clínico do paciente durante uma eventual sessão com o médico.
- O paciente não tem posse do processo clínico, mesmo sendo titular do mesmo. O processo clínico pertence ao hospital e é controlado pelo hospital. Portanto, não existe garantia de que a privacidade do paciente está sendo assegurada.

- Maior exposição a perdas de processos clínicos: o modelo actual do SNS não garante segurança. Por causa da centralização da informação, qualquer incidente ou ataque pode ser catastrófico e sem reversão.
- Os sistemas podem sofrer ataques informáticos: Ex. DoS, provocando indisponibilidade do sistema ou da informação.

Estes factores podem influenciar negativamente a qualidade da assistência aos pacientes e, consequentemente, a própria saúde do paciente, trazendo deficiências ao cumprimento de um dos objectivos pelo qual o SNS foi instituído, o de promover a saúde, prevenção de doenças, assistência e reabilitação de todo o cidadão nacional.

3.2 Utilização da tecnologia *blockchain* para a partilha de processos clínicos no SNS.

A utilização da tecnologia *blockchain* para a partilha de processos clínicos no SNS representa um grande avanço na área da saúde e tecnologia em Moçambique, e contribui significativamente na qualidade da assistência médica aos doentes e reflete, consequentemente, de forma positiva na manutenção da saúde dos doentes.

Com a utilização da *blockchain*, os pacientes passariam a possuir e controlar o acesso às suas informações clínicas. Assim, além de garantir a sua privacidade sobre informações que julgarem confidenciais, podem ainda de forma autónoma instituir regras de acesso ao seu processo, como por exemplo autorizar a utilização do seu histórico para fins de investigação, através dos *smart contracts*.

Os participantes podem partilhar os dados com segurança entre os seus pares, sem necessitarem da criação de redes complexas de relacções de confiança intermediadas.

Porque os dados estão encriptados e só podem ser decifrados com a chave privada do paciente, mesmo que a rede seja infiltrada por um agente malicioso, não existe uma forma prática de aceder aos dados.

Entretanto, a literacia digital ainda constitui um desafio no contexto moçambicano. Uma vez que um dos utilizadores do sistema é o paciente, há que considerar que parte deste grupo é formado por idosos, outra por menores de idade e outra por jovens e adultos, porém não familiarizados com o uso da tecnologia, o que pode constituir um desafio para a implementação da solução, pois nem todos os pacientes estariam em condições de, de forma autónoma, fazer uso das possibilidades que o sistema proposto os oferece.

Neste sentido, uma das formas de mitigação passa por, de igual modo ao que acontece no sistema actual (ou tradicional), onde alguns pacientes têm acompanhantes de confiança que se responsabilizam por eles, permitir que estes acompanhantes operem no lugar dos pacientes incapacitados, assim a eficácia da solução permanece conservada mesmo diante do desafio levantado.

3.3 Proposta de solução

Descrição

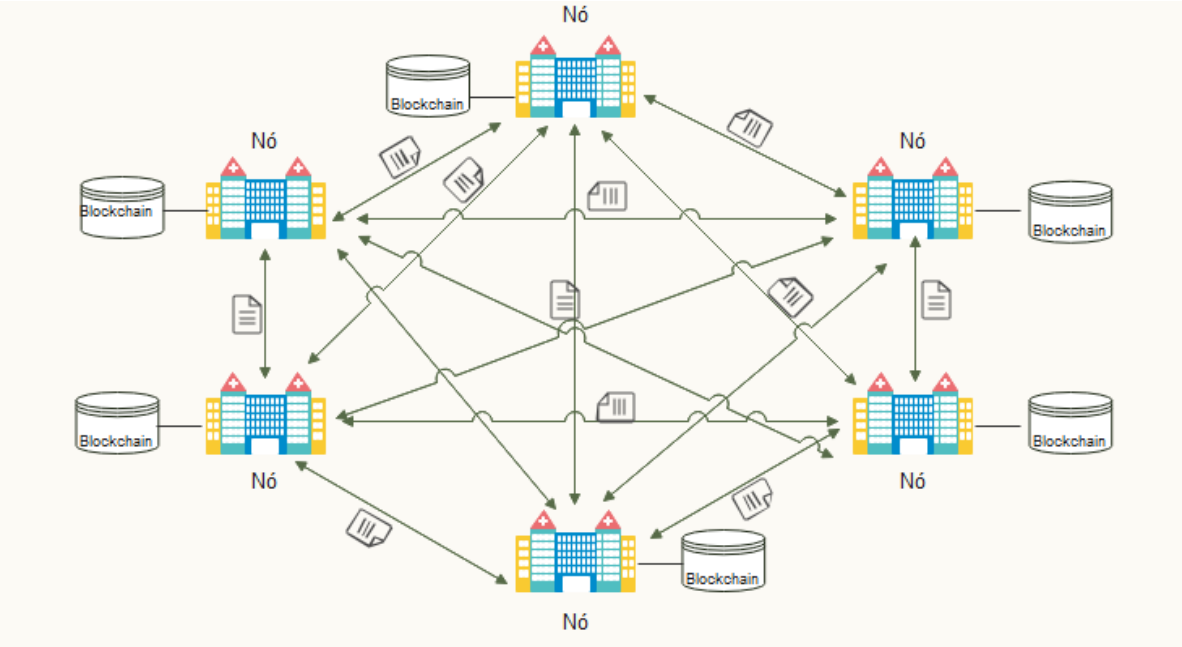


Figura G: Partilha de processos clínicos entre as unidades sanitárias do SNS baseada em *blockchain*.

Diante dos constrangimentos identificados no modelo em actual funcionamento no SNS, uma plataforma de partilha de processos clínicos baseada em *blockchain* é apontada como solução para a erradicação de tais constrangimentos. Esta plataforma é, na verdade, um sistema descentralizado que permite que todas as unidades sanitárias que compõem o SNS partilhem informações clínicas de pacientes para fins relaccionados à prestação de serviços de saúde.

Essencialmente, o sistema permitirá que cada processo clínico aberto, cada informação acrescentada ao processo clínico esteja disponível em todos os pontos (ou nós) integrantes da rede, que são as unidades sanitárias, já que cada um desses pontos passa a conter, por padrão, uma réplica dos ficheiros (descentralização e

disponibilidade). Uma vez disponível a informação, o seu acesso é controlado pelo próprio paciente titular do processo clínico (privacidade).

No processo de garantir acessos ao processo clínico, o paciente decide que permissões dar e a quem dar (dentre os diversos profissionais de saúde autorizados, do SNS), estas permissões podem ser para ler apenas ou ler e escrever (adicionar informação). Para tal, no sistema, o profissional de saúde faz a requisição do acesso ao processo clínico, com especificação de qual permissão deseja ter e então é enviada uma mensagem para o titular com o código de acesso que será informado ao requisitante, caso o acesso seja consentido e, a partir daí, o profissional de saúde passa a ter acesso ao processo clínico do paciente em questão. Quando, por parte do paciente, houver necessidade de retirar o acesso do profissional de saúde ao seu processo clínico, bastar-lhe-á abrir a lista de profissionais de saúde com acesso e remover o que desejar da lista. Note-se que, uma vez na rede, os processos clínicos jamais poderão ser apagados.

Quando uma nova informação for adicionada a rede, as Unidades Sanitárias responsáveis deverão proceder com a validação e só depois a informação poderá ser persistida na rede. O sistema de *Hash,* explicado no ponto 2.3.2 do cap. II, impossibilita modificações fraudulentas (imutabilidade, integridade e auditabilidade).

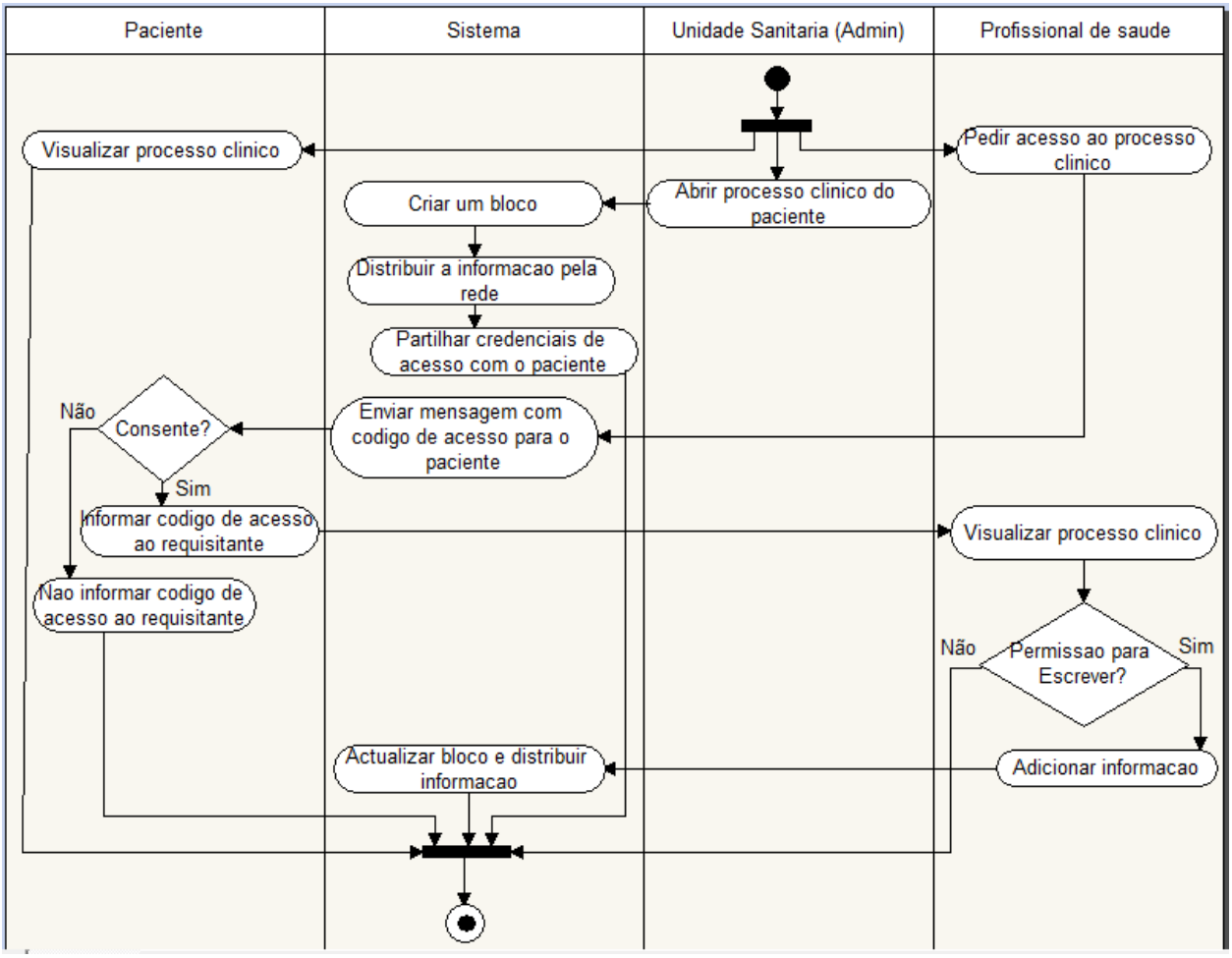


Figura H: Proposta de solução

Nesta solução, será utilizada a tecnologia *blockchain* do tipo permissionada, já que cada participante terá a sua identidade verificada e privada por ser de responsabilidade de uma instituição que a vai manter operacional, no caso, o SNS. Será baseada na plataforma *Hyperledger Fabric* pelas seguintes vantagens:

- É uma rede autorizada que estabelece confiança descentralizada em uma rede de participantes conhecidos (portanto, mais adequada ao contexto em estudo);
- Gasta menos energia em relacção ao *ethereum* (tecnologia base das criptomoedas);
- É relativamente mais fácil de implementar.

Cenário de uso da solução

Suponha-se o seguinte cenário:

Anabela, uma cidadã moçambicana, residente em Maputo, tem um quadro anémico e precisa ser internada no HCM. Dá entrada ao Hospital, lhe é aberto um processo clínico, onde se registam algumas informações da paciente referente ao seu quadro clínico. Após guardar a informação, o processo clínico da Anabela é replicado entre os nós da rede, que são as US do SNS, em um bloco que, a seguir, é aprovado por alguns administradores das outras US para que, então, seja persistido na rede. Nesse momento, o bloco que contém a informação clínica da Anabela é atribuído um *hash*[7] que vai garantir a integridade e imutabilidade da informação, já que este *hash* estará ligado ao bloco anterior (conforme explicado no ponto 2.3.3 do cap. II) e qualquer modificação implicará discrepância entre os *hash's* que conectam estes dois últimos blocos.

Depois de três dias, a Anabela apresenta melhorias e recebe alta. Um tempo depois, ela muda-se para a cidade da Beira, à trabalho. Ela volta a ter uma crise, dirige-se ao HCB e, além de precisar ser assistida por um médico, ela precisa fazer exames médicos. No HCB, através do sistema proposto, o profissional de saúde que a recebe consegue ter acesso ao seu processo clínico, observando e seu histórico e adicionando o resultado dos exames que a Anabela precisou fazer, dando continuidade ao histórico do seu quadro clínico da seguinte maneira: Anabela é recebida pelo médico, o médico pergunta o NID da Anabela e informa ao sistema. Depois de localizar o processo da Anabela, através do sistema, este pede permissão para ver e escrever. Nesse momento, um código é enviado por mensagem de texto para o celular da Anabela, que por sua vez, informa o código ao médico. Dessa forma, o médico consegue ver e adicionar informação ao processo clínico da Anabela, que significará a criação de um novo bloco que seguirá o fluxo descrito no início da descrição do cenário.

Constrangimentos resolvidos com a solução proposta

A solução proposta resolve os constrangimentos identificados na medida em que:

1. Os processos clínicos dos pacientes deixam de ser centralizados, já que cada ponto da rede, ou seja, cada unidade sanitária integrante do SNS detém consigo uma réplica do processo clínico. Portanto, com a indisponibilidade de um servidor

[7] Explicado no ponto 2.3.2 do Cap. II.

para aceder a informação, continuam a existir vários outros disponíveis, sendo, portanto, mais tolerante à falhas.

2. Os pacientes ganham autonomia sobre os seus processos clínicos. Além de poder ter acesso, controlar a concepção ou remoção de acessos ao seu processo clínico permite ao paciente garantir a privacidade da sua informação clínica, pois ele tem o poder de autorizar ou negar os acessos ao seu histórico clínico.
3. Garante que as unidades sanitárias do SNS partilhem os processos clínicos dos pacientes, com garantia de segurança, já que a tecnologia da solução proposta é baseada em criptografia, reduzindo consideravelmente o risco de ataques cibernéticos.
4. Permite construir um histórico contínuo e completo, incorruptível, imutável e que jamais será descartado. Além de beneficiar a própria saúde do paciente, o histórico clínico com estas características viabiliza, igualmente, os estudos científicos que poderão evoluir na precisão de diagnósticos.
5. Elimina a dependência de um terceiro para conceder acesso ao processo clínico, isto é, não é mais necessária a disponibilidade de um administrativo para conceder acesso ao paciente ou profissional de saúde; o paciente e o médico são suficientes para este processo.

4. Capítulo IV – Desenvolvimento da solução proposta

Para o desenvolvimento da solução proposta, foi empregada a metodologia de desenvolvimento de *software* em cascata, conforme apresentado no capítulo I. Desta forma, são detalhadas, a seguir, as actividades que compõem cada uma das fases do modelo em cascata.

