Proposta para Grupo de Trabalho 2022

GT-SmartMed: Dados Médicos Distribuídos com Controle de Acesso baseado em Atributos através de Contratos Inteligentes

Prof. Dr. Diogo Menezes Ferrazani Mattos

25 de setembro de 2022

1. Título

GT-SmartMed: Dados Médicos Distribuídos com Controle de Acesso baseado em Atributos através de Contratos Inteligentes

2. Coordenador Acadêmico

Coordenador: Diogo Menezes Ferrazani Mattos
Instituição: Universidade Federal Fluminense
TET / PPGEET / TCE
LabGen / MídiaCom

Lattes: http://lattes.cnpq.br/6177045546956476
ResearchGate: https://www.researchgate.net/profile/Diogo-Menezes-4
Google Scholar: https://goo.gl/SBL27U

3. Líder e Assistente(s) de Inovação

Líder: Dianne Scherly Varela de Medeiros
Instituição: Universidade Federal Fluminense
TET / PPGEET / TCE
LabGen/MídiaCom

Lattes: http://lattes.cnpq.br/8119805151400395
ResearchGate: https://www.researchgate.net/profile/Dianne-Medeiros
Google Scholar: https://scholar.google.com/citations?user=aAvUGv0AAAAJ

Assistente: Nicollas Rodrigues de Oliveira
Instituição: Universidade Federal Fluminense
TET / PPGEET / TCE
LabGen / Mídiacom

Lattes: http://lattes.cnpq.br/5122206871931818
ResearchGate: https://www.researchgate.net/profile/Nicollas-Oliveira
Google Scholar: https://scholar.google.com/citations?user=Z7t7FuQAAAA

4. Tópicos de Interesse

Blockchain; Gestão de Identidades; Telessaúde

5. Parcerias e respectivas contrapartidas

Amsterdam University Medical Centers (Amsterdã, Holanda) – O Laboratório MídiaCom desenvolve colaboração com a pesquisadora Silvia Delgado Olabarriaga do Departamento de Epidemiologia, Bioestatística e Bioinformática de Amsterdam University Medical Centers, em Amsterdã, Holanda, inclusive com a participação da exorientada de mestrado do proponente, Marcela de Oliveira Tuler. A colaboração conta com a mobilidade de alunos de graduação para a participação de projetos de pesquisa e desenvolvimento no Amsterdam University Medical Centers. A contrapartida do AMC

é não financeira e consiste no apoio técnico e científico para o desenvolvimento do projeto. Parte da pesquisa que fomenta e embasa o desenvolvimento do produto descrito no projeto foi desenvolvida *a priori* através da parceria entre MídiaCom e AMC. A contrapartida técnica e não financeira do AMC é importante para o compartilhamento de técnicas, requisitos e conhecimentos prévios adquiridos.

Prefeitura Municipal de Niterói (Niterói, RJ) – O Prof. Diogo Mattos coordena um projeto de pesquisa e desenvolvimento de tecnologia através da colaboração entre a Prefeitura Municipal de Niterói e Universidade Federal Fluminense. O projeto prevê a aplicação de recursos no apoio a pesquisas para o desenvolvimento de Tecnologias da Informação e Comunicação que contribuam para o aumento da eficiência das ações do governo municipal. A parceira apresenta como contrapartida não financeira a possibilidade acesso a instituições de saúde municipais para o contato com possíveis usuários do produto, além de ter a facilidade de adoção do produto como *early adopters* ou *beta testes*, dado que já há um acordo de colaboração pré-estabelecido.

Technology Innovation Institute (Abu Dhabi, Emirados Árabes Unidos) – O Laboratório MídiaCom desenvolve colaboração com o pesquisador Martin Andreoni, D.Sc., do *Technology Innovation Institute* (TII – Abu Dhabi), centro de pesquisa global dedicado a expandir as fronteiras do conhecimento. A colaboração com o pesquisador já está bem estabelecida e já foram realizados trabalhos em diversas áreas de tecnologia da informação e comunicação, em especial na área de segurança da informação. Atualmente a colaboração está centrada no desenvolvimento de soluções para segurança em redes de computadores, e na pesquisa e desenvolvimento de soluções baseadas em inteligência artificial, com foco em processamento de dados em fluxo em tempo real. A contrapartida da parceria é não financeira e consiste no apoio técnico e científico para o desenvolvimento de artigos e propostas que viabilizem a entrega do produto mínimo viável deste projeto.

