



# **Uma proposta de integração de sistemas da Secretaria do Patrimônio da União ao blockchain para incentivo à transparência de processos: resultados de uma pesquisa em andamento**

**Iago Fernandes, Pamella Soares, Raphael Saraiva, Bruno Vicente, Alexandre Sertã,  
Ricardo Loiola, Allysson Araújo, Jerffeson Souza**



UNIVERSIDADE  
ESTADUAL DO CEARÁ



Programa de Pós-Graduação  
em Ciência da Computação

# Agenda

1. Introdução
2. Fundamentação Teórica
3. Trabalhos Relacionados
4. Processos Metodológicos
5. Solução Proposta
6. Avaliação Técnica
7. Avaliação Social
8. Ameaças à Validade
9. Considerações Finais

# 01. Introdução

# INTRODUÇÃO

## PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)

É uma estrutura para manutenção da informação eletrônica sobre a saúde do indivíduo e os cuidados recebidos durante sua vida.

[Massad et al. 2003]

- ❖ Armazenamento
- ❖ Comunicação
- ❖ Garantir a continuidade do cuidado ao paciente
- ❖ Interoperabilidade
- ❖ Privacidade [Ricarte et al. 2017]

### Lei Geral de Proteção de Dados

Prover acesso a dados sensíveis de modo seguro e que preserve a privacidade e anonimidade dos pacientes [da Conceição et al. 2018].

Massad, E., Marin, H. d. F., and Azevedo Neto, R. S. d. (2003). O prontuário eletrônico do paciente na assistência, informação e conhecimento médico. Pages 1-202  
Ricarte, I. L. (2019). Sistemas nacionais de prontuários eletrônicos frente à privacidade de dados. *E-prints in library information science*. Disponível em: <http://eprints.rclis.org/33929/>.  
da Conceição, A. F., da Silva, F. S. C., Rocha, V., Locoro, A., and Barguil, J. M. (2018). Eletronic health records using blockchain technology. *arXiv preprint arXiv:1804.10078*.

# INTRODUÇÃO

## BLOCKCHAIN

A tecnologia blockchain se demonstra promissora por sua viabilização de que **partes anônimas** e que **não confiam entre si** formem uma rede que armazena informações **confiáveis**, garantindo a **auditabilidade, disponibilidade e integridade** das transações armazenadas.

*Um banco de dados distribuído, protegido por criptografia e governado por um mecanismo de consenso, ou seja, um registro de eventos transparente, seguro e resiliente.*

[Beck et al. 2017]

# INTRODUÇÃO

## BLOCKCHAIN E SISTEMAS COLABORATIVOS

As **pessoas**, as **instituições** e os **diferentes setores**, colaboram entre si para a solução de diferentes problemas, sendo possível a **criação dos atuais espaços sociais** para o trabalho por meio de **sistemas colaborativos**.



O uso de tecnologias como blockchain pode **transformar** diferentes dimensões de um **contexto real da sociedade**. [Prinz 2018]

A adoção de blockchain no contexto de PEP tem sido avaliada apenas sob o ponto de vista técnico, denotando, assim, uma **escassez de estudos que buscam compreender os relevantes efeitos da tecnologia sobre as pessoas, de forma individual e coletiva**.

Prinz, W. (2018). Blockchain and cscw—shall we care? In *Proceedings of 16th European Conference on Computer-Supported Cooperative Work—Exploratory Papers*. European Society for Socially Embedded Technologies (EUSSET)

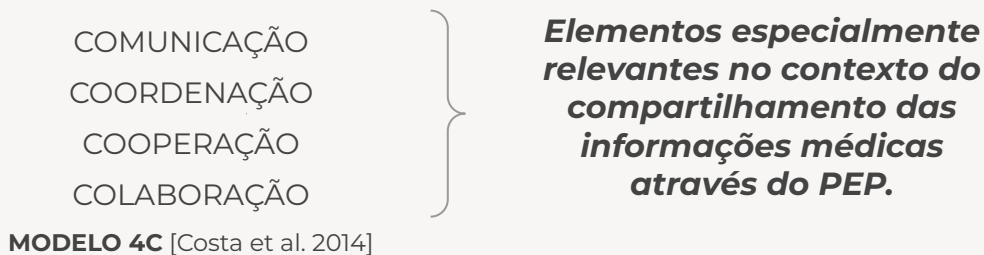
# INTRODUÇÃO

## ABORDAGEM SOCIOCÉNICA

Em suma, a abordagem sociotécnica além de se preocupar com o **viés tecnológico**, considera também a análise de **como os usuários são impactados**. [Bassan de Moraes et al. 2019].