4.1 Elicitação de requisitos

A fase da elicitação de requisitos constitui uma das fases cruciais para a concepção do *software* que se pretende e tomou lugar logo no início do trabalho. Foi constituída pelas entrevistas, levantamento documental, questionários e observações com vista a fazer o levantamento e refinamento dos requisitos da solução proposta. Assim sendo, o resultado desta etapa passa por uma lista de requisitos refinada. Pelo que, essencialmente, o sistema deve permitir criar, visualizar e adicionar informações aos processos clínicos; aos pacientes, garantir e remover permissões de acesso aos seus processos clínicos por profissionais de saúde específicos; entre outros básicos como cadastrar e excluir utilizadores do sistema; iniciar e terminar sessões.

4.2 Análise da solução

Para a efectivação do sistema proposto é importante a identificação do grupo de interesse. O grupo de interesse é representado por entidades que partilham pelo menos um interesse em comum que os une, fazendo com que actuem em direcção ao alcance de seu objectivo. Assim sendo, a seguir é apresentado o grupo de interesse para o sistema proposto.

- **Grupos de interesse**

  Para o presente trabalho, os principais grupos de interesse são: o SNS, os profissionais de saúde e os pacientes.

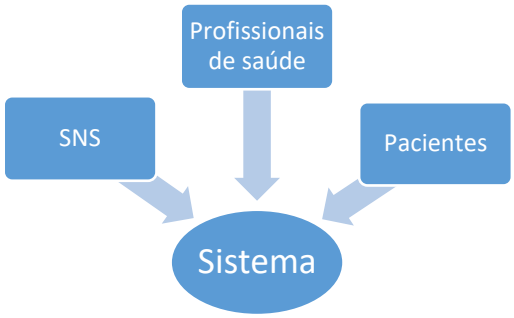


Figura I: Grupos de interesse

SNS: Um dos maiores esforços do SNS tem sido proporcionar serviços de saúde com qualidade ao nível nacional. Este esforço começa com a garantia de que todos os cidadãos tenham acesso aos cuidados de saúde. A utilização deste sistema é do interesse do SNS a medida em que contribui para a melhoria da prestação dos serviços de saúde, pois com ele os pacientes podem se beneficiar da diversificação dos provedores de serviços de saúde sem limitações no acesso ao seu processo clínico permitindo com que profissionais de saúde assistam com perícia.

Profissionais de saúde: este sistema é do interesse dos profissionais de saúde pois auxilia o seu trabalho na assistência aos pacientes. Quando diante de um paciente o sistema permite que eles tenham o acesso ao processo clínico do paciente, conhecendo o seu histórico de modo a fazer análises e poder tomar decisões conscientemente mais acertadas. Portanto, as funcionalidades do sistema dedicadas aos profissionais de saúde são:

a) Visualizar processo clínico de pacientes que o tenham dado permissão para tal;
b) Fazer registos relevantes, actualizando o histórico clínico do paciente.

Pacientes: os pacientes constituem o grupo com maior interesse neste sistema, que usam o sistema para conseguir melhores condições para cuidar da sua saúde. O sistema permite a este grupo:

a) Visualizar o seu processo clínico sem, no entanto, poder fazer qualquer edição sobre ele;
b) Dar acesso ao seu processo clínico, decidindo quem pode e quem não pode visualizar o seu processo clínico, garantindo, desta forma, a sua privacidade;
c) Remover acesso ao seu processo clínico, impedindo ao profissional que alguma vez teve acesso ao seu histórico de continuar a visualizar por qualquer motivo que justifique tal remoção.

4.2.1 Requisitos do sistema: Prioridades, Requisitos Funcionais e Requisitos Não Funcionais

- **Prioridades**

A priorização de requisitos é uma actividade crítica do desenvolvimento de um software. Esta actividade envolve a análise do nível de relevância de cada requisito, de modo a definir a ordem de implementação de tais requisitos.

Quanto à prioridade, os requisitos de um *software* são classificados em:

- **Essencial:** aquele que é fundamental e imprescindível para o funcionamento do sistema, sem o qual o sistema deixa de se aplicar ao propósito da sua concepção.
- **Importante:** aquele em que é imperioso que faça parte do escopo, porém não impede o sistema de entrar em produção.
- **Desejável:** aquele que não compromete a usabilidade do sistema. O sistema pode responder ao propósito pelo qual foi concebido com ou sem a sua implementação.

- **Requisitos**

Segundo Young (2004), requisitos de um sistema são atributos necessários para que o mesmo tenha valor e utilidade. Este afirma, ainda, que os requisitos de um sistema são importantes pois fornecem a base para todo o processo de desenvolvimento do *software*. Os requisitos do sistema podem ser vistos, ainda, como declarações articuladas de forma clara sobre o que um sistema deve ser capaz de fazer para satisfazer as necessidades e requisitos dos intervenientes e que derivam de requisitos negociais e de requisitos do utilizador. Os requisitos de um *software* podem ser divididos entre funcionais e não-funcionais.

  - **Requisitos funcionais**

    De acordo com Filho (2003) citado por Generoso (2019), requisitos funcionais representam os comportamentos que um sistema deve apresentar diante de certas acções de seus utilizadores. Ou seja, requisitos funcionais referem-se às funcionalidades desejadas para determinado *software*.

Tabela 3: Descrição dos requisitos funcionais

ID	Requisito	Descrição	Prioridade	Referência
RF01	Cadastrar utilizador	Possibilita o registo de novos utilizadores do sistema (pacientes ou profissionais de saúde). Importa referir que este cadastro só poderá ser realizado por um utilizador com privilégios de administrador.	Essencial	
RF02	Excluir utilizador	Permite remover determinado utilizador do grupo de utilizadores do sistema. Para o caso dos profissionais de saúde que deixem, por alguma razão, de fazer parte do quadro de profissionais de saúde do SNS.	Importante	RF01, RF03
RF03	Iniciar sessão	Funcionalidade que permite autenticar os utilizadores	Essencial	RF01

		cadastrados para que acedam as demais funcionalidades do sistema.		
RF04	Terminar sessão	Permite ao usuário cadastrado e com sessão iniciada, terminar a sessão no sistema.	Essencial	RF03
RF05	Garantir acessos	Permite ao paciente dar acesso ao seu processo clínico, de modo a que só o profissional de saúde com autorização do paciente consiga visualizar o seu processo clínico, reservando a sua privacidade.	Essencial	RF03
RF06	Remover acessos	Permite ao paciente remover o acesso ao seu processo clínico, do profissional de saúde que, por alguma razão, sentir não mais conveniente que tenha acesso.	Essencial	RF03
RF07	Visualizar processo clínico	Permite visualizar as informações que compõem o processo clínico do paciente, seja por parte dos profissionais saúde para fins de análise para tomada de decisões e outros fins, ou do lado paciente titular do processo clínico.	Essencial	RF03
RF08	Criar/abrir processo clínico	Funcionalidade que permite criar um processo clinico, onde serão reunidas as informações clínicas dos pacientes.	Essencial	RF03
RF09	Adicionar informação ao processo clínico	Permite adicionar informação ao processo clínico sempre que for necessário, mantendo o processo sempre actualizado.	Essencial	RF03, RF08

RF10	Pesquisar processo clínico	Esta funcionalidade destina-se a auxiliar no processo de busca de processos clínicos da forma mais rápida e dinâmica possível.	Essencial	RF03
RF11	Recuperar Senha	Permite que um utilizador cadastrado recupere a sua senha de acesso caso se tenha esquecido.	Essencial	RF01
RF12	Cadastrar Unidade Sanitária	Permite com que uma unidade sanitária seja adicionada como um ponto da rede.	Essencial	RF3

- **Requisitos Não-Funcionais**

Requisitos não funcionais são aqueles que não estão diretamente relaccionados à funcionalidade de um sistema. Os requisitos não funcionais abordam aspectos de qualidade importantes em sistemas de software.

Tabela 4: Descrição dos requisitos não funcionais

ID	**Requisito**	**Descrição**	**Prioridade**	**Referência**
RNF01	Segurança	Permite que as informações sejam guardadas e partilhadas de forma segura, com garantia de integridade, privacidade e autenticidade.	Essencial	
RNF02	Disponibilidade	Permite que o sistema esteja disponível todos os dias, 24h/24h, para atender as necessidades dos seus utilizadores.	Essencial	
RNF03	Confiabilidade	O sistema em si oferece confiança, sem a	Essencial	

		necessidade de entidades intermediárias para a garantir confiança, o sistema em si já oferece esta garantia, através do seu mecanismo de consenso.		
RNF04	Boa experiência de utilizador	Permite que a interface do sistema seja simples e de fácil uso para o utilizador.	Essencial	
RNF05	Escalabilidade	Poder para responder a quantidade de processos clínicos que vão sendo criados e acedidos no sistema, sem que haja uma alteração abrupta no funcionamento ou desempenho do sistema.	Essencial	

4.2.2 Modelagem da Proposta de Solução

Os processos de modelagem são parte das principais actividades que conduzem à implementação de um *software* consistente. Para a modelagem da solução proposta foram adoptadas as anotações UML. UML (*Unified Modeling Language*) é uma linguagem padrão para visualização, especificação, construção e documentação de um projeto de *software*, conforme a definição de Gustavo (2009). UML permite obter uma visão lógica de todo o processo, optimizando as etapas que envolvem o desenvolvimento de um sistema antes da sua concepção.

Gustavo (2009), afirma ainda que a UML implementa uma modelagem com uma visão orientada à objectos, porém isso não implica que a ferramenta e a linguagem utilizada para a implementação do modelo sejam também orientadas à objectos.

Modelos de casos de uso

Segundo Stadzisz (2002), o modelo de casos de uso é um instrumento eficiente para a determinação e documentação das funcionalidades a serem desempenhadas pelo sistema. Tal como afirma Sommerville (2011), os modelos de casos de uso permitem modelar interacções entre um sistema e actores externos (utilizadores ou outros sistemas).

Os casos de uso de um projeto de software são descritos na linguagem UML através de diagramas de casos de uso. Estes diagramas utilizam como primitivas, essencialmente, actores, casos de uso, relacionamentos e fronteira do sistema.

- **Actores**: constituem os elementos que interagem com o sistema, os papéis desempenhados por elementos externos ao sistema. Ex: humanos (utilizadores).
- **Casos de Uso**: representam uma funcionalidade do sistema (um requisito funcional) e é geralmente iniciado por um actor ou até mesmo por outro caso de uso.
- **Relaccionamentos**
    - **Relaccionamento de associação**: indica que há uma interação (comunicação) entre um caso de uso e um actor. Um actor pode se comunicar com vários casos de uso.
    - **Relaccionamento de generalização**: Quando dois ou mais atores podem se comunicar com o mesmo conjunto de casos de uso, um filho (herdeiro) pode se comunicar com todos os casos de uso que seu pai se comunica - **Generalização de actores**.

      Quando o caso de uso filho herda o comportamento e o significado do caso de uso pai; o caso de uso filho pode incluir ou sobrescrever o comportamento do caso de uso pai; o caso de uso filho pode substituir o caso de uso pai em qualquer lugar que ele apareça - **Generalização de casos de uso**.
    - **Relaccionamento de dependência**: representa uma variação/extensão do comportamento do caso de uso base; o caso de uso estendido só é executado sob certas circunstâncias – **Extensão**.

A **Inclusão** – por sua vez, evita repetição ao fatorar uma atividade comum a dois ou mais casos de uso; um caso de uso pode incluir vários casos de uso.

- **Fronteira do Sistema**: elemento opcional que serve para definir a área de atuação do sistema. Representado por um retângulo, que alberga todos os outros elementos.

Abaixo são apresentadas as anotações de alguns dos elementos acima descritos, os quais são utilizados na construção do diagrama de casos de uso da solução proposta.

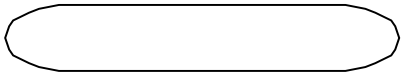
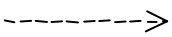
Anotação	Descrição
	Representa o caso de uso.
	Representa o actor.
	Relaccionamento de dependência (acompanhado da expressão <<*extend*>>
	Estabelece a relacção entre o actor e o caso de uso.

Tabela 5: Elementos do diagrama de casos de uso

A seguir é apresentado o diagrama de casos de uso do sistema proposto.

Nota: A descrição dos casos de uso é apresentada no anexo 4 do presente trabalho.

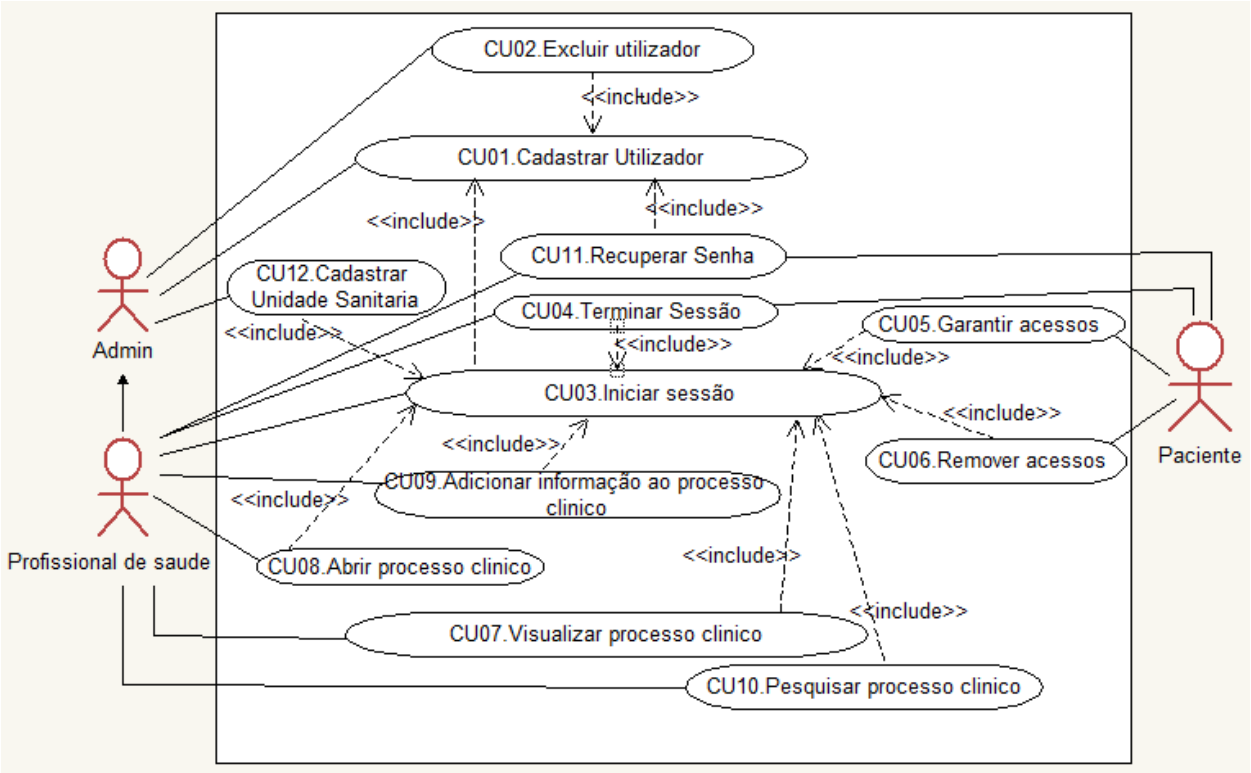


Figura J: Diagrama de casos de uso

4.3 Projecto

Arquitectura

As arquitecturas de referência surgem como um tipo especial de arquitectura de *software* que alcança uma compreensão bem reconhecida de domínios específicos, promovendo a reutilização da experiência em projecto, facilitando o desenvolvimento, padronização e evolução dos sistemas de *software*. (NAKAGAWA et al., 2012) citado por (ABREU, 2020).

O desenho da arquitectura do sistema proposto basea-se nas arquitecturas propostas por Lu et al. (2018), Wan et al. (2019), Xu et al. (2018), Xu et al. (2019). Seus elementos estão descritos a seguir:

Aplicação: esta camada inclui as aplicações que fazem uso dos recursos da *blockchain*. Esta camada alberga a interface gráfica do utilizador que os permite interagir com o sistema, acedendo as funcionalidades do mesmo.