LIP6 (Paris, França) – O Laboratoire d'Informatique de Paris 6 da Université Pierre et Marie Curie (UPMC) é uma instituição parceira deste GT através do professor Guy Pujolle (https://www-phare.lip6.fr/~pujolle/), da professora Thi-Mai-Trang Nguyen (https://www-phare.lip6.fr/~trnguyen/) e do pesquisador do CNRS Marcelo Dias de Amorim (http://www-rp.lip6.fr/~amorim/). Os professores têm participação ativa em diversas pesquisas conjuntas realizadas pelos grupos MídiaCom, Brasil, e o LIP6, França. A contrapartida do laboratório LIP6 é não financeira e consiste no apoio técnico e científico para a realização da pesquisa de base que suporta o projeto.

Ressalta-se que as parcerias elencadas são essencialmente não financeiras e são justificadas por parcerias pré-estabelecidas e consolidadas através de pesquisas realizadas no laboratório LabGen / MídiaCom.

6. Descrição da Proposta

6.1. Sumário Executivo

Nas últimas décadas, as organizações de saúde têm processado cada vez mais dados pessoais; no entanto, garantir que os dados sejam aproveitados apenas para fins legítimos continua sendo um desafio significativo. Políticas de proteção de dados privados, cada vez mais severas, impõem limites para abordagens centralizadas de processamento de dados. As leis de proteção de dados pessoais estipulam direitos aos titulares dos dados e obrigações às instituições que detêm tais dados. Uma lei de

destaque é a *General Data Protection Regulation* (GDPR), vigente em toda a União Europeia (UE), que estabelece diretrizes quanto ao tratamento, por uma pessoa, empresa ou organização, dos dados pessoais de todos na UE [1]. A legislação enfatiza a preocupação em defender os direitos e as liberdades fundamentais dos indivíduos em relação ao manuseio de seus dados e tem inspirado outros países a assumirem compromissos semelhantes, tal como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil[1]. A Lei Geral de Proteção de Dados Pessoais identifica como agentes de tratamento a pessoa natural ou jurídica de direito público ou privado que realiza qualquer operação de tratamento sobre os dados pessoais de outrem. Dentre os deveres estabelecidos a esses agentes estão a coleta de consentimento explícito do titular do dado e a disponibilização de relatórios que identifiquem as operações de tratamento aplicadas ao dado, incluindo a especificação de seu local de armazenamento, mascaramento do dado e medidas de proteção.

O setor da saúde é um exemplo típico de compartilhamento de dados pessoais entre organizações porque os profissionais de saúde de várias organizações precisam processar os dados dos pacientes para realizar suas tarefas. Os dados do paciente são registros médicos eletrônicos (EMR), que contêm dados pessoais sobre o paciente. Os dados do paciente geralmente são distribuídos entre hospitais e clínicas que trataram o paciente pelo menos uma vez ao longo de sua vida. O EMR armazena as informações privadas do paciente sobre diagnóstico e tratamentos. Essas informações privadas são altamente confidenciais, mas são frequentemente compartilhadas entre participantes não confiáveis, como profissionais de saúde, farmácias, familiares de pacientes e outros médicos [2]. O gerenciamento de EMR impõe um desafio para preservar a privacidade enquanto garante a disponibilidade de dados para os pares autorizados. Paralelamente, os registros são mantidos principalmente fragmentados em bancos de dados locais, o que impede que um paciente tenha um prontuário eletrônico consolidado [3]. A tecnologia de Contratos Inteligentes em *blockchain* permite que o EMR seja verificado e registrado por meio de um consenso de pares na rede, garantindo a execução confiável de políticas de acesso aos dados e, portanto, assegurando integridade dos dados, responsabilidade e não repúdio [4]. A *blockchain* impõem o desafio de não limitar o acesso dos participantes às informações armazenadas e não especifica permissões refinadas sobre a privacidade dos usuários.

Este projeto propõe o sistema SmartMed que realiza o controle de acesso a dados médicos através da arquitetura de referência do padrão XACML e contratos inteligentes que implementam componentes do controle de acesso baseado em atributos. A interface entre sistemas de armazenamento de dados médicos e o controle de acesso é realizada através *edge datacenters* de pequeno porte, instalados nas instituições de saúde. A ideia central do projeto é propiciar o armazenamento de dados distribuído em diferentes provedores de armazenamento *off-chain,* em diferentes nuvens, com controle de acesso baseado atributos implementados em contratos inteligentes na *blockchain.*

6.2. Desenvolvimento Tecnológico

Hospitais e clínicas detêm silos de dados que armazenam registros médicos eletrônicos (EMR), que contêm dados pessoais sobre o paciente, fragmentados. Dados pessoais de um mesmo paciente ficam espalhados em diferentes locais de armazenamento, sujeitos às mais diversas políticas de controle de acesso. Contudo, em caso de necessidade de consulta a esses dados, muita das vezes, a integração dos dados é

[1] Disponível em https://www.lgpdbrasil.com.br/.