Com esta abordagem pode-se concretizar análises sobre o atendimento dos pilares:



Bassan de Moraes, C. R., Valentim, M. L., and Pinheiro de Souza, L. P. (2019). Recursos informacionais para a construção do conhecimento em empresas de software: Abordagem sistêmica. *Brazilian Journal of Information Science*, 13(3)

Costa, A. P., Loureiro, M. J., and Reis, L. P. (2014). Do modelo 3c de colaboração ao modelo 4c: Modelode análise de processos de desenvolvimento de software educativo. *Revista Lusófona de Educação*, (27):181–200.

# OBJETIVO GERAL



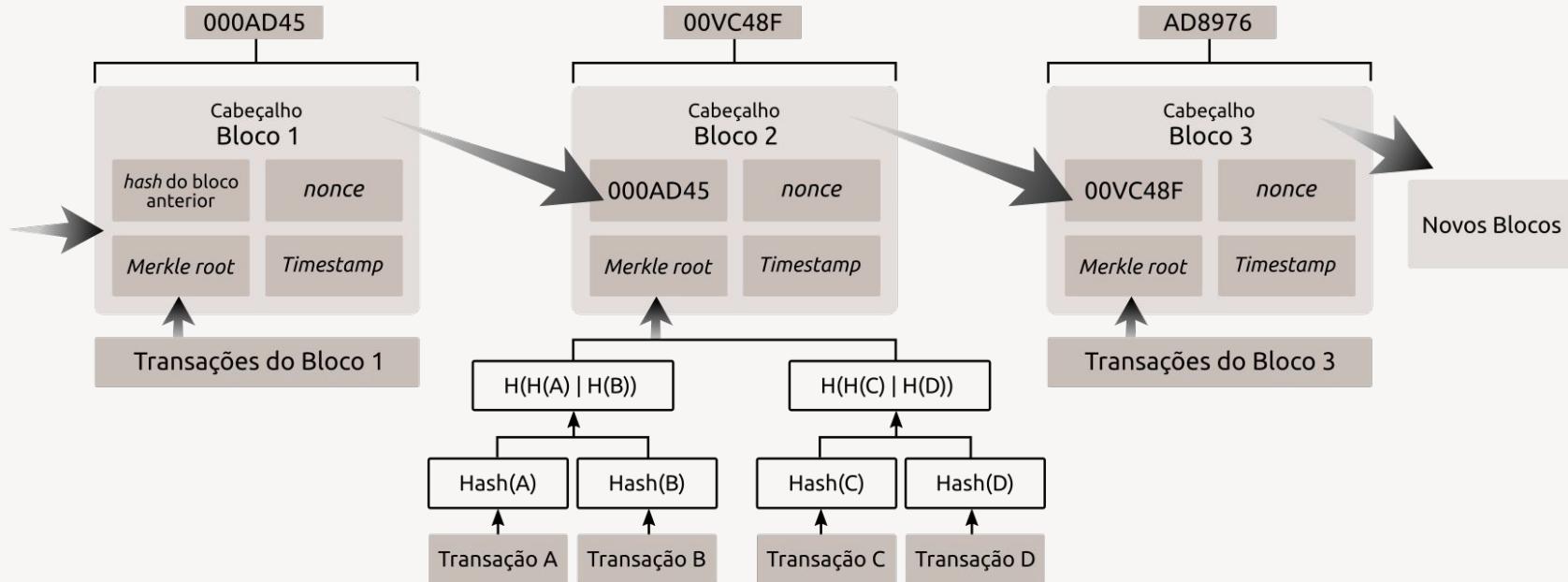
Propor e avaliar, através de uma **metodologia sociotécnica** multi-método, uma **arquitetura de software** para integração de **blockchain** no contexto de **Prontuário Eletrônico do Paciente** para permitir o **controle de acesso e compartilhamento de registros médicos** entre diferentes entidades de saúde.