API: a utilização da API está relaccionada ao conjunto de normas que possibilita a comunicação entre sistemas através de uma série de padrões e protocolos. Para o

protótipo da solução proposta, a API será utilizada para possibilitar a interacção com a componente *blockchain* e a base de dados auxiliar.

***Blockchain*:** A camada de *blockchain* é responsável por armazenar e compartilhar dados, além de executar os contractos inteligentes. Está subdividida nos seguintes componentes:

i. Contractos inteligentes: Um contracto inteligente é um programa criado pelo utilizador, implantado e executado na *blockchain* e pode representar as regras de negócios. Eles também podem ser implementados como parte de uma transacção. Das regras predefinidas na concepção da solução proposta estão:

- Para ter acesso aos processos clínicos dos pacientes, o profissional de saúde precisa estar associado a uma unidade sanitária cadastrada no sistema como um ponto da rede;
- Se um profissional de saúde teve o seu acesso removido, pode pedir outra vez;
- O paciente não tem permissão para editar o seu processo clínico.

Claro que estas serão traduzidas para uma linguagem de programação para que possa ser executável e perceptível à nível computacional.

ii. Transacções: esta componente possui implementações para a geração e validação dos blocos e seu pedido. Algumas das transacções aplicadas a solução proposta são:

- Pedir acesso ao processo clínico de um paciente;
- Remover o acesso de um profissional de saúde;
- Abrir um processo clínico novo;
- Adicionar informação a um processo clínico.

Portanto, o bloco será composto por estas transacções e cabeçalhos contendo metadados, conforme detalhado no cap. II, no ponto 2.3.2.

iii. Chaves: esta constitui uma componente essencial na *blockchain*. Cada participante da rede possui uma ou mais chaves privadas, por si utilizadas para assinar digitalmente as transacções relativas aos seus endereços.

iv. Livro-razão (*ledger*) – representa o livro de registos distribuído na *blockchain*.

Bases de dados convencionais: devido às limitações de armazenamento da *blockchain*, no que diz respeito a escalabilidade, existem bases de dados auxiliares, fora da cadeia, usadas no sistema. Para o caso em estudo, apenas as referências dos processos clínicos serão armazenadas na *blockchain*, os processos clínicos em si precisarão ser armazenados em uma base de dados *off-chain*, ou seja, fora da cadeia, em um serviço em nuvem, o IPFS.

Algoritmos de consenso: esta camada permite implementações para gerar a ordem dos blocos e validações pelos nós da rede, com algoritmos definidos. Para a solução proposta, o algorítimo empregado será o *Proof of Stake*. Apesar de ser novo e, consequentemente, menos consolidado, será mais adequado ao contexto do SNS à medida em que consome menos energia eléctrica, se comparado ao *Proof of Work,* é menos exigente quanto a capacidade dos equipamentos e permite maior escalabilidade.

Rede - a camada de rede ponto a ponto é responsável pela comunicação entre os nós. A camada de consenso fornece implementações para gerar a ordem de criação de blocos e validar blocos criados pelos nós da rede.

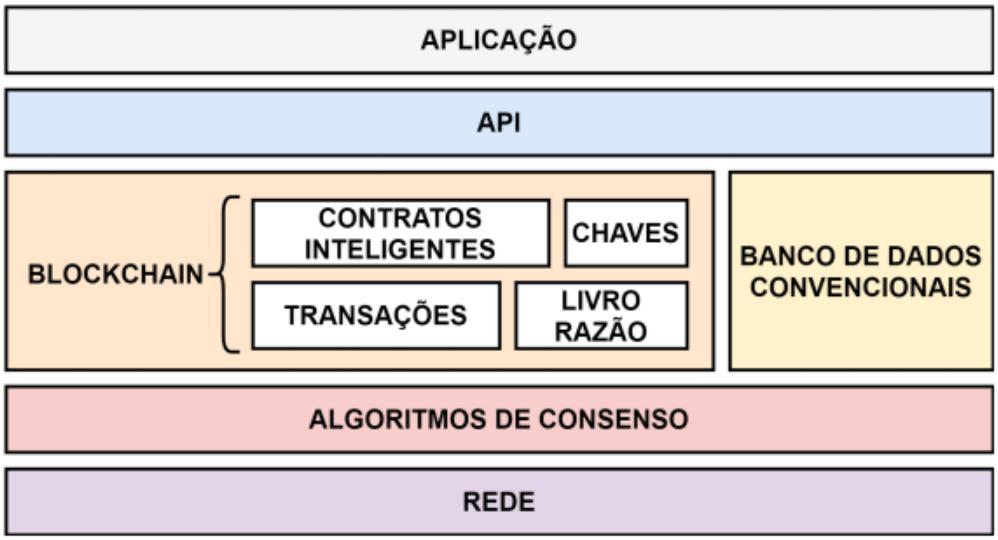


Figura K: Arquitectura da solução proposta.

Fonte: (ABREU, 2020)

4.4 Codificação do protótipo

A codificação foi feita mediante tecnologias de desenvolvimento *web: JavaScript, Node.js e React.js*, permitindo que qualquer membro da rede aceda à plataforma através da internet, executando a aplicação a partir de um navegador.

A informação detalhada das tecnologias utilizadas na codificação do protótipo está descrita no ponto 1.5.3 do capítulo I na tabela 1.

4.5 Testes do protótipo

Para efectuar o teste do protótipo desenvolvido fez-se a utilização do navegador Google Chrome em um computador portátil da marca Dell, modelo Inspiron 15300, com processador i5-7200U CPU @ 2.50 GHz 2.70 GHz, memória de 8Gb, através do sistema operativo Windows 10 Home.

A seguir serão apresentados os testes de uma das principais funcionalidades do protótipo, onde o profissional de saúde de uma das unidades sanitárias que fazem parte da rede, no caso, do Hospital Central de Maputo, acede ao sistema, pesquisa por um paciente através do NID e assim que o paciente é apresentado na tela, o profissional de saúde pressiona no botão “Pedir para ver” e, então, um código é enviado por SMS para o paciente em questão. Este último, por sua vez, partilha o código com o profissional de saúde que, a seguir, informa ao sistema e pressiona o botão “submeter” e, por fim, é apresentado o processo clínico do paciente na tela do profissional de saúde.

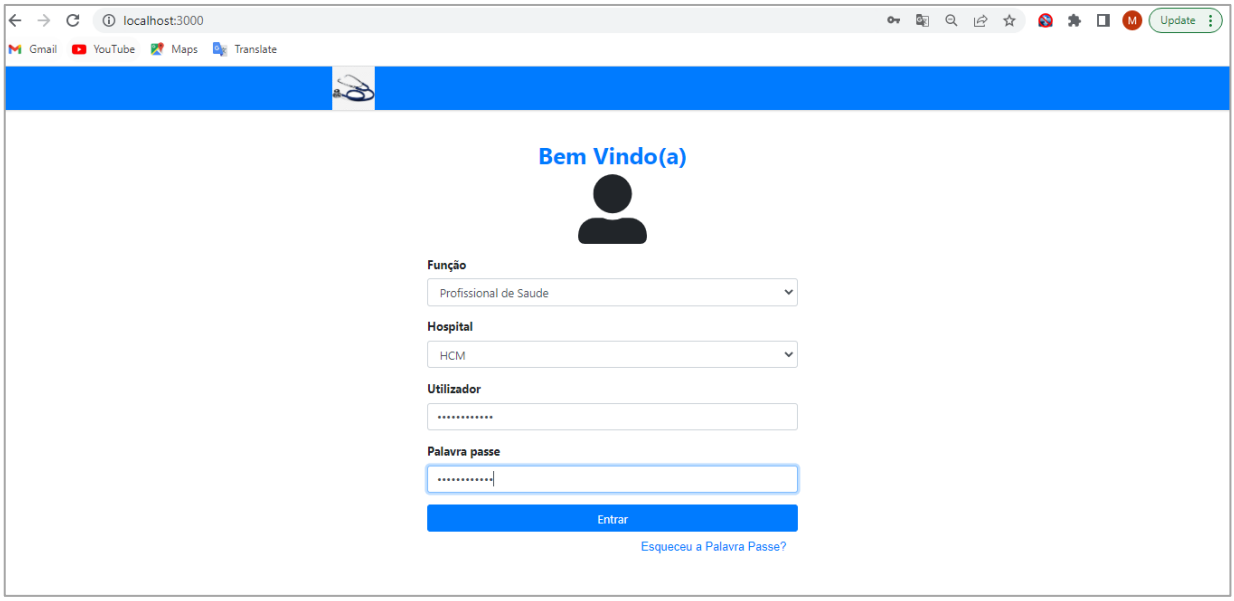


Figura L: Teste da tela de *Login*

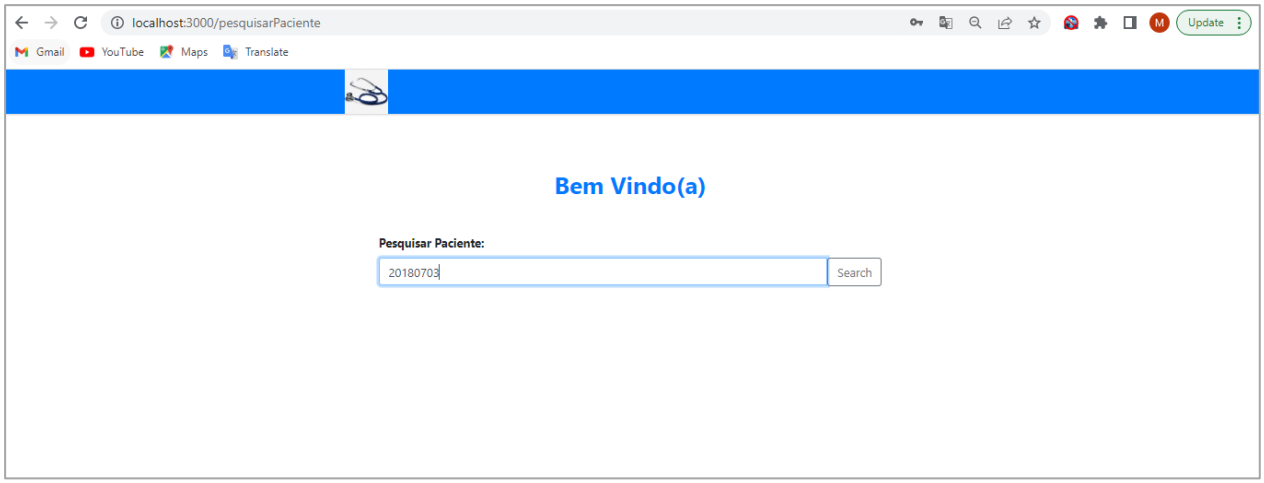


Figura M: Teste da tela de pesquisa de paciente

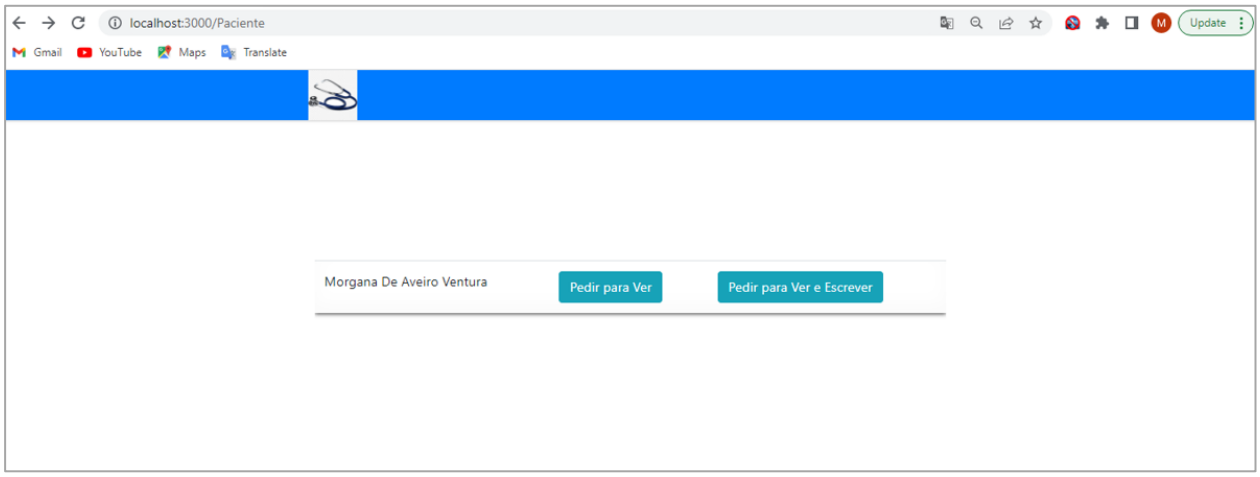


Figura N: Teste da apresentação de paciente pesquisado

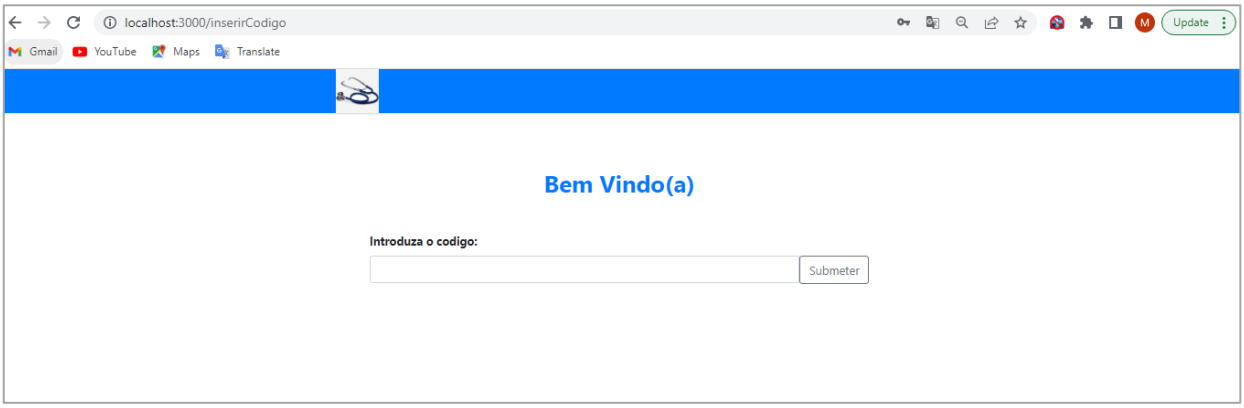


Figura O: Teste da tela de inserção do código enviado para o paciente

Figura P: Teste da tela de apresentação do processo clínico do paciente pesquisado

5. Capítulo V – Discussão de resultados

Com vista o alcance do objectivo geral do presente trabalho '*Desenvolver uma plataforma de partilha de processos clínicos, para o SNS, baseada em blockchain, que garanta a descentralização, disponibilidade, integridade, privacidade e autenticidade da informação,* como proposta de solução para o problema identificado, recorreu-se a revisão de literatura, pesquisa documental e entrevistas ao Arquivo Clínico do Hospital Central de Maputo como forma a colher informações sobre a situação actual da partilha de processos clínicos de pacientes entre as Unidades Sanitárias do SNS. Como resultado das etapas mencionadas, foi concebido um modelo de partilha de processos clínicos baseado em *blockchain* e, finalmente, desenvolvido um protótipo funcional para testar o modelo.

5.1 Revisão de Literatura

Na revisão de literatura, através de fontes e autores credíveis, são abordados conceitos relevantes para o sustento da importância de sistemas baseados em *blockchain* no que tange a partilha de documentos sensíveis e confidenciais como os processos clínicos de pacientes, entre entidades diferentes.