impossível devido à falta de comunicação e estabelecimento de interfaces bem definidas entre as diferentes organizações de saúde. Assim, cada organização detém apenas

uma parte dos dados. Uma dor frequente nas organizações do setor da saúde é que partes dos dados permanecem inacessíveis, mesmo em emergências, porque estão localizadas em sistemas de informação fora dos limites da organização responsável pelo tratamento. Essa limitação é comumente mitigada usando sistemas de registros médicos compartilhados que exploram soluções em nuvem [5]–[7] ou sistemas de banco de dados distribuídos, como o *InterPlanetary File System* (IPFS)[2]. Esses sistemas compartilhados prometem fornecer a consistência e disponibilidade de dados necessária para fins de saúde. As organizações de saúde atuam então como controladores conjuntos dos dados, definindo e aplicando um controle de acesso estrito entre organizações aos dados dos pacientes. Contudo, um sistema setor de saúde para o gerenciamento de dados bem sucedido deve ser capaz de federar novas organizações através de um sistema de controle de acesso dinâmico e granular para suportar a natureza complexa do compartilhamento de dados entre organizações. Ademais, o sistema de gerenciamento de dados em saúde deve ser capaz de permitir o armazenamento de dados em servidores confiáveis externos, como nuvens de armazenamento e silos de dados em outras organizações. Por exemplo, um médico deve ter acesso aos dados de um paciente durante o tratamento, mesmo que os dados estejam em outra organização. No entanto, o acesso deve ser revogado quando o médico terminar o atendimento. Além disso, todos os registros de acesso devem estar disponíveis para o processo de auditoria e conformidade regulatória.

O modelo de controle de acesso baseado em atributos (*Attribute-Based Access Control* - ABAC) oferece uma abordagem de controle de acesso dinâmica e refinada para proteger dados pessoais [8]. O modelo ABAC define políticas como combinações de regras e atributos que podem ser tão granulares quanto necessário. O ABAC também utiliza expressão de contexto e atributos contextuais, o que confere dinamicidade à avaliação da política. Assim, ABAC define não apenas “por que” e “como”, mas também “por quem”, “quando” e “onde” os dados pessoais podem ser processados. Uma desvantagem dos sistemas atuais que usam o modelo ABAC é que eles geralmente delegam o gerenciamento do controle de acesso ao administrador do sistema de armazenamento de dados centralizado, em que políticas são definidas, gerenciadas, avaliadas e aplicadas. Dessa forma, os controladores e titulares de dados devem confiar que o administrador do sistema de armazenamento seguirá as políticas definidas e não permitirá qualquer processamento de dados pessoais que não cumpram as políticas.

Em relação à transparência, os controladores de dados também dependem dos sistemas de armazenamento de dados para manter e divulgar registros sobre a atividade de processamento de dados pessoais. Recentemente, os conceitos de *blockchain* e contratos inteligentes (*Smart Contracts*) foram propostos para facilitar a transparência sobre o controle de acesso a dados [9]–[11]. Nessas propostas, o processamento de dados é registrado como transações na *blockchain*, que são imutáveis e transparentes para auditoria. No entanto, nenhuma das propostas considera a complexidade e a dinamicidade necessárias para o compartilhamento de dados entre organizações de saúde. Na maioria das propostas, o “proprietário dos dados” define as políticas de controle de acesso, mas o “proprietário dos dados” dos dados do paciente é um papel pouco claro [12] e não é definido na GDPR ou na LGPD. Além disso, depender dos pacientes para definir políticas de controle de acesso ou assumir que os participantes

[2] Disponível em https://ipfs.tech/.

tenham conhecimento técnico para usar sistemas complexos não são hipóteses realistas.

A comunicação entre as partes interessadas na área da saúde por meio de APIs (*Application Programming Interfaces*), denominada integração *Business to Business* (B2B), é essencial para permitir a unificação dos registros médicos. É obrigatório padronizar as interfaces para facilitar a comunicação entre as empresas. A padronização da integração B2B se concentra em três pilares: o formato dos dados, o processo de negócios e o protocolo de comunicação [13], [14]. A tecnologia *blockchain* satisfaz esses pilares. A *blockchain* define um único formato de dados em todos os nós da rede par-a-par e, portanto, todos os participantes seguem o padrão. Consequentemente, o uso do *blockchain* reduz os custos de integração. Os sistemas de saúde baseados em *blockchain* são estruturas de dados altamente distribuídas comumente propostas para armazenar, compartilhar e consultar EMR [15].

Este projeto concentra-se na exploração de elementos de computação em borda associados a contratos inteligentes, na tecnologia *blockchain*, por meio do modelo ABAC para controle de acesso dinâmico de dados pessoais nas organizações. Assim, a proposta visa superar os seguintes desafios: (i) as organizações de saúde devem concordar e cumprir as políticas comuns de controle de acesso para processamento de dados de pacientes como controladores conjuntos de dados; (ii) o sistema de controle de acesso deve garantir uma finalidade válida para o processamento de dados; (iii) as decisões políticas e sua aplicação não devem depender de uma parte confiável centralizada; (iv) os registros de atividade de acesso a dados devem ser transparentes e auditáveis; e (v) o sistema deve ser transparente e fácil de usar para o usuário final.