# OBJETIVOS ESPECÍFICOS

- ❖ Propor uma arquitetura para um Prontuário Eletrônico do Paciente baseada em blockchain sob o contexto brasileiro;
- ❖ Avaliar a conformidade de tal solução frente aos requisitos, normas e resoluções vigentes definidos pela certificação da Sociedade Brasileira de Informática em Saúde e Lei Geral de Proteção de Dados;
- ❖ Implementar uma Prova de Conceito (PoC, do inglês Proof-of-Concept) baseada na arquitetura modelada;
- ❖ Implementar técnicas de armazenamento off-chain a fim de amenizar os desafios de escalabilidade;
- ❖ Realizar uma avaliação de desempenho da arquitetura proposta conforme as métricas utilizadas em sistemas blockchain;
- ❖ Realizar uma avaliação social através de Grupo Focal (GF) a fim de entender como a solução pode contribuir em questões colaborativas.

## 02. Fundamentação Teórica

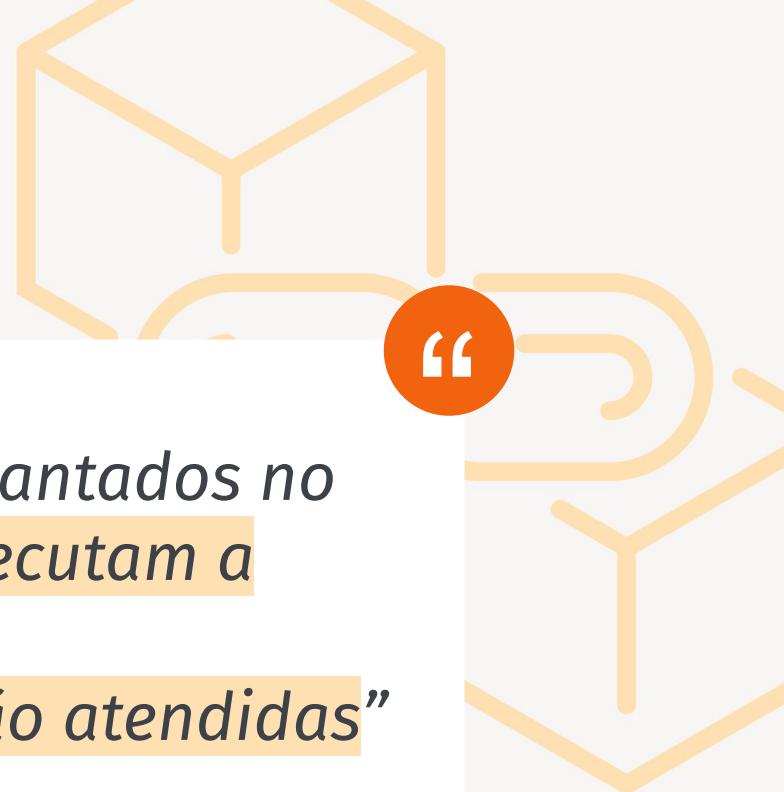
# BLOCKCHAIN



- Esta estrutura proporciona a integridade e imutabilidade das informações, visto que qualquer modificação invalidaria a cadeia de blocos.

# CONTRATOS INTELIGENTES

“Consistem em **scripts** implantados no topo da blockchain que **executam a lógica de negócios** quando determinadas **condições são atendidas**”



# DECENTRALIZED APPLICATIONS (DAPPS)

“Os aplicativos descentralizados têm como uma de suas principais características o fato de que não há um único servidor ou entidade controlando-os como em um modelo cliente-servidor. Além disso, esses têm como base o uso de blockchain como armazenamento e processamento, através da implementação de contratos inteligentes”

# PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)

- ❖ O prontuário é um documento **único composto por diversas informações, sinais e imagens registradas**.
- ❖ Permite a **comunicação entre membros da equipe multiprofissional** de saúde, que garante continuidade da assistência ao indivíduo.
- ❖ Fast Healthcare Interoperability Resources (FHIR) - Padrão que descreve **formatos e elementos de dados**, denominados de “recursos” e uma Application Programming Interface (API) para troca de registros eletrônicos de saúde [BENSON; GRIEVE, 2021].