Deste capítulo, é possível constactar que já diversos países estão a dar a devida importância e atenção à partilha de processos clínicos, pelo menos, dentro do seu SNS. Destes países, nem todos o fazem com recurso a tecnologia *blockchain*, mas alguns já implementaram esta tecnologia para a partilha de processos clínicos, pelos seus altissonantes benefícios, dos quais, além de possibilitar a construção de um histórico clínico completo, altamente disponível e acessível de qualquer ponto da rede, possibilita ainda a construção de *datasets* que viabilizam estudos científicos, contribuindo para a precisão de diagnósticos.

Trata-se de uma tecnologia relativamente nova que vem sendo considerada como revolucionária por diversos sectores em todo mundo, em que a segurança é imprescindível. Das soluções alternativas existentes no mercado, *blockchain* ganha pelo facto de reunir, por padrão, propriedades de extrema importância que, em outras tecnologias, seria possível apenas com auxilio de outras tecnologias. Este facto não significa, porém, que *blockchain* é uma solução para todo e qualquer problema. É preciso analisar a viabilidade e necessidade, tal como abordado no ponto 2.3.10 do capítulo II.

5.2 Caso de Estudo

O SNS, caso de estudo do presente trabalho, é constituído pelo sector público, privado e comunitário. Não existe partilha de processos clínicos entre estes. Das entrevistas realizadas aos profissionais de saúde do arquivo clínico, foi possível auferir que os processos clínicos dos pacientes são, exclusivamente, armazenados nas Unidades Sanitárias em que tiverem sido abertas. Quando um paciente precisa ser transferido, é emitida uma guia de transferência com apenas uma parte do histórico clínico do paciente ou então um relatório médico, caso o paciente requisite para fins diversos, mas nunca o processo clínico completo.

Segundo Mércia Mandlate (2021), médica no Hospital Provincial da Matola, afirmou que em alguns raros casos os processos clínicos são permitidos a permanecer com o paciente, como forma a reduzir a irresponsabilização por perdas de processos clínicos, no entanto, esta acção não garante qualquer garantia de disponibilidade ou segurança do processo clínico.

A não partilha de processos clínicos no SNS tem consequências que se refletem em um mesmo paciente ter que abrir um novo processo clínico em cada Unidade Sanitária que fica internado, ou pior, abrir um novo processo clínico mais de uma vez na mesma unidade sanitária.

No final, o resultado das entrevistas e observações realizadas revelaram que a utilização das TICs para a partilha de processos clínicos entre as Unidades Sanitárias do SNS, com garantias de segurança e privacidade do paciente, contribuiria significativamente para a melhoria da qualidade dos serviços de assistência médica aos pacientes nas Unidades Sanitárias.

Ademais, foi possível constatar a existência de sistema de gestão de processos clínicos, no entanto, estes sistemas não se comunicam, ou seja, não existe interoperabilidade entre eles. Indo mais a fundo na entrevista, constatou-se a existência de computadores, não só nas unidades sanitárias visitadas (HCM e Clinicare), como também nas outras unidades sanitárias espalhadas, pelo menos a nível da Cidade e Província de Maputo, havendo, portanto, condições para testar e até implementar a solução, em caso de sucesso.

Em Moçambique, ainda não existe uma lei específica em torno dos processos clínicos. É, na verdade, um projecto em curso entre o Arquivo Clínico do HCM e o departamento

jurídico do mesmo lugar, que poderá se extender às demais unidades sanitárias, pois que actualmente opera-se à luz do decreto 84/2018 de 26 de Dezembro, do Sistema Nacional de Arquivos do Estado.

Quanto aos desafios constactados, o acesso à internet poderá ser um deles.

5.3 Desenvolvimento da proposta de solução

Com base nos conceitos abordados no capítulo II, os constrangimentos identificados na situação actual da partilha de processos clínicos no SNS, foi possível modelar os requisitos de um sistema que respondesse à necessidade.

O desenvolvimento do protótipo funcional do sistema proposto, foi feito seguindo a metodologia de desenvolvimento descrita no ponto 1.5.2 do capítulo I, como forma a demonstrar os conceitos apresentados no capítulo II, resolver os constrangimentos identificados no capítulo do caso de estudo, tendo em conta as informações colhidas nas entrevistas, observações e inquéritos realizados. Desta forma, o protótipo passa por uma plataforma que possibilita a partilha de processos clínicos, no SNS, baseada em *blockchain*, que garanta a descentralização, disponibilidade, integridade, privacidade e autenticidade da informação. Uma aplicação *web*, desenvolvida mediante as ferramentas e tecnologias descritas no ponto 1.5.3 do capítulo I. A aplicação poderá ser do proveito dos profissionais de saúde, bem como pacientes, estes últimos para visualizarem e concederem acessos aos seus processos clínicos.

6. Capítulo VI – Considerações finais

6.1 Conclusões

Blockchain é uma tecnologia que cobre muitas das lacunas dos modelos actuais de Tecnologia de Informação de saúde, que incluem segurança, integridade, privacidade de dados e imutabilidade, que garante identificações (codificadas), criando assim uma trilha de auditoria robusta, melhorando, consequentemente, a segurança relaccionada à saúde dos pacientes.

Por se tratar de um objecto sensível (processo clínico do paciente), cujo estado precisa ser perpetuamente armazenado, por existirem várias entidades envolvidas, por existir a necessidade de eliminar dependência de intermediários e de garantir confiança entre as partes envolvidas, *blockchain* é uma solução que se adequa a necessidade de partilha de processos clínicos, especialmente no contexto moçambicano.

Durante o curso da pesquisa, constatou-se que a inexistência de um mecanismo seguro para a partilha de processos clínicos entre as Unidades Sanitárias, incluindo o próprio paciente, é uma dor vivida pelo SNS que, no fim último, afecta a própria saúde do paciente e, portanto, comprometendo o objectivo pelo qual foi instituído o SNS, o de promover a saúde, prevenção de doenças, assistência e reabilitação para todo o cidadão Nacional.

Com vista a cooperar para a melhoria da qualidade da prestação de serviços de saúde, impactando de forma positiva a saúde dos cidadãos moçambicanos, desenvolveu-se um protótipo que demonstrasse como os processos clínicos dos pacientes podem ser compartilhados entre as Unidades Sanitárias do SNS, através da tecnologia *blockchain*, que garante alta disponibilidade, integridade, privacidade, autenticidade e descentralização da informação. E, portanto, o objectivo geral do presente trabalho foi alcançado, mediante o alcance dos objectivos específicos também definidos no início do trabalho.

6.2 Recomendações

Com a aplicação da solução proposta, espera-se poder ajudar aos pacientes em suas navegações por diferentes unidades sanitárias em busca de assistência médica, permitindo que o seu histórico clínico os acompanhe sempre, auxiliando igualmente aos profissionais de saúde na precisão das suas intervenções sobre os pacientes. Assim, recomenda-se que a solução seja experimentada nas unidades sanitárias com os

requisitos mínimos (tal como o HCM, Clinicare e Hospital Privado de Maputo) e, em caso de sucesso, os outros pontos sejam progressivamente prontificados para acomodar a solução.

Para os trabalhos futuros, recomenda-se a implementação de outros conceitos modernos como Inteligência Artificial e Análise de Dados, de modo a aproveitar os históricos clínicos de pacientes armazenados no sistema, para contribuir para o alcance de diagnósticos mais precisos, prevenção de doenças, entre outros benefícios, agregando valor a esfera da saúde.

Bibliografia

Referencias bibliográficas

[1]. Abreu, A. W. (2020). Uma Abordagem Baseada Em *Blockchain* Para Armazenamento E Controle De Acesso Aos Dados De Certificados De Alunos Do Ensino Superior.

[2]. Alves, P., Nasser, R., & Laigner, R. (2018). Desmistificando *Blockchain*: Conceitos e Aplicações.

[3]. Amadeu Martins, Rui Pedro Freitas, Sérgio Ribeiro, Atlas de Oportunidades | Ficha de País | Alemanha, 2013.

[4]. A.S. Tanenbaum, “Computer Networks”, 5th Edition, Pearson Education, 2010.

[5]. Barbosa, Eduardo F., Instrumentos de coleta de dados em pesquisas educacionais, s/ed., s/l., 2008. Obtido em:http://www.inf.ufsc.br/~vera.carmo/Ensino_2013_2/Instrumento_Coleta_Dados_Pesquisas_Educacionais.pdf. 22/06/2021, 00:51.

[6]. Boiani, F. (2018). *Blockchain* Based Electronic Health Record Management For Mass Crisis Scenarios. Stockholm.

[7]. Coelho, Beatriz (2019). Tipos de pesquisa: abordagem, natureza, objetivos e procedimentos. Obtido em: https://blog.mettzer.com/tipos-de-pesquisa/. 23/03/2021, 12:45

[8]. Costa, Andre (2012). Metodologia de pesquisa, Rio grande do norte. Obtido em: https://docente.ifrn.edu.br/andreacosta/desenvolvimento-de-pesquisa/metodologia-da-pesquisa. 22/06/2021, 01:03.

[9]. da Silva, L. (2020). Saúde Digital: a Interoperabilidade e a Tecnologia *Blockchain*.

[10]. Decreto-Lei n. 5/75 de 19 de agosto de 1975 (MZ). Dispõe sobre a nacionalização das clínicas privadas. Boletim da República, I Série, n. 24, 19 de agosto de 1975.

[11]. Diploma Ministerial nº 127/2002. Caracterização técnica, enunciado de funções específicas, critérios e mecanismos para a classificação das instituições do SNS;

[12]. Estatuto do Servico Nacional de Saude, (1993), Lei nr 11/93, Ministerio da Saude. Portugal

[13]. Generoso, M. A. (2019). Dependency Rank: Método De Priorização De Requisitos Baseado Nas Relações De Dependência Identificadas Por Pln.

[14]. Gerhardt, T. E. & Silveira, D. T., 2009. Métodos de Pesquisa, s.l.

[15]. Gil, A. C. (2002). Como elaborar projetos de pesquisa (4a Ed.). São Paulo: Atlas.

[16]. Gil, Antônio Carlos (2002). Como elaborar projetos de pesquisa (4 ed.). São Paulo: Atlas.

[17]. Gustavo. (2009). Introdução a UML.

[18]. Hopper, T. Distributed relational database architecture: connectivity guide. IBM Corporation, 4 ed. Prentice Hall PTR, 1995.

[19]. Kumar, R., & Marchang, N. (2020). Distributed off-chain Storage of Patient Diagnostic Reports in Healthcare System using IPFS and *Blockchain*.

[20]. Lei n. 25/91 de 31 de dezembro de 1991 (MZ). Dispõe sobre a criação do Serviço Nacional de Saúde. Boletim da República. I Série, n. 54, 31 de dezembro de 1991.

[21]. Leslie Lamport. Paxos made simple. ACM SIGACT News (Distributed Computing Column) 32, 4 (Whole Number 121, December 2001), pages 51–58, December 2001.

[22]. Mandlate, M. (2021). Entrevista com profissionais de saúde.

[23]. Manhica, R. (14 de Junho de 2021). Entrevista com enfermeiras.

[24]. Marconi, M. d., & Lakatos, E. M. (2003). Fundamentos de Metodologia Científica (5a ed.). São Paulo: Editora Atlas.

[25]. Martins, Everton (2019). Coleta de dados: o que é, metodologias e procedimentos. Obtido em: https://blog.mettzer.com/coleta-de-dados/. 23/03/2021, 13:14.

[26]. Ministério da Saúde. (2007). Informe sobre Recursos Humanos para Saúde no Serviço Nacional de Saúde de Moçambique. Maputo.

[27]. Mitano, Fernando; Ventura, Carla; Lima, Monica; et. al, Direito à saúde: (in)congruência entre o arcabouço jurídico e o sistema de saúde, Rev. Latino-Am. Enfermagem, 2016.

[28]. Morsch, José (2020). O que é importante constar no histórico do paciente . Obtido em: https://telemedicinamorsch.com.br/blog/historico-do-paciente. 22/03/2021 , 18:09.

[29]. PEREIRA, Kevin. Bitcoin: uma análise jurídico-tributária da moeda virtual. 2016. 71f. Trabalho de Conclusão de Curso – UFAM, Manaus. 2016

[30]. Relatório de Revisão do Sector de Saúde (RSS) de Moçambique. MISAU. Dezembro 2012.

[31]. República De Moçambique. Ministério Da Saúde. Direcção Nacional De Assistência Médica - Carga tipo Hospital rural e geral. Pacote de serviços prestados e equipamento médico necessário. Setembro de 2007. Maputo: Direcção Nacional de Assistência Médica. Ministério da Saúde. República de Moçambique, 2007.

[32]. Rocha, V., & De Paula, R. (2019). *Blockchain* e Aplicações em Saúde.

[33]. Rodrigues, R. (2003). O pontuário electrónico do paciente na assistência, informação e conhecimento médico.

[34]. Satoshi Nakamoto (2008). Bitcoin: A peer-to-peer electronic cash system.

[35]. Spruit, M., & Brinkhuis, M. (2018). Decoding the hype: *Blockchain* in Healthcare. *A Software Architecture for the provision of a patient summary to overcome interoperability issues.*

[36]. Sommerville, I. (2011). Software Engineering (19 ed.). Nova Iorque: Pearson.

[37]. Stadzisz, Paulo (2002). Projeto de Software usando a UML. Paraná: Centro Federal de Educação Tecnológica do Paraná.

[38]. Terence, Ana, Escrivão Filho, Edmundo (2006). Abordagem quantitativa, qualitativa e a utilização da pesquisa-ação nos estudos organizacionai. Fortaleza, CE, Brasil.

[39]. Vitalik Buterin. On public and private *blockchain*s. Ethereum blog, 7, 2015.

[40]. Young, R. R. The Requirements Engineering Handbook. Boston: Artech House, 2004. 251p.

[41]. Yuhong, J., & Zhang, M. (2018). *Blockchain* for healthcare records: a data perspective.

Outras bibliografias consultadas

[1]. Lu, Q.; Xu, X.; Liu, Y.; Zhang, W. *Design pattern as a service for blockchain applications. In: 2018 IEEE International Conference on Data Mining Workshops (ICDMW). New York*, NY, USA: IEEE, 2018. p. 128–135. ISSN 2375-9259.

[2]. Nakagawa, E. Y.; Oquendo, F.; Becker, M. Ramodel*: A reference model for reference architectures. In: 2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture. New York*, NY, USA: IEEE, 2012. p. 297–301.