Para atender aos desafios elencados, o projeto foca no desenvolvimento de uma tecnologia de controle de acesso baseado em contratos inteligentes associada à implementação de *edge datancenters* de pequeno porte nas organizações de saúde. Cada *edge datacenter* age como um nó da *blockchain* subjacente ao sistema e realiza o escalonamento do acesso aos dados médicos provenientes de diversas fontes. Ressalta-se que o consumidor de dados de saúde, por vezes, representa médicos, farmacêuticos, enfermeiros e técnicos, além de outras partes envolvidas no setor da saúde, que detém pouco ou nenhum conhecimento quanto à utilização de sistemas de computação complexos. Assim, a introdução de um controle de acesso elaborado e complexo pode tornar-se uma dor para o consumidor de dados. Nesse sentido, o projeto define como meta tornar o controle de acesso transparente e, para tanto, os *edge datacenters* exercem a função de *proxy* entre o usuário e as diversas fontes de dados, para que o acesso aos dados seja transparente para o consumidor, ao mesmo tempo em que as políticas de acesso são validadas e registradas.

Quando um contrato inteligente é implantado, o proprietário do contrato transmite uma transação que transporta a carga útil como um código vinculado a um endereço público. Depois que essa transação é extraída, todos os nós armazenam uma réplica do contrato inteligente [16]. Para executar uma função de contrato inteligente, o 'nó emissor' transmite uma transação para a rede com o endereço público do contrato inteligente, carregando os argumentos de entrada da função dentro da carga útil da transação. O nó emissor espera então que a transação seja validada e extraída em um bloco. Enquanto isso, do ponto de vista de todos os outros nós, a transação ainda não aconteceu. Uma vez que a transação é extraída e transmitida para a rede, a transação é considerada executada. O nó minerador envia um 'recibo de transação' para o

endereço do nó emissor, confirmando que a transação foi minerada. Portanto, o 'evento' é emitido nesse ponto. Isso significa que o nó emissor executa a função de contrato inteligente com os argumentos de entrada da transação e emite o evento que o *frontend* do usuário, implantado no *edge datacenter*, pode processar. Embora a função seja executada localmente, qualquer nó pode verificar as transações de eventos que executam os contratos inteligentes com os mesmos argumentos inseridos. Uma função de contrato inteligente também pode executar funções de outros contratos como um processo. Para enviar transações e executar funções, pode ser necessário que o remetente pague uma taxa. Na *Ethereum*, a taxa é chamada de 'gás'. Na *blockchain* baseada em *Ethereum Virtual Machine* (EVM), o gás é uma excelente maneira de avaliar a complexidade dos contratos inteligentes, pois o uso do gás aumenta com a complexidade das transações. O estado global dos contratos inteligentes pode ser visto como uma máquina virtual executando todo o código no *blockchain*.

O sistema SmartMed implanta o conceito de computação em borda ao trazer para as premissas dos usuários parte do recurso de computação (*edge datacenter*), a fim de reduzir a latência da comunicação e agir como *proxy* para a execução do controle de acesso através de contratos inteligentes. O SmartMed oferece suporte a diversos nós de armazenamento descentralizados através dos *edge datacenters*. A descentralização no gerenciamento de documentos e a não dependência de um único participante detentor de todos os dados é uma das principais motivações do SmartMed. Na área da saúde, cada organização, hospital ou clínica, tem potencialmente seu próprio armazenamento. Portanto, a vantagem de usar a *blockchain* (privada) para gerenciamento de documentos é ter um mecanismo de controle de acesso descentralizado para proteger esses dados distribuídos, seguindo as políticas acordadas em consenso com todas as organizações que fazem parte da rede *blockchain*. Outra vantagem é a confiança e a reputação construídas entre a organização de saúde com base na transparência das políticas do usuário e registros coletados sobre o processamento de dados disponível para auditoria e conformidade com a LGPD ou a GDPR.

Destaca-se que os *edge datacenters* representam nós de computação em borda. Esses nós consistem de um aglomerado de pequeno porte que é instalado nas instituições federadas ao sistema SmartMed e, assim, intermedia o acesso aos dados e documentos armazenados na nuvem ou em silos de dados nas instituições participantes. Para um usuário interno a uma instituição participante, o portal SmartMed é apresentado como uma aplicação web em execução no *edge datacenter*. Contudo, o *edge datacenter* executa o cliente da *blockchain* responsável por realizar o controle de acesso distribuído e age como *proxy* para a recuperação dos documentos armazenados nos servidores de armazenamento distribuídos, seja na nuvem ou em outros *edge datacenters* de instituições federadas.