# COMPUTER SUPPORTED COOPERATIVE WORK (CSCW)

- ❖ Visa compreender a função da tecnologia em um ambiente de trabalho e, especialmente, **como as pessoas lidam de forma colaborativa na construção de tecnologias;**
- ❖ CSCW possibilita uma gama de teorias e modelos de colaboração que podem ser utilizadas para fornecer uma visão sobre como e porque as pessoas trabalham em grupo, como o **Modelo 3C e 4C de Colaboração.**

COMUNICAÇÃO

COORDENAÇÃO

COOPERAÇÃO

COLABORAÇÃO

## 03. Trabalhos Relacionados

# TRABALHOS RELACIONADOS

- ❖ Socio-technical considerations for the use of blockchain technology in healthcare (Wong et al., 2018);
- ❖ The socio-technical assemblages of blockchain system: How blockchains are framed and how the framing reflects societal contexts (Shin e Ibahrine, 2020);
- ❖ Blockchain security as “people security”: Applying sociotechnical security to blockchain technology (Nabben, 2021).
- ❖ Electronic health records using blockchain technology (Conceição et al., 2018);
- ❖ Unificação de dados de saúde através do uso de blockchain e smart contracts (Agostinho et al., 2019);
- ❖ Blockchain para gerenciamento de prontuários (Viana et al., 2020).
- ❖ Medblock: efficient and secure medical data sharing via blockchain (Fan et al., 2018);
- ❖ Clinicappchain: a low-cost blockchain hyperledger solution for healthcare (Fuentes et al., 2019);
- ❖ FHIRchain: applying blockchain to securely and scalably share clinical data (Zhang et al., 2020).

# TRABALHOS RELACIONADOS

- ❖ Lacuna quanto ao entendimento de **aspectos colaborativos**.
- ❖ Soluções nacionais não sugerem **adequação aos requisitos** estabelecidos por autoridades nacionais.
- ❖ Não apresentaram os padrões de **interoperabilidade** pelos quais se basearam.
- ❖ Não discutem questões e estratégias para amenizar o desafio da **escalabilidade**.

# 04. Processos Metodológicos

# CARACTERIZAÇÃO DA PESQUISA

A natureza metodológica desta proposta é classificada como uma abordagem **quali-quantitativa** do tipo **exploratória** apoiada em **Design Science Research (DSR)** [Vaishnavi e Kuechler (2004)].



# DESIGN DAS AVALIAÇÕES

## AVALIAÇÃO TÉCNICA

### AVALIAÇÃO DE ADERÊNCIA DOS REQUISITOS ADVINDOS DE NORMAS TÉCNICAS (SBIS E LGPD)

- ❖ Análise de requisitos técnicos frente às funcionalidades do artefato proposto;
- ❖ Identificação dos possíveis requisitos impactados pela adoção de blockchain evidenciando, com base numa análise de dados empíricos secundários, as **potencialidades e desafios** associados.

### ANÁLISE DE DOCUMENTAL [BOWEN et al., 2009]

1. Reunir os textos relevantes;
2. Desenvolver um esquema de organização e gestão;
3. Fazer resumos dos originais para anotação;
4. Avaliar a autenticidade dos documentos;
5. Explorar a organização e vieses dos documentos;
6. Explorar informações básicas;
7. Fazer perguntas sobre o documento e, finalmente;
8. Explorar o conteúdo.

# DESIGN DAS AVALIAÇÕES

## AVALIAÇÃO TÉCNICA

### AVALIAÇÃO DE DESEMPENHO

Análise de desempenho demonstra-se como um **requisito de qualidade** necessário nos sistemas de forma a impactar diretamente na **experiência do usuário**.

### MÉTRICAS ANALISADAS

- ❖ Tempo de **publicação** dos dados inseridos e;
- ❖ Tempo de **busca** dos dados pesquisados.

# DESIGN DAS AVALIAÇÕES

## AVALIAÇÃO SOCIAL

- ❖ Entendimento sobre os **constructos colaborativos** os quais a solução pode afetar na interação e desempenho das atividades entre os profissionais de saúde.
- ❖ Quasi-experimento baseado na realização de tarefas com um grupo de usuários os quais interagiram sequencialmente com a interface do artefato;

- ❖ Utilização de **Grupos Focais** e supervisionado de forma *online*:
  - *Google Meet*

### CRITÉRIO DE SELEÇÃO DOS PARTICIPANTES

- ❖ maior de 18 anos;
- ❖ profissionais da saúde ou representantes de instituição da saúde;
- ❖ usuários que pudessem assumir o papel de paciente.