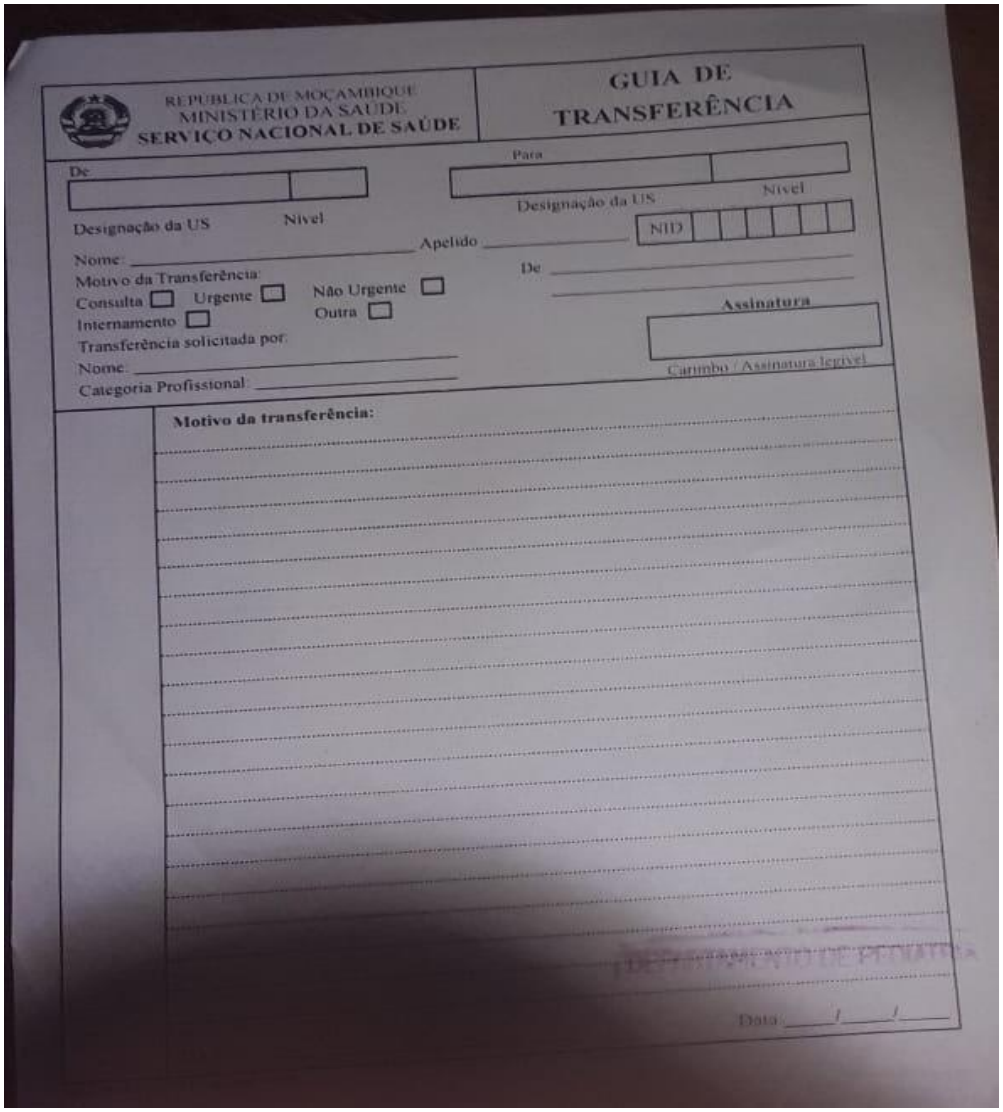
[3]. Wan, Z.; Xia, X.; Hassan, A*. E. What is discussed about blockchain? a case study on the use of balanced lda and the reference architecture of a domain to capture online discussions about blockchain platforms across the stack exchange communities. IEEE Transactions on Software Engineering*, p. 1–1, 2019. ISSN 1939-3520

[4]. Xu, X.; Pautasso, C.; Zhu, L.; Lu, Q.; Weber, I. *A pattern collection for blockchain based applications. In: Proceedings of the 23rd European Conference on Pattern Languages of Programs. New York, NY, USA: Association for Computing Machinery*, 2018. (EuroPLoP ’18). ISBN 9781450363877. Disponível em: https://doi.org/10.1145/3282308.3282312. Acesso em: 20 nov. 2020.

[5]. Xu, X.; Weber, I.; Staples, M. *Blockchain in software architecture. In: Architecture for Blockchain Applications. Cham: Springer International Publishing*, 2019. p. 83–92. ISBN 978-3-030-03035-3. Disponível em: https:// doi.org/10.1007/978-3-030-03035-3_5. Acesso em: 20 nov. 2020.

Anexos

Anexo 1: Exemplo de guia de transferência em uso no SNS.


REPUBLICA DE MOÇAMBIQUE
MINISTÉRIO DA SAÚDE
SERVIÇO NACIONAL DE SAÚDE

GUIA DE TRANSFERÊNCIA

De
Designação da US
Nivel
Nome
Apelido
Motivo da Transferência:
Consulta ☐ Urgente ☐ Não Urgente ☐
Internamento ☐ Outra ☐
Transferência solicitada por:
Nome
Categoria Profissional

Para
Designação da US
Nivel
NID
De
Assinatura
Carimbo / Assinatura legível

Motivo da transferência:

Data ____/____/____

Figura A1-1: Guia de transferência em uso no SNS.

Anexo 2: Guião de Entrevista

Entrevista aberta ao chefe do arquivo clínico do HCM.

1. Onde são guardados os processos clínicos dos pacientes?
2. Os processos clínicos são completamente partilhados com outras unidades sanitárias do SNS?
3. De que forma as informações clínicas dos pacientes são partilhados com outras unidades sanitárias do SNS (processo/fluxo) e em que circunstancias?
4. Os pacientes têm tido acesso aos seus processos clínicos?
5. Tem conhecimento da existência de algum sistema de gestão de processos clínicos em utilização dentro do SNS?
6. Existem computadores na unidade Sanitária? Se sim, quantos?
7. Tem conhecimento da existência de alguma lei moçambicana em torno dos processos clínicos dos pacientes?
8. Durante o processo de assistência médica a um paciente quais são os desafios enfrentados quando não se tem o histórico clínico do paciente?

Respostas

1.R: os processos clínicos dos pacientes são armazenados em formato físico, no arquivo clínico.

2.R: Não. Os processos clínicos não são partilhados entre as unidades sanitárias.

3.R: as informações clínicas dos pacientes são partilhadas através de guias de transferência ou relatório médico. Caso o paciente que se encontra internado precise ser transferido para outra unidade sanitária, é emitida uma guia transferência. Caso o paciente precise de informações relaccionadas a sua saúde para qualquer fim, este pode solicitar um relatório médico.

4.R: geralmente não. No entanto, algumas unidades sanitárias já experimentaram deixar o processo clínico na posse do paciente, na tentativa de contornar a ocorrência de perdas de processos clínicos de pacientes na unidade sanitária.

5.R: sim. Existem sistemas informáticos em fase inicial de utilização. No entanto, estes não se comunicam, ou seja, o processo clínico aberto na unidade sanitária X, não é visível na unidade sanitária Y.

6.R: Sim. Existem computadores nas enfermarias (dois por cada, isto porque as urgências não reúnem ainda condições para tal), no arquivo clínico (4) e nas urgências (até o dia da entrevista, ainda nenhum pois a rede de internet do hospital não tinha alcance).

7.R: Não. Não existe uma lei nacional que rege a questão dos processos clínicos dos pacientes. No entanto, opera-se à luz do decreto 84/2018 de 26 de Dezembro, do Sistema Nacional de Arquivos do Estado, de onde cada instituição deverá criar uma legislação mediante o seu contexto. O Arquivo Clínico e o departamento jurídico do HCM estão a trabalhar no sentido de produzir esta legislação e então expandir para as outras unidades sanitárias do SNS.

8.R: depender apenas da guia de transferência não oferece uma visão holística da saúde do paciente. Assim, as intervenções são feitas apenas com base nas informações disponíveis naquele momento.

Anexo 3: Descrição de casos de uso

O sistema é composto por doze (12) casos de uso, sendo apresentadas as suas especificações a seguir.

CU01. Cadastrar utilizador

Tabela A3-1: CU01.Cadastrar utilizador

Nome	Cadastrar utilizador
Descrição	Permite registar utilizadores no sistema para que possam ter acesso ao sistema e para que seja possível relaccionar determinadas acções com os respectivos actores no sistema.
Actor	Profissional de saúde (admin)
Prioridade	Essencial
Pré-condição	Ter acesso e permissões no sistema.
Pós-condição	Posse das credenciais do novo utilizador.
Fluxo principal de eventos	
Actor	**Actividades**
Admin	1.Fazer login;
Admin	2.Seleccionar a opção “Cadastrar Paciente” ou “Cadastrar profissional de Saúde”;
Admin	3.Preencher formulário de cadastro e guardar informação;
Sistema	4.Registar informação e gerar credenciais do utilizador;
Sistema	5.Imprimir as credenciais do utilizador.

CU02. Excluir utilizador

Tabela A3-2: CU02.Excluir utilizador

Nome	Excluir utilizador
Descrição	Consiste em apagar as credenciais de determinado utilizador, barrando o seu acesso ao sistema.
Actor	Profissional de saúde (admin)

Prioridade	Importante
Pré-condição	Tanto o utilizador que exclui como o que é excluído devem estar cadastrados no sistema.
Pós-condição	Menos utilizadores com acesso ao sistema.
Fluxo principal de eventos	
Actor	**Actividades**
Admin	1.Seleccionar a opção “Lista de utilizadores”;
Sistema	2.Imprimir lista de utilizadores cadastrados;
Admin	3.Seleccionar a opção “Excluir” ao lado do nome do utilizador;
Sistema	4.Remover utilizador do sistema .

CU03. Iniciar sessão

Tabela A3-3: CU03.Iniciar sessão

Nome	Iniciar sessão
Descrição	Permite que os utilizadores acedam ao sistema, ganhando permissão para utilizar funcionalidades específicas, de acordo com o tipo de conta associada.
Actor	Profissional de saúde, Paciente
Prioridade	Essencial
Pré-condição	Estar cadastrado no sistema
Pós-condição	Acesso as funcionalidades do sistema, de acordo com o tipo de utilizador
Fluxo principal de eventos	
Actor	**Actividades**
Utilizador	1.Introduzir credenciais de acesso;
Sistema	2.Validar
Sistema	3.Redireccionar utilizador a sua página inicial, em caso de sucesso, ou emitir mensagem “Credenciais Inválidas, tente novamente”, em caso de insucesso.

CU04.Terminar sessão

Tabela A3-4: CU04.Terminar sessão

Nome	Terminar sessão
Descrição	Permitir que um utilizador, dentro do sistema, saia do sistema quando sentir necessidade de o fazer
Actor	Profissional de saúde, Paciente
Prioridade	Essencial
Pré-condição	Ter a sessão iniciada.
Pós-condição	Inacessibilidade das funcionalidades do sistema para este utilizador
Fluxo principal de eventos	
Actor	**Actividades**
Utilizador	1.Seleccionar opção “Terminar Secção”;
Sistema	2.Pedir confirmação e terminar secção;
Sistema	3.Exibir a página de introdução de credenciais.

CU05.Garantir acessos

Tabela A3-5: CU05.Garantir acessos

Nome	Garantir acessos
Descrição	Permite ao paciente dar acesso ao seu processo clínico aos profissionais de saúde que precisem visualizar ou também adicionar informação ao seu processo, com o seu consentimento.
Actor	Paciente
Prioridade	Essencial
Pré-condição	Estar com a sessão inciada no sistema.
Pós-condição	Mais um profissional de saúde com acesso ao processo clínico do paciente em questão.
Fluxo principal de eventos	

Actor	Actividades
Profissional de saúde	1.Enviar requisição;
Sistema	2.Enviar mensagem contendo o código de acesso ao titular do processo clínico;
Paciente	3.Partilhar código de acesso com o profissional de saúde;
Profissional de saúde	4.Introduzir código;
sistema	5.Exibir processo clínico do paciente.

CU06.Remover acessos

Tabela A3-6: CU06.Remover acessos

Nome	Remover acessos
Descrição	Permite ao paciente remover o acesso ao seu processo clínico, do profissional de saúde que, por alguma razão, sentir não mais conveniente que tenha acesso.
Actor	Paciente
Prioridade	Essencial
Pré-condição	Estar com a sessão inciada no sistema.
Pós-condição	Indisponibilidade do processo clínico para o profissional de saúde com os acessos retirados.
Fluxo principal de eventos	
Actor	**Actividades**
Paciente	1.Seleccionar a opção “Ver lista de profissionais de saúde”;
Sistema	2.Carregar lista de profissionais de saúde;
Paciente	3.Clicar no botão “Remover acesso”, referente a determinado profissional de saúde;
Sistema	4.Excluir profissional de saúde do sistema.

CU07.Visualizar processos clínicos

Tabela A3-7: CU07.Visualizar processos clínicos

Nome	Visualizar processos clínicos
Descrição	Permite aos utilizadores, tanto o paciente quanto o profissional de saúde devidamente autorizado, visualizarem o processo clínico, sem possibilidade de edição, para o caso do paciente.
Actor	Profissional de saúde, Paciente
Prioridade	Essencial
Pré-condição	Ter acesso, permissões e a sessão iniciada no sistema.
Pós-condição	Exibição do processo clínico
Fluxo principal de eventos	
Actor	**Actividades**
Paciente	1.Introduzir credenciais de acesso;
Sistema	2.Validar credenciais e exibir processo clínico, em caso de sucesso;
Profissional de Saúde	3.Pesquisar paciente através do NID;
Sistema	4.Carregar paciente;
Profissional de saúde	5.Clicar no botão “Pedir para ver” ou “Pedir para ver e escrever”;
Paciente	6.Partilhar código de acesso, enviado pelo sistema, com o profissional de saúde;
Profissional de saúde	7.Inserir código e Visualizar processo clínico.

CU08.Abrir processo clínico

Tabela A3-8: CU08.Abrir processo clínico

Nome	Abrir processo clínico
Descrição	"Abrir processo clínico" é a funcionalidade do sistema que permite ao profissional de saúde reunir todos os documentos e dados clínicos de um determinado paciente no sistema.
Actor	Profissional de saúde
Prioridade	Essencial
Pré-condição	Ter acesso e permissões no sistema.
Pós-condição	Processo clínico aberto, disponível para adicionar novas informações
Fluxo principal de eventos	
Actor	**Actividades**
Admin	1.Fazer *login*;
Admin	2.Cadastrar paciente.

CU09. Adicionar informação ao processo clínico

Tabela A3-9: CU09. Adicionar informação ao processo clínico

Nome	Adicionar informação ao processo clínico
Descrição	Esta funcionalidade permite manter os processos clínicos dos pacientes actualizados, através da adição de mais informações sobre a evolução da saúde dos pacientes aos processos outrora abertos.
Actor	Profissional de saúde
Prioridade	Essencial
Pré-condição	Ter acesso e permissões no sistema e o processo clínico ao qual se deseja adicionar informação deverá estar criado.
Pós-condição	Processo clínico actualizado.
Fluxo principal de eventos	

Actor	Actividades
Profissional de saúde	1.Pesquisar paciente;
Sistema	2.Exibir paciente;
Profissional de saúde	3.Pedir acesso para ver e escrever;
Paciente	4.Conceder acesso;
Profissional de saúde	5.Visualizar e adicionar informação.

CU10. Pesquisar processo clínico

Tabela A3-10: CU10. Pesquisar processo clínico

Nome	Pesquisar processo clínico
Descrição	Permite aos utilizadores pesquisarem processos clínicos de forma dinâmica. O utilizador poderá filtrar de acordo com o Número de Identificação do Doente (NID).
Actor	Profissional de saúde.
Prioridade	Essencial
Pré-condição	Ter acesso e permissões no sistema.
Pós-condição	Exibição do processo clínico ou da mensagem de indicação de inexistência do mesmo no sistema.
Fluxo principal de eventos	
Actor	**Actividades**
Profissional de saúde	1.Fazer *login*;
Sistema	2.Exibir página para pesquisa de processo clínico/paciente;
Profissional de saúde	3.Pesquisar pelo NID.

CU11.Recuperar senha

Tabela A3-11: CU11.Recuperar senha

Nome	Recuperar senha
Descrição	Permite que o utilizador recupere sua senha, caso se tenha esquecido, para que continue a ter permissão para aceder ao sistema.
Actor	Profissional de saúde, Paciente
Prioridade	Essencial
Pré-condição	não existe pré-condição
Pós-condição	posse de uma nova senha de acesso
Fluxo principal de eventos	
Actor	**Actividades**
Utilizador	1.Seleccionar a opção “Recuperar senha”
Sistema	2.Enviar email ou mensagem para o utilizar com a senha nova.