O SmartMed é baseado na rede *blockchain Ethereum*, implantada como uma rede privada, contratos inteligentes e na computação em borda. Os nós da rede usam os contratos inteligentes para definir políticas de controle de acesso, solicitar permissão de acesso e verificar se a solicitação é permitida ou não. Quando o acesso é garantido, os nós da rede agem como *proxy* para recuperar os documentos solicitados em um dos servidores de armazenamento participantes da rede.

Os *edge datacenters* fornecem os meios para que os usuários sejam autenticados, pesquisem os identificadores de recursos e solicitem o recurso armazenado fora da cadeia (*off-chain*). O usuário acessa os recursos do SmartMed como uma aplicação *web*

através de qualquer dispositivo que tenha acesso ao *edge datacenter* e procede com a autenticação necessária em cada instituição.

A rede é composta por nós controlador, armazenamento e processador de dados, que possuem diferentes funções de acordo com sua função em relação à LGPD ou à GDPR. Os contratos inteligentes executados nos nós oferecem funções para gerenciar a rede privada e fornecer controle de acesso a um recurso fora da cadeia. Definem-se quatro contratos inteligentes que seguem o modelo XACML*: Enforcement Smart Contract, Decision Smart Contract, Policies Smart Contract* e *Information Smart Contract*. Os contratos serão desenvolvidos no contexto do projeto.

A rede *blockchain* proposta é privada e com permissão, na qual os nós são adicionados e removidos da rede e possuem funções e permissões. Um nó é um dispositivo ou servidor conectado de onde o usuário pode enviar transações, executar contratos inteligentes e armazenar a estrutura de dados da *blockchain*. Um nó também executa um aplicativo que implementa a camada de lógica de negócios. Cada nó possui um par de chaves assimétricas usadas para gerar seu endereço e assinatura digital.

Assim, o desenvolvimento tecnológico do projeto foca na implantação da rede *blockchain* privada baseada na plataforma *Ethereum* entre os nós *edge datacenters* a serem desenvolvidos. Ressalta-se que os *edge datacenters* intermediam a comunicação e realizam o controle de acesso de usuários locais de organizações de saúda a dados e documentos armazenados em nuvens de armazenamento distintas. Os processadores de dados executam os contratos inteligentes de controle de acesso localmente em seus *edge datacenters* sem depender de uma parte central. Cada função executada nos contratos inteligentes gera uma transação auditável publicada na *blockchain*. Portanto, qualquer nó da rede pode sempre pesquisar as solicitações de acesso que foram realizadas para determinados dados, os valores dos atributos naquele momento, a política aplicada durante a avaliação de acesso e a decisão resultante.

6.3. Modelo de Negócios

A metodologia Canvas foi utilizada para definir os principais pontos que compõem o modelo de negócio a seguir.

Segmento de Clientes: O segmento de clientes compreende o conjunto de clientes pessoas físicas ou empresas para o qual se pretende vender o produto desenvolvido e o serviço de operação associado. Esse bloco tem grande importância, uma vez que influencia de forma significativa os outros blocos do modelo, principalmente a proposta de valor. O segmento de clientes é bastante evidente no projeto. Contudo, há a necessidade de executar a validação da hipótese inicial acerca do seguimento de clientes. A primeira hipótese sobre o público-alvo é que é composto por três segmentos de clientes: (i) hospitais universitários, (ii) ambulatórios e clínicas especializados e (iii) consultórios médicos. A validação do público alvo será realizada durante a execução do projeto. Ressalta-se que os clientes do produto são as organizações de saúde, enquanto os usuários são funcionários da organização e também pacientes e outros *stakeholders.*

Proposta de Valor: O conceito de proposta de valor é uma visão geral do pacote de produtos e serviços de uma empresa que são valiosos para os clientes. A proposta deve atender a três questões fundamentais: como resolver a dor do cliente, quais benefícios apresenta e quais são os diferenciais de mercado em relação aos concorrentes. A proposta de valor foca na integração de diferentes fontes de dados médicas e no

gerenciamento eficiente do controle de acesso sobre os dados dos pacientes. As dores identificadas são: (i) a dispersão de dados de pacientes em diferentes servidores de armazenamento; (ii) a ausência de um formato pré-estabelecido para a comunicação de dados entre diferentes servidores de armazenamento; (iii) a ausência de um sistema de controle de acesso descentralizado capaz de atender diferentes organizações de saúde ao passo que não dependa de uma terceira parte confiável; e (iv) a consolidação dos dados de pacientes através de uma interface simples, intuitiva e que não seja impeditiva para usuários sem conhecimentos profundos da área de tecnologia. Dessa forma, o produto é adequado para atender a essas necessidades, viabilizando a resolução das dores identificadas.