# DESIGN DAS AVALIAÇÕES

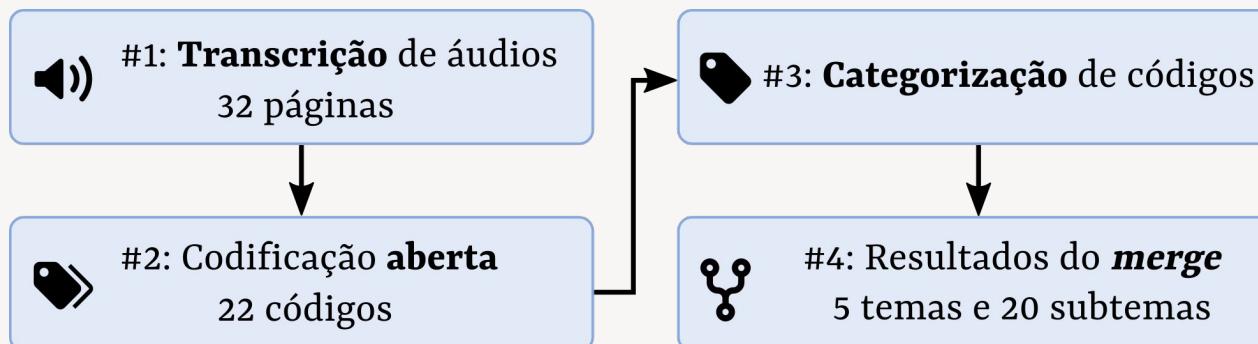
	ID*	Idade	Escolaridade	Área de Formação	Atuação Profissional	Atuação em Saúde
GRUPO FOCAL 1	Paciente1	24 anos	Médio**	Ciência da Computação	Supor te de Operações	-
	PS1	25 anos	Superior	Medicina	Médico(a)	1 ano
	IS1	29 anos	Mestrado***	Enfermagem	Bolsista do CNPq	7 anos
	LM1	32 anos	Especialização	Biomedicina	Biomédico(a)	2 anos e 6 meses
GRUPO FOCAL 2	Paciente2	27 anos	Superior	Ciência da Computação	Supervisor(a) - Gestão e Infraestrutura de TI	-
	PS2	40 anos	Doutorado	Medicina	Médico(a)/Professor(a)	16 anos
	IS2	35 anos	Mestrado	Enfermagem	Orientador(a) do Célula de Urgência e Emergência	14 anos
	LM2	25 anos	Superior****	Biomedicina	Biomédico(a)	1 anos e 6 meses

# DESIGN DAS AVALIAÇÕES

## ANÁLISE DOS DADOS DO GRUPO FOCAL

- ❖ Análise de conteúdo;
- ❖ Uso da ferramenta ATLAS.ti;

**Passos do Processamento de Dados do Grupo Focal** [Groeneveld et al. (2021)]:



GROENEVELD, W.; LUYTEN, L.; VENNEKENS, J.; AERTS, K. Exploring the role of creativity in software engineering. In: IEEE. 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSESEIS). [S.L.], 2021. p. 1-9.

# 05. Solução Proposta

# PAPÉIS ENVOLVIDOS NA SOLUÇÃO

Segundo à Resolução CFM nº 1.638/2002:

“compete à instituição de saúde e/ou ao médico o dever de guarda do prontuário”

Em relação aos locais em que o prontuário do paciente deve estar disponível, a resolução prescreve que ambulatórios, enfermarias e serviços de emergência portem tais dados para possibilitar um tratamento adequado ao paciente.

PACIENTE

PROFISSIONAL DE  
SAÚDE (PS)

LABORATÓRIO  
MÉDICO (LM)

INSTITUIÇÃO DE  
SAÚDE (IS)

# ATIVOS E SEU ARMAZENAMENTO NA REDE

Segundo à Resolução CFM nº 1.638/2002:

“o prontuário requer um conjunto mínimo de informações que devem ser obrigatoriamente