CU12. Cadastrar Unidade Sanitária

Tabela A3-12: CU12. Cadastrar Unidade Sanitária

Nome	Cadastrar Unidade Sanitária
Descrição	Permite que uma unidade sanitária seja adicionada a rede.
Actor	Admin
Prioridade	Essencial
Pré-condição	Ter permissões no sistema
Pós-condição	Mais um ponto integrante da rede, isto é, mais uma unidade sanitária cadastrada na rede.
Fluxo principal de eventos	
Actor	**Actividades**
Utilizador	1.Fazer “*Login*”
Sistema	2.Clicar em “Cadastrar Unidade Sanitária”

Anexo 4: Diagrama de classes

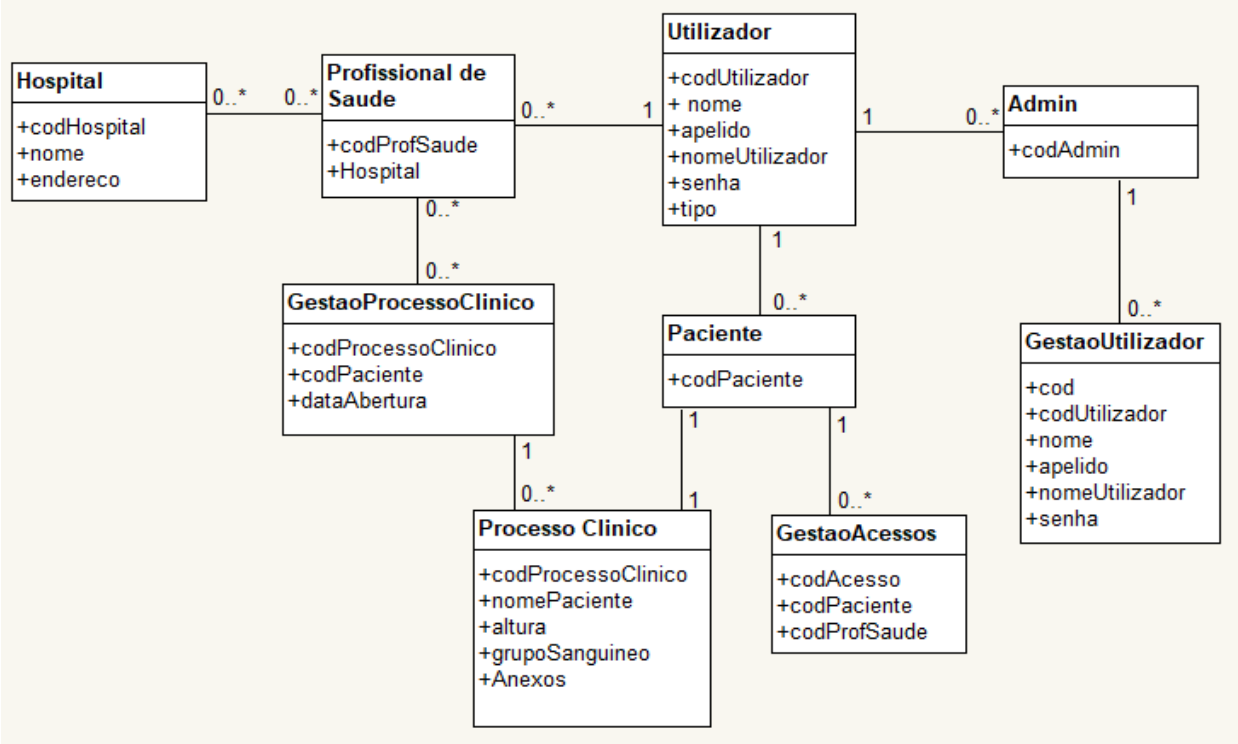


Figura A4- 1: Diagrama de classes

Anexo 5: Diagrama de actividade

- **DA01. Abrir Processo Clínico**

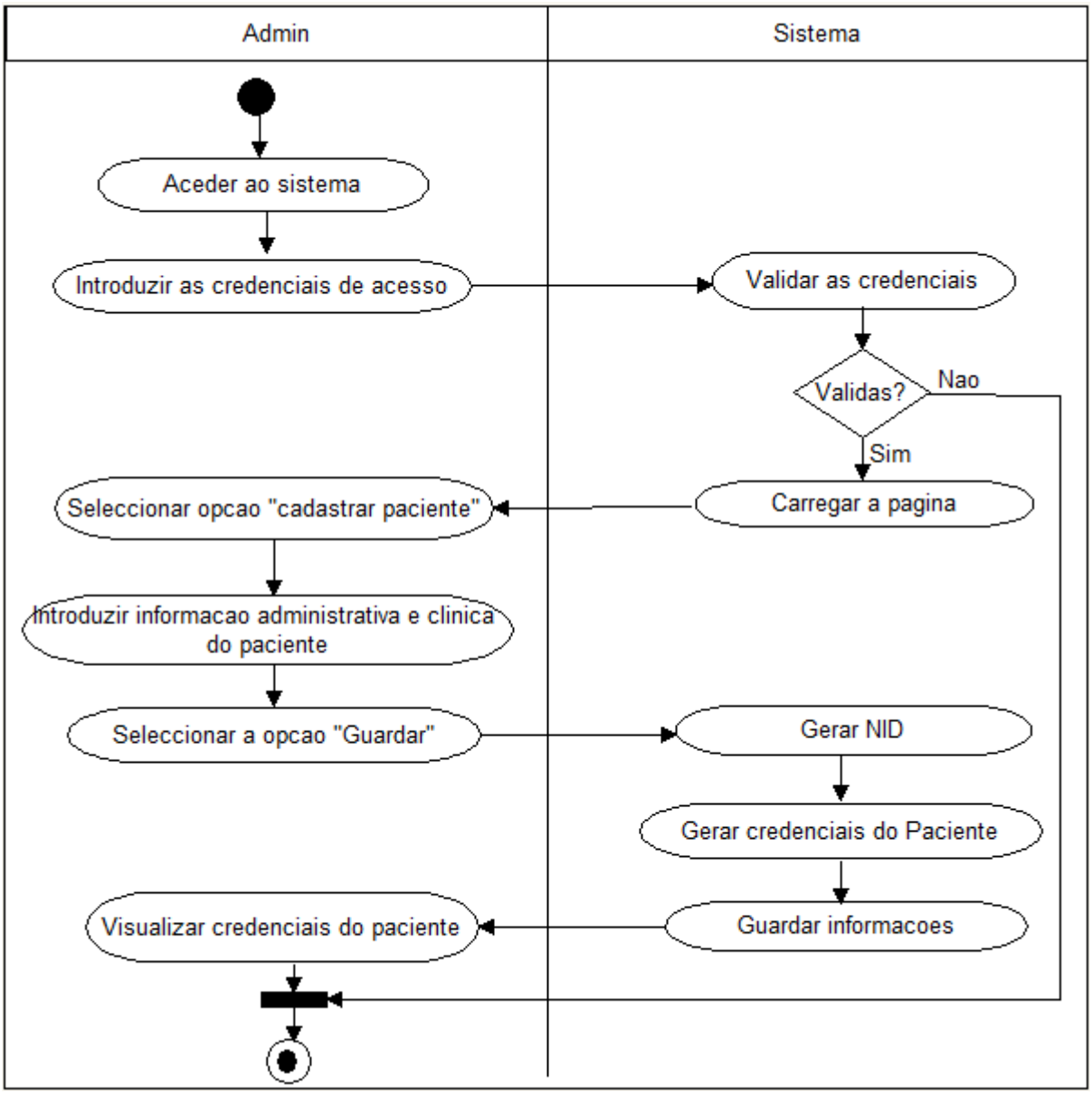


Figura A5- 1: DA01. Abrir Processo Clínico

- **DA02.Visualizar Processo Clínico**

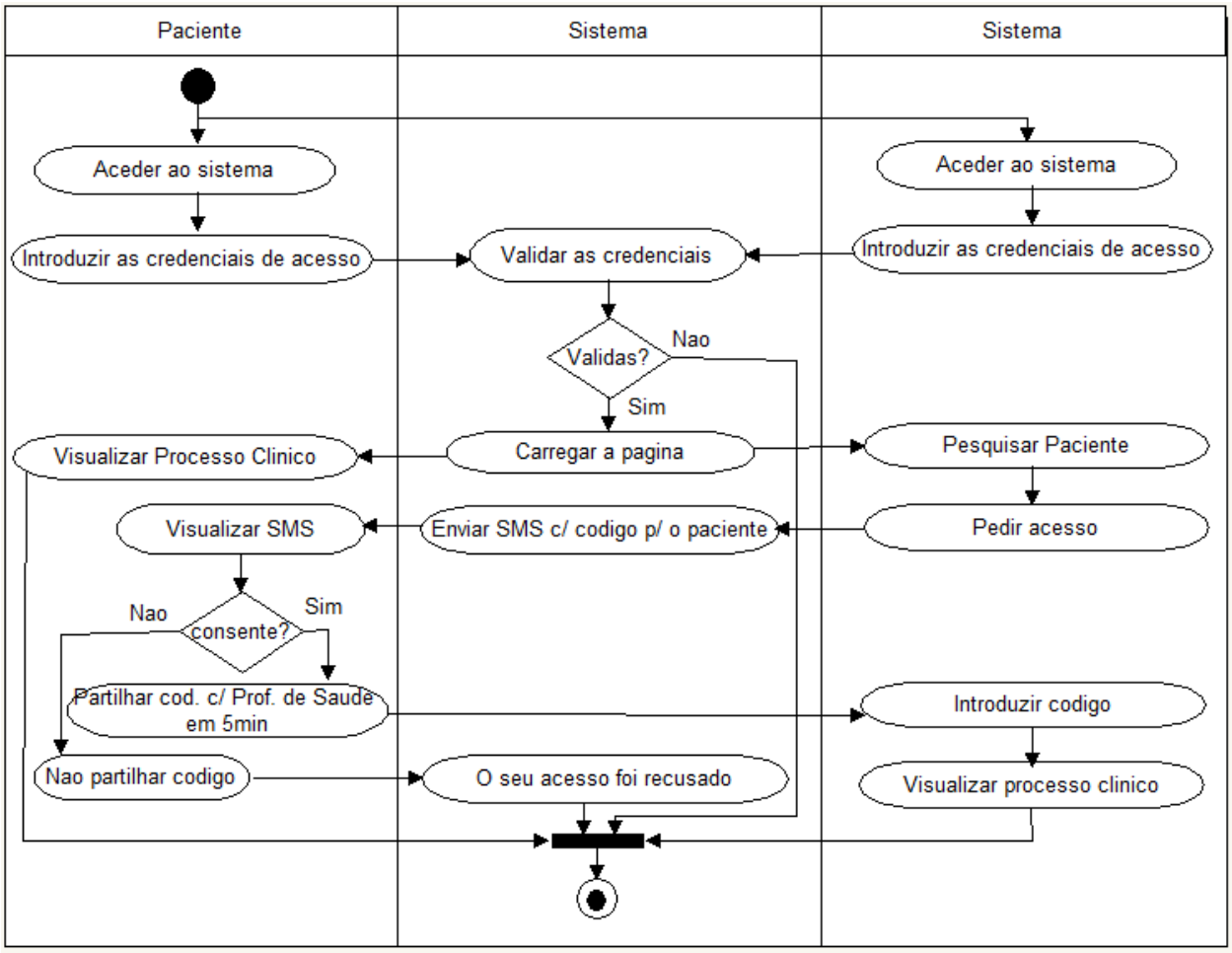


Figura A5- 2: DA02.Visualizar Processo Clínico

- **DA03. Remover Acesso**

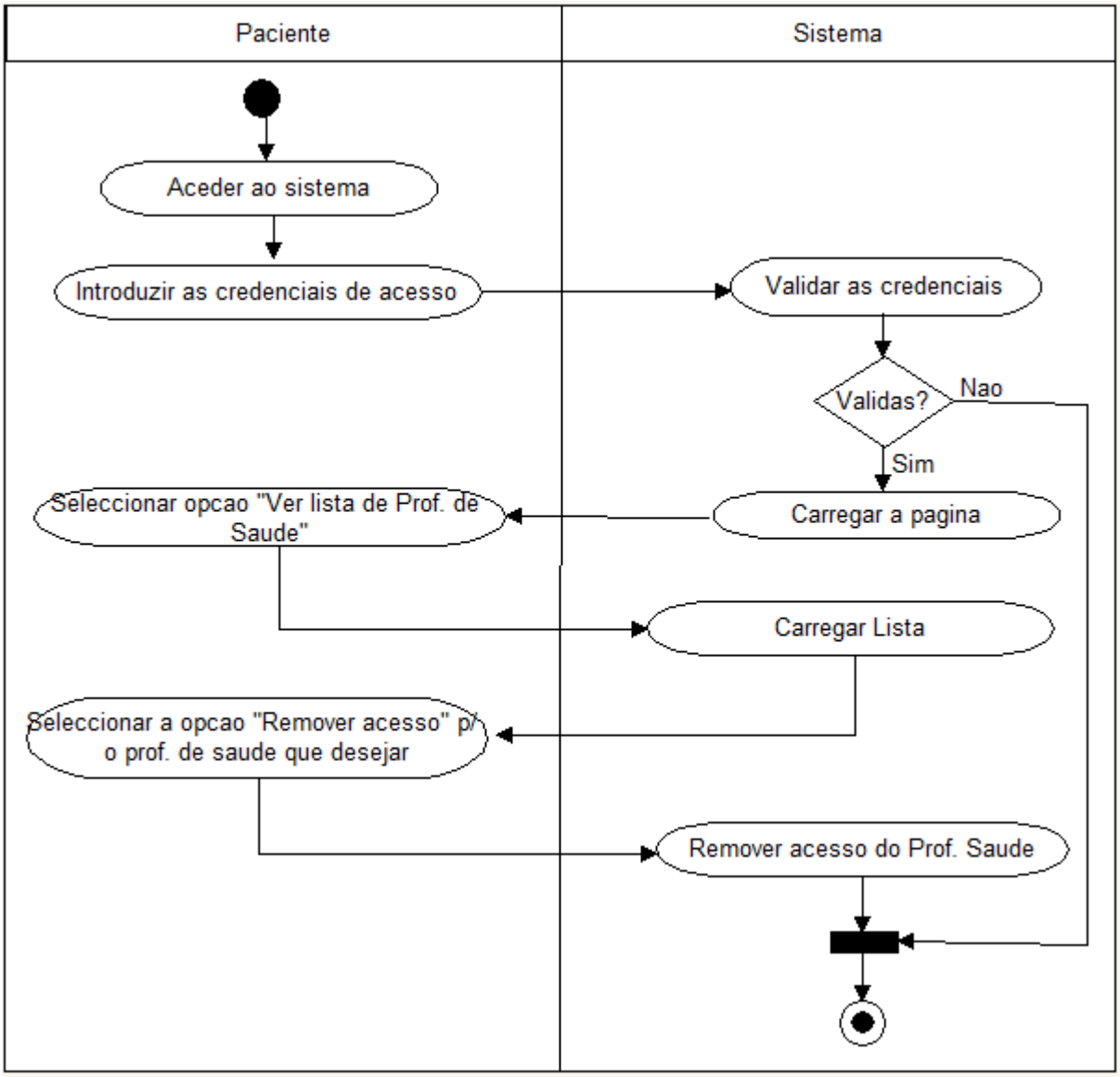


Figura A5- 3: DA03. Remover Acesso

Anexo 6: Diagrama de sequência

- **Diagrama de sequência do caso de uso “Abrir Processo Clínico”**

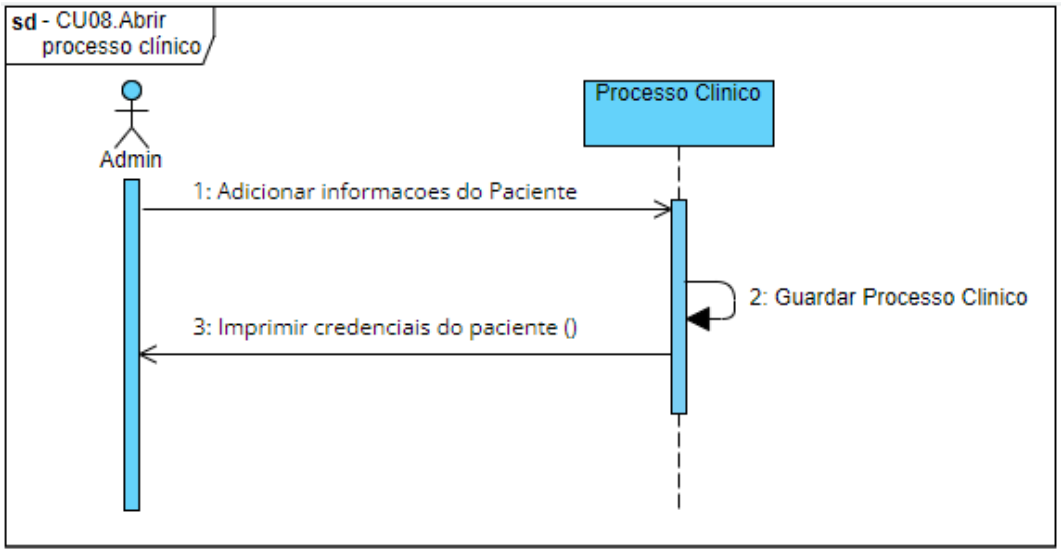


Figura A6- 1: Diagrama de sequência do caso de uso “Abrir Processo Clínico”