Canais: Os Canais são como o negócio alcança o cliente, a fim de entregar a proposta de valor. Assim, o canal é o ponto de conexão entre o negócio e os segmentos de cliente. O canal deve oferecer meios para entregar o produto e os serviços ao cliente, ajudar o cliente a perceber a proposta de valor do negócio, viabilizar a compra dos produtos e serviços, entregar a proposta de valor ao cliente e viabilizar o relacionamento pós-venda. Os principais canais a serem explorados são através de contatos em mídias sociais e através de parcerias com instituições de saúde em universidades públicas. As estratégias de relacionamento com o cliente visam suprir questões relacionadas às expectativas de cada segmento de cliente sobre o relacionamento com a empresa, qual o tipo de relacionamento existente, bem como, qual o custo atrelado à manutenção desse relacionamento. Têm-se as seguintes abordagens: (i) Canais Virtuais; (ii) Redes sociais; e (iii) Co-criação.

Atividades Chave: As atividades chave são o conjunto de atividades cuja execução é essencial para manter a operação do serviço e do produto oferecidos. Essas atividades devem ser praticadas para possibilitar a execução e manutenção do modelo de negócios. Nesse contexto, as atividades chave para o modelo de negócios do produto são: (i) Desenvolvimento de software; (ii) Análise de marketing; (iii) Análise econômica; (iv) Implantação do produto; e (v) Capacitação operacional do cliente.

Parceiros Chave: A relação com entidades como RNP, CNPq, CAPES e FINEP pode ser firmada através de *joint-venture*, uma colaboração para fins comerciais e/ou tecnológicos. Além desses parceiros, serão estabelecidas e fortificadas parcerias com hospitais e clínicas universitários.

Estrutura de Custos: A Estrutura de Custos reúne os custos mais importantes para a operação do negócio. A estruturação dos custos envolvidos na implementação do projeto é dividida em: (i) Custos Fixos que englobam a manutenção dos recursos humanos, a manutenção da infraestrutura física, estrutura de atendimento ao cliente; (ii) Custos Variáveis que incluem os investimentos em marketing; e (iii) Economia de Escala que consiste em reduzir o custo de produção por unidade quando o volume cresce.

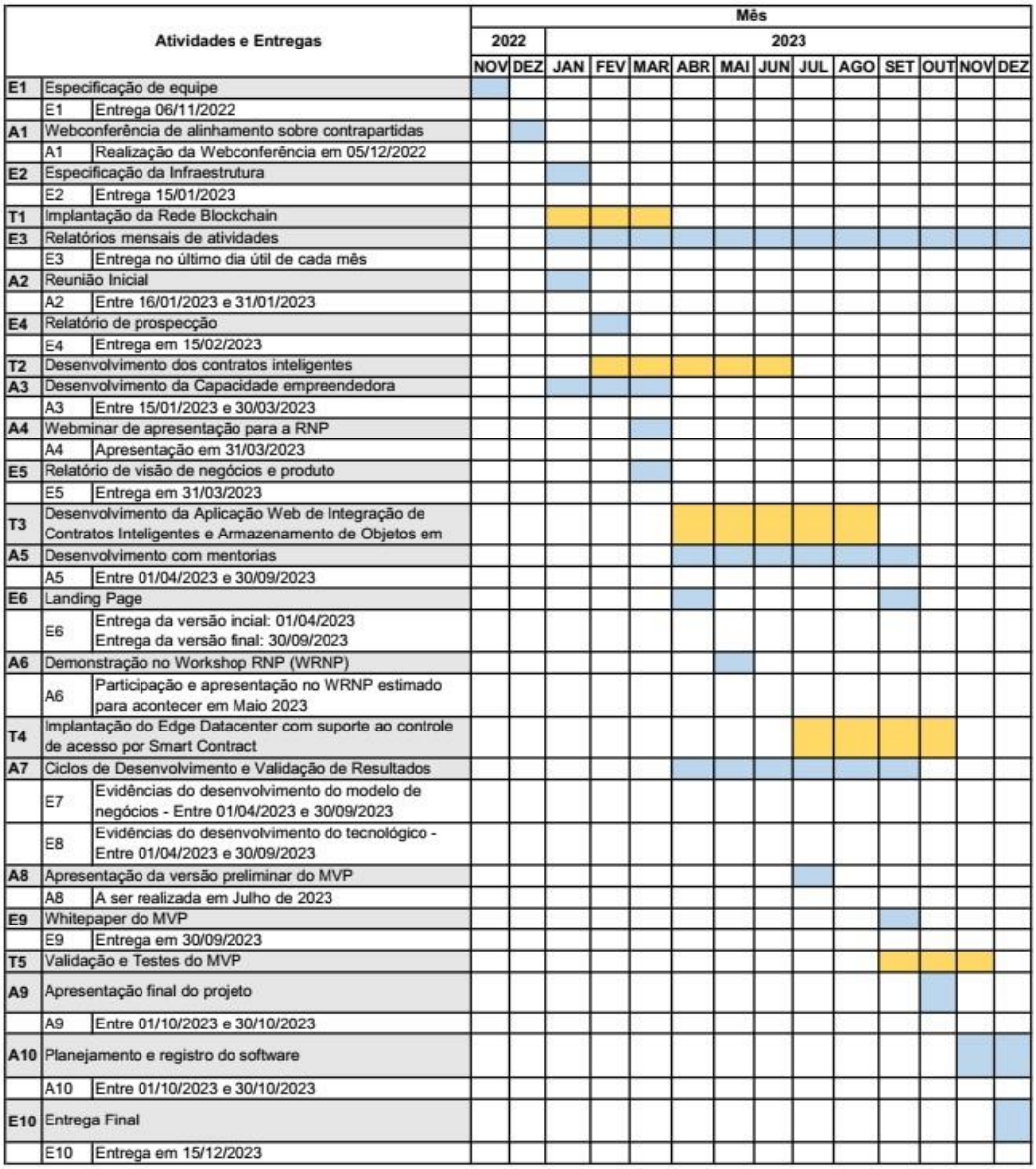
Fluxo de Receita: Sendo fundamental para a sobrevivência a longo prazo de um negócio, o fluxo de receitas mede a capacidade de o negócio traduzir o valor que oferece a seus clientes em dinheiro e fluxos de receita de entrada. Apresentando volatilidade, previsibilidade, risco e retorno, os diferentes fluxos de receita possíveis de uma empresa podem também admitir mecanismos de precificação distintos. O fluxo de receita será composto por (i) Monetização por Licenciamento de Funcionalidade, pois pretende-se adotar um modelo de monetização recorrente que se adeque às necessidades de cada cliente; (ii) manutenção, atualização e adaptação da solução às necessidades do cliente pode ser provida como um serviço recorrente, permitindo a monetização previsível e tornando o serviço de manutenção e atualização do produto um ativo para o modelo de

negócios; e (iii) Intermediação de vendas entre desenvolvedores de funcionalidades e clientes que desejam funcionalidades personalizadas.

7. Ambiente de validação da solução proposta e documentação dos aprendizados

O ambiente de desenvolvimento e testes da proposta será o Laboratório de Ensino e Pesquisa em Redes de Nova Geração (LabGen/UFF). O LabGen conta com uma infraestrutura de nuvem privada capaz de fornecer os recursos necessários para o teste da proposta, assim como permitir o desenvolvimento do produto mínimo viável. O ambiente disponível no LabGen conta com uma infraestrutura de rede *Gigabit Ethernet* interconectando mais de dez servidores de serviços em nuvem sobre a plataforma *OpenStack*. A validação do produto mínimo viável será realizada com possíveis clientes através da instalação de *edge datacenters* em instituições parceiras como o Hospital Universitário Antônio Pedro (UFF) para a validação inicial com o público alvo (usuários do setor de saúde), mas também com a prospecção de possíveis *early adopters* dentro e fora do sistema RNP. O produto mínimo viável é composto por um servidor representando o *edge datacenter*, conectando-se à nuvem privada provida pela infraestrutura hospedada no LabGen e participando de uma rede privada da *blockchain Ethereum*, configurada entre os nós participantes. Os contratos inteligentes são escritos em *Solidity* e instanciados na rede privada. Essa abordagem de teste e validação em rede privada reduz os custos de desenvolvimento, já que não requer o pagamento de ‘gás’, ao passo em que permite a validação do conceito e a verificação da aceitação do produto por parte dos usuários. Paralelamente, o acompanhamento do projeto e a documentação dos aprendizados serão realizados através da plataforma de comunicação e colaboração da RNP, Integra RNP.

8. Cronograma de marcos



9. Recursos financeiros

9.1. Pessoal

9.1.1. Equipe alocada com recursos do edital

Nome	Função	Tipo	Data início (d/m/a)	Data fim (d/m/a)	Alocação de horas por mês	Valor em R$ Mensal	Total em R$ Anual
Diogo Menezes Ferrazani Mattos	Coordenador geral	Grupo de pesquisa	01/01/2023	31/12/2023	20		
Dianne Scherly Varela de Medeiros	Líder de Inovação	Grupo de pesquisa	01/01/2023	31/12/2023	20		
Nicollas Rodrigues de Oliveira	Assistente de Inovação	Grupo de pesquisa	01/01/2023	31/12/2023	50		
Guilherme Nunes Nasseh Barbosa	Assistente de desenv. 1	Grupo de pesquisa	01/01/2023	31/12/2023	40		

Nathalia Cuciniello dos Santos	Assistente de desenv. 2	Grupo de pesquisa	01/01/2023	31/12/2023	60	[redacted]
a definir	Graduando	Grupo de pesquisa	01/01/2023	31/12/2023	50	
a definir	Graduando	Grupo de pesquisa	01/03/2023	31/12/2023	50	
[redacted]						

9.2. Infraestrutura

9.2.1. Recursos de Nuvem

O projeto não prevê o uso de recursos de nuvem, pois o laboratório LabGen/MídiaCom conta com uma infraestrutura de nuvem privada que será usada como contrapartida no desenvolvimento, teste e validação do Produto Mínimo Viável (MVP).