- **Diagrama de sequência do caso de uso “Visualizar Processo Clínico” (Profissional de Saúde)**

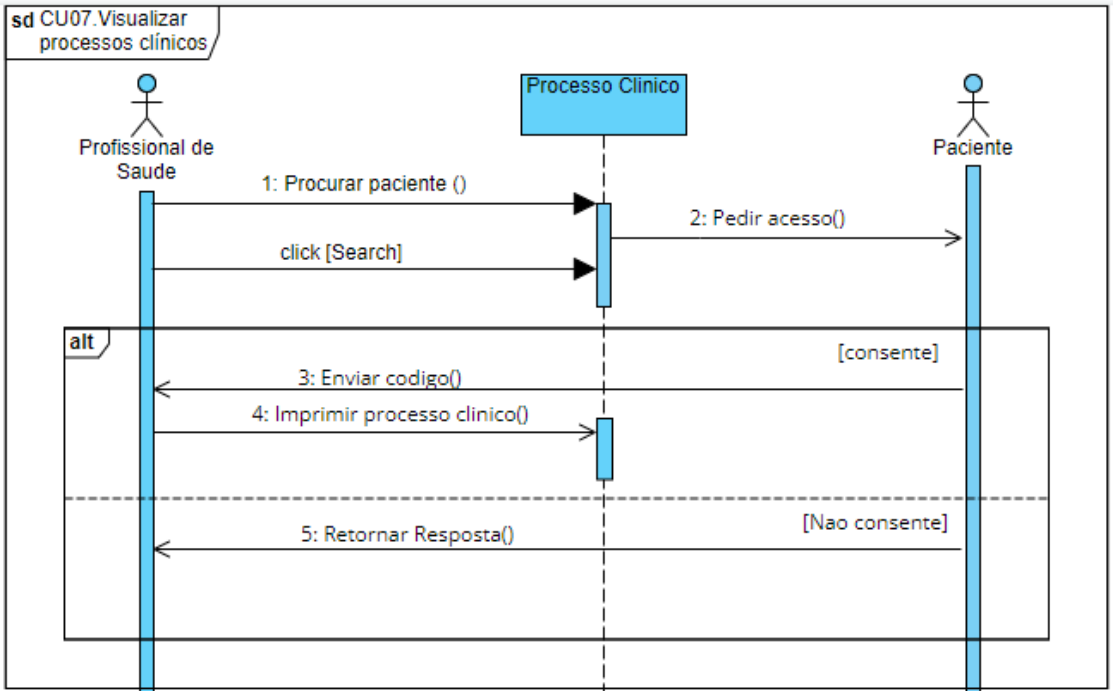


Figura A6- 2: Diagrama de sequência do caso de uso “Visualizar Processo Clínico” (Profissional de Saúde)

- **Diagrama de sequência do caso de uso “Remover acessos”**

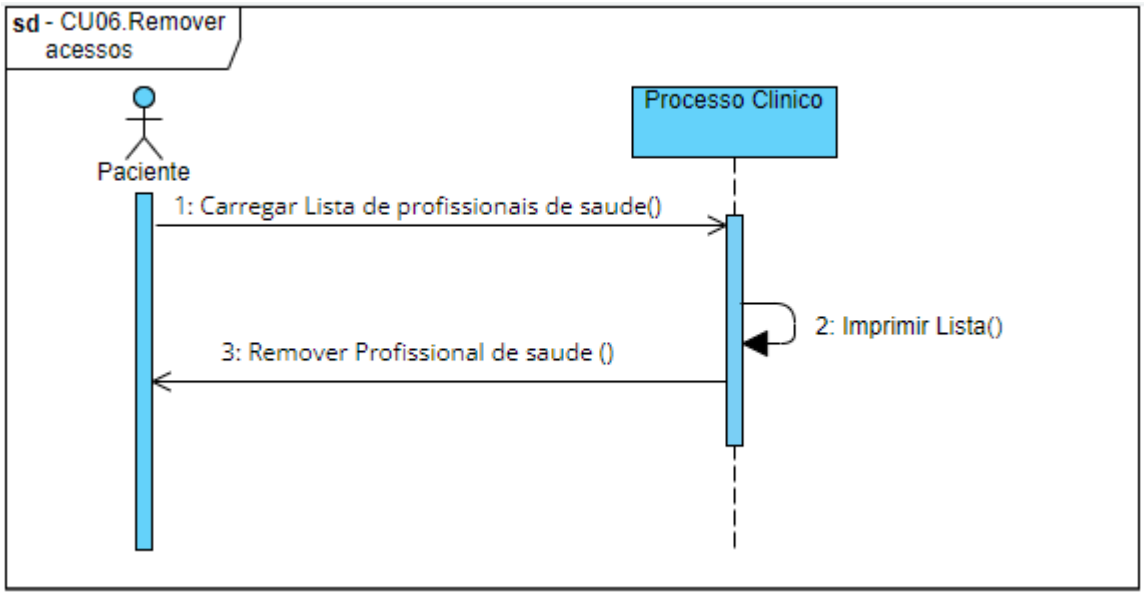


Figura A6- 3: Diagrama de sequência do caso de uso “Remover acessos”

Anexo 7: Diagrama de estado

- **Diagrama de estado do objecto “Pedir acesso”**

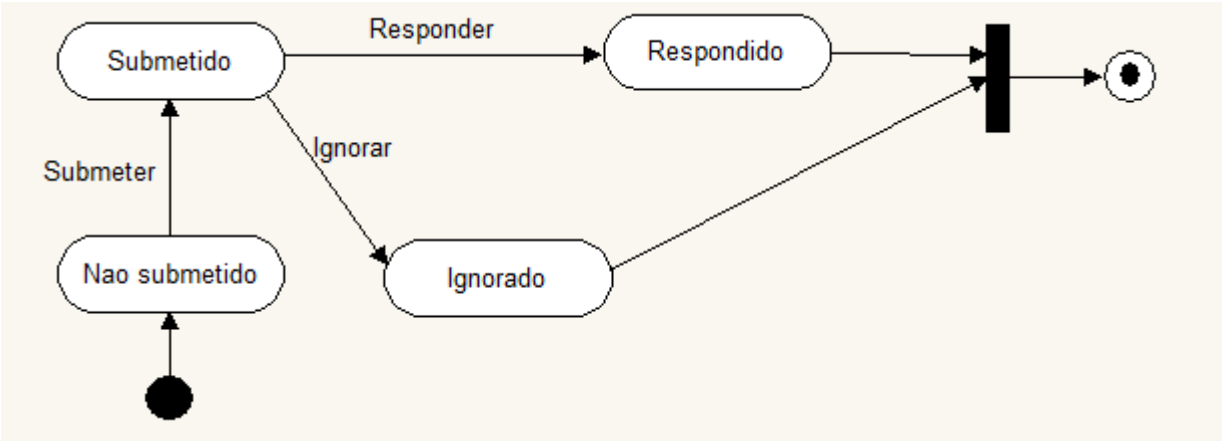


Figura A7- 1:Diagrama de estado do objecto “Pedir acesso”

Anexo 8: Protótipo

Nesta secção são apresentadas as interfaces que compõem as janelas funcionais do sistema.

- **Página de *Login***

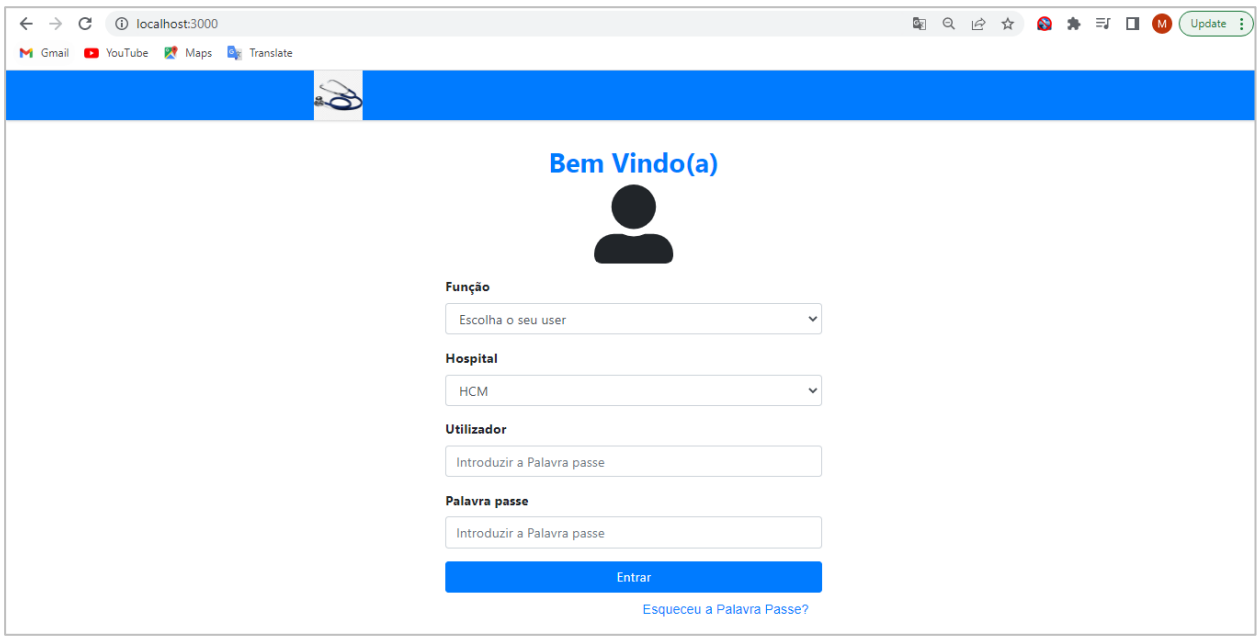


Figura A8- 1: Página de Login

- **Página de Admin**

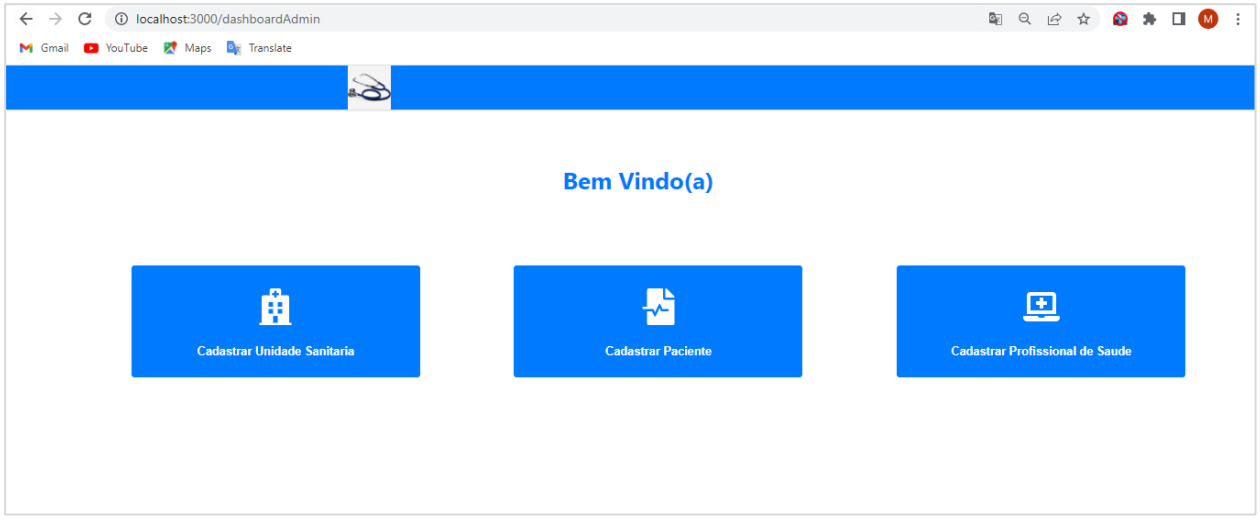


Figura A8- 2: Página de Admin

- **Cadastrar Unidade Sanitária**

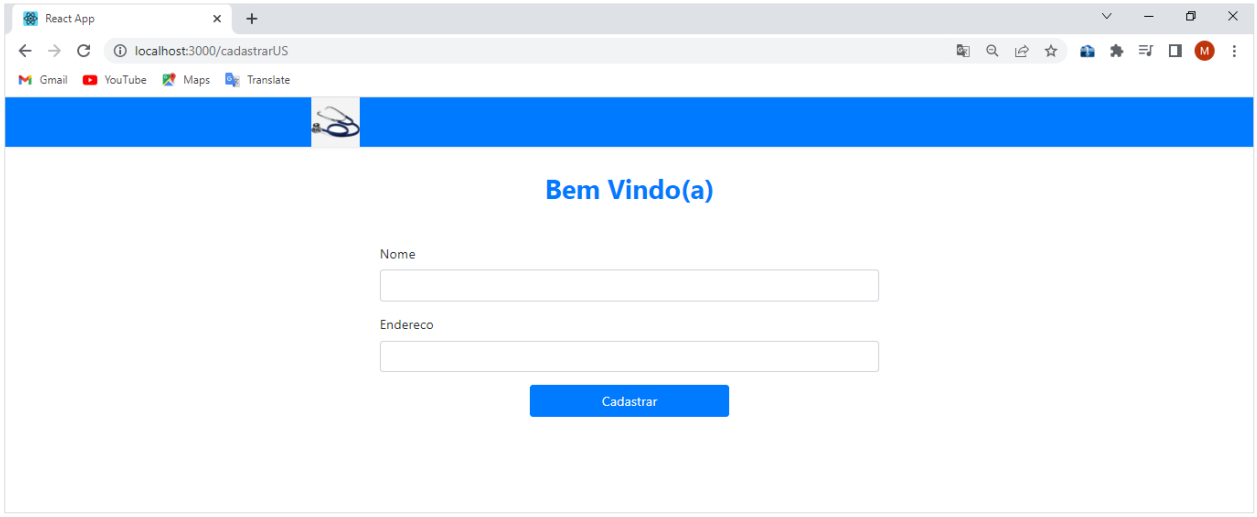


Figura A8- 3: Cadastrar Unidade Sanitária

- **Cadastrar Paciente**

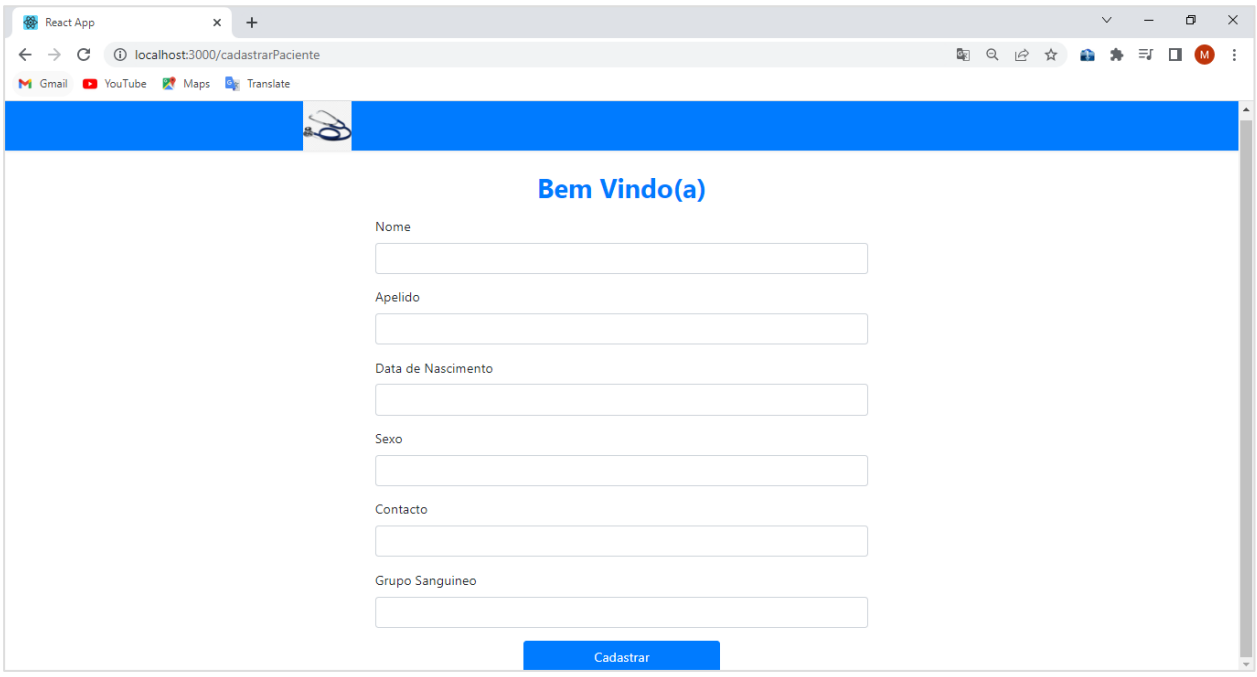


Figura A8- 4: Cadastrar Paciente

- **Cadastrar Profissional de saúde**

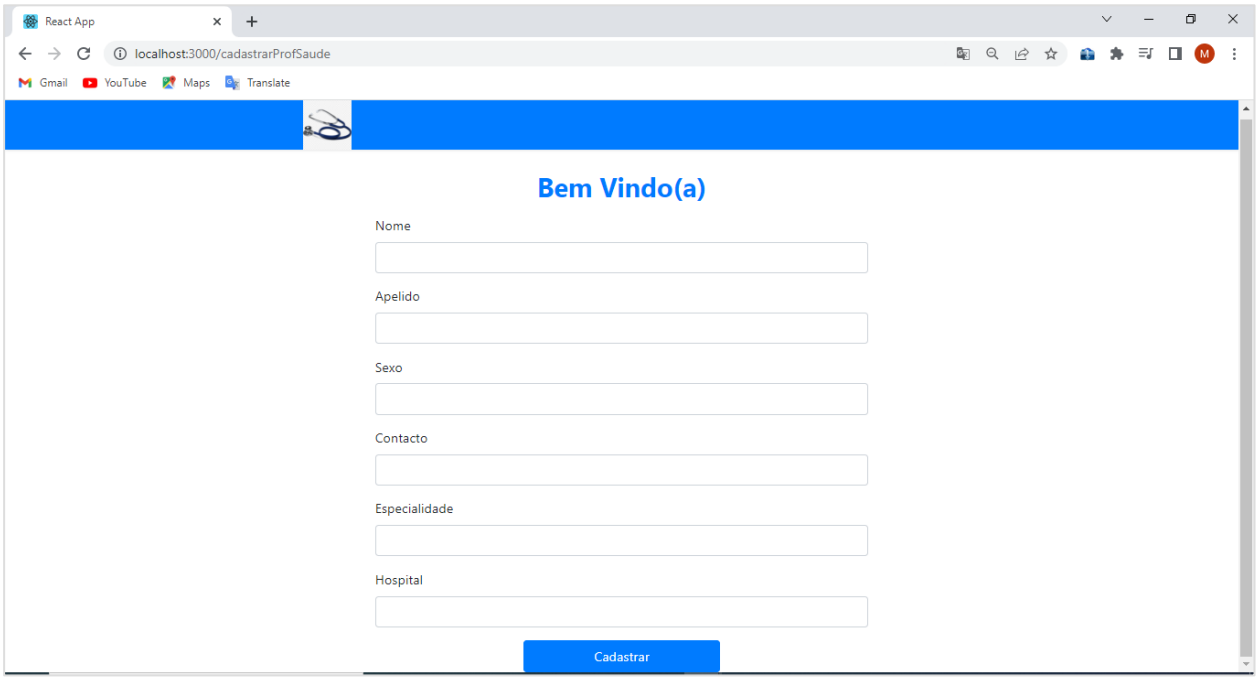


Figura A8- 5: Cadastrar Profissional de saúde

- **Visualizar Processo Clínico**

Figura A8- 6: Visualizar Processo Clínico

- **Ver Lista de Profissionais de Saúde (pelo paciente)**

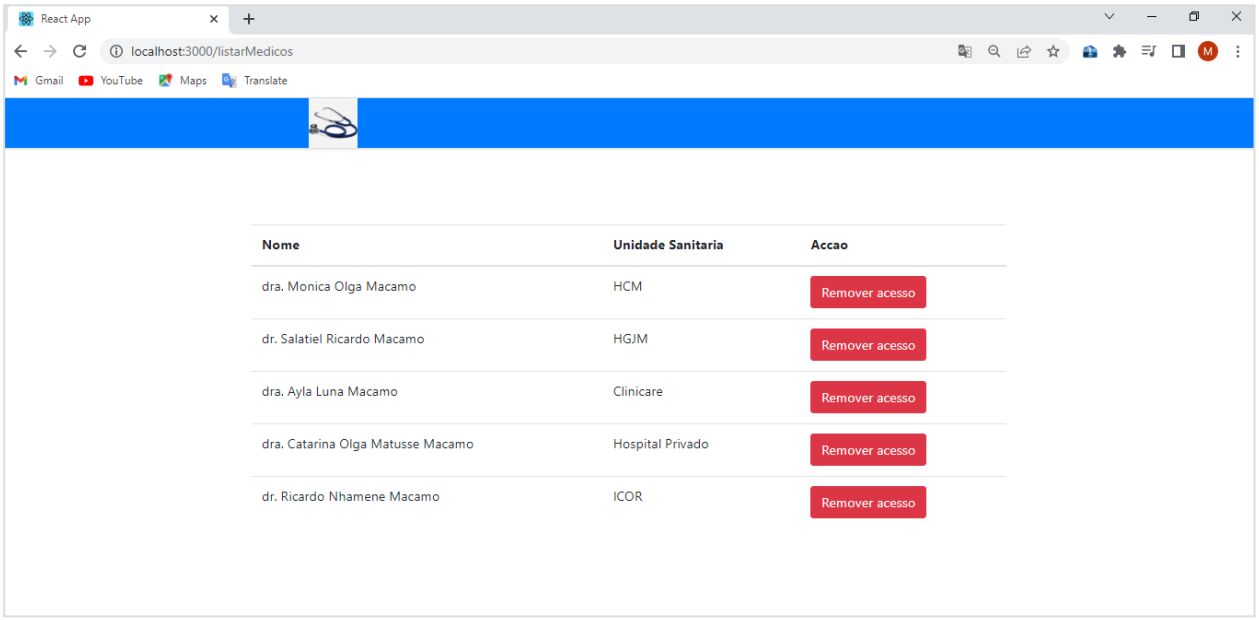


Figura A8- 7: Ver Lista de Profissionais de Saúde (pelo paciente)

- **Pesquisar Paciente**

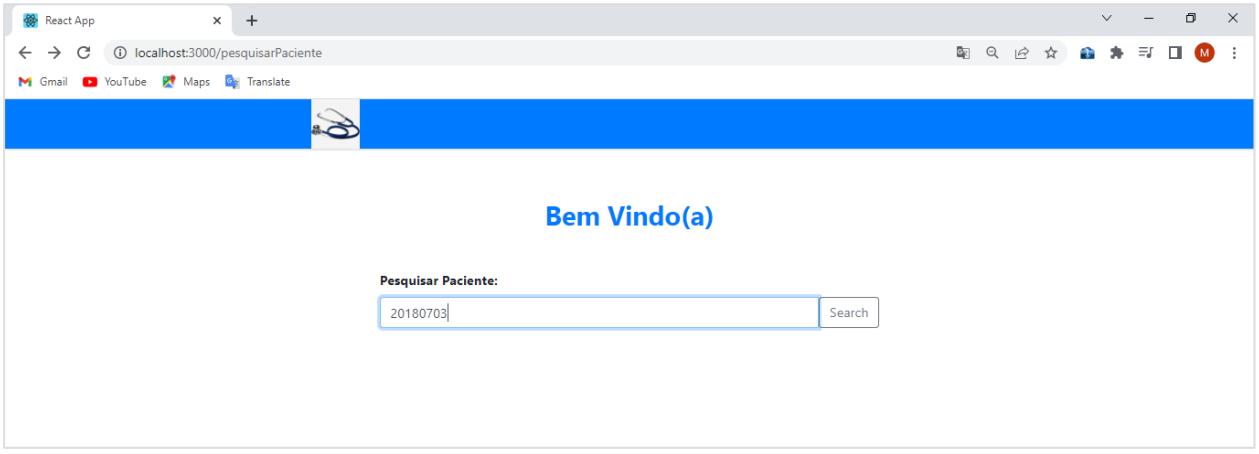


Figura A8- 8: Pesquisar Paciente

Segue o resultado após a inserção de um NID válido:

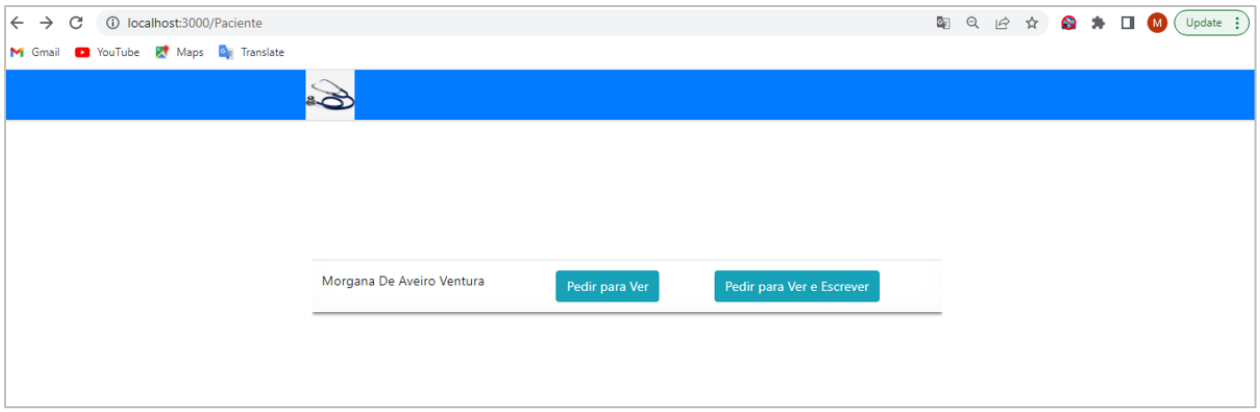


Figura A8- 9: Paciente pesquisado

Após pedir para Ver ou Ver e Escrever é enviado um código de acesso para o paciente, o qual, por sua vez, partilhará com o Profissional de saúde, para que este possa inserir no sistema.

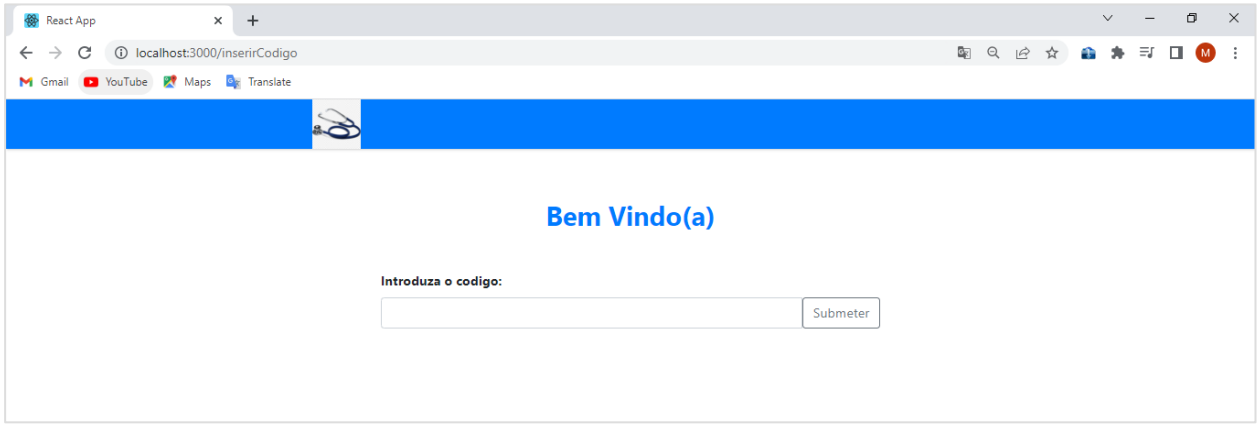


Figura A8- 10: Inserção do código enviado para o paciente

Após inserir o código válido, será exibido o processo clínico, sobre o qual o profissional de saúde realizar as actividades segundo a permissão que tiver requisitado.

Figura A8- 11: Apresentação do processo Clínico do paciente

Anexo 9: Guião de observação

Resultados

Foram observados os procedimentos no arquivo clínico do Hospital Central de Maputo, nas urgências e enfermarias do mesmo Hospital, para apuramento do funcionamento dos processos relacionados a partilha de processos clínicos.

As urgências constituem um dos locais onde os pacientes elegíveis a abertura de processos clínicos são recebidos, tais pacientes foram, na sua maioria, pacientes a serem internados e pacientes enviados com uma guia de transferência.

Segundo o observado, os processos clínicos são criados a nível administrativo, e são actualizados pelos profissionais de saúde, no caso, médicos. São armazenados temporariamente, na enfermaria, os processos clínicos de pacientes ainda em observação (internados), os dos outros vão para o arquivo clínico. Portanto, os processos clínicos no papel ainda não foram descontinuados, apesar de já existerem sistemas que visam digitalizar estes documentos. Alguns pacientes têm os processos clínicos armazenados no sistema, no entanto, a efectivação do uso destes sistemas é ainda um desafio pois estes não se comunicam. Observou-se um cenário de um paciente que teve o seu processo clínico a partir de um sistema vigente no Hospital, a seguir, precisou fazer exames laboratoriais que também foram lançados em um sistema sem nenhuma comunicação com o primeiro (onde está armazenado o processo clínico), as informações colectadas na radiologia também são enviadas a parte para o processo clínico, os sistemas lá presentes não possuem comunicação alguma, tampouco com os sistemas de outras unidades sanitárias, tal como a clinicare.