9.2.2. Equipamentos, Periféricos e Garantias

Os equipamentos solicitados a seguir são adequados e suficientes para as atividades de desenvolvimento, teste e validação do projeto. Os notebooks são necessários e suficientes para o desenvolvimento e demonstrações. O Desktop exercerá a função de nó do *edge datacenter.*

Modelo	**Descrição**	**Instituição de Destino**	**Qtd.**	**Valor Unitário em R$**	**Subtotal em R$ estimado**
N2	Notebook N2 - i7 - 512GB SSD - 16GB Notebook para o desenvolvimento e teste de códigos	UFF	2	R$ 7,519.95	R$ 15,039.90
N3	Notebook N3 - i7 - 1TB SSD - 32G Notebook para demonstrações como *edge datacenter*	UFF	1	R$ 5,920.55	R$ 5,920.55
D1	Desktop D1 - i5 - 256GB SSD - 16GB Desktop a ser utilizado como implantação de um *edge datacenter* de validação.	UFF	1	R$ 3,988.80	R$ 3,988.80
				Total	R$ 24,949.25

10. Referências

[1] Parlamento Europeu e Conselho da União Européia, “Regulamento (UE) 2016/679”. 2016.

[2] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, e F. Wang, “Secure and trustable electronic medical records sharing using blockchain”, in *AMIA ’17*, 2017, vol. 2017, p. 650–659.

[3] M. Mettler, “Blockchain technology in healthcare: The revolution starts here”, in *Healthcom ’16*, 2016, p. 1–3.

[4] K. Christidis e M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things”, *IEEE Access*, vol. 4, p. 2292–2303, 2016.

[5] A. Ullah, H. Dagdeviren, R. C. Ariyattu, J. DesLauriers, T. Kiss, e J. Bowden, “MiCADO-Edge: Towards an Application-level Orchestrator for the Cloud-to-Edge Computing Continuum”, *J. Grid Comput.*, vol. 19, nº 4, p. 1–28, 2021.

[6] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hübsch, e I. Paraskakis, “PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services”, *J. Grid Comput.*, vol. 15, p. 219–234, 2017.

[7] Y. Verginadis *et al.*, “Context-aware Policy Enforcement for PaaS-enabled Access Control”, *IEEE Trans. Cloud Comput.*, vol. 10, nº 1, p. 276–291, 2019.

[8] E. Psarra, Y. Verginadis, I. Patiniotakis, D. Apostolou, e G. Mentzas, “Securing Access to Healthcare Data with Context-aware Policies”, in *11th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 2020, p. 1–6.

[9] S. Rouhani, R. Belchior, R. S. Cruz, e R. Deters, “Distributed attribute-based access control system using permissioned blockchain”, *World Wide Web*, vol. 24, nº 5, p. 1617–1644, 2021.

[10] D. D. F. Maesa, P. Mori, e L. Ricci, “A blockchain based approach for the definition of auditable access control systems”, *Comput. Secur.*, vol. 84, p. 93–119, 2019, [Online]. Available at: https://doi.org/10.1016/j.cose.2019.03.016.

[11] A. Ghorbel, M. Ghorbel, e M. Jmaiel, “Accountable privacy preserving attributebased access control for cloud services enforced using blockchain”, *Int. J. Inf. Secur.*, p. 1–20, 2021.

[12] A. Ballantyne, “How should we think about clinical data ownership?”, *J. Med. Ethics*, vol. 46, nº 5, p. 289–294, 2020, doi: 10.1136/medethics-2018-105340.

[13] M. T. de Oliveira *et al.*, “Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications”, in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, p. 1–6, doi: 10.1109/ICC.2019.8761307.

[14] M. Merz, “Potential of the Blockchain Technology in Energy Trading”, in *Blockchain Technology: An Introduction for Business and IT Managers*, D. Burgwinkel, Org. Alemanha: DE GRUYTER, 2016, p. 51–97.

[15] X. Zhang e S. Poslad, “Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR)”, in *ICC ’18*, 2018, p. 1–6, doi: 10.1109/ICC.2018.8422883.

[16] K. Christidis e M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things”, *IEEE Access*, vol. 4, p. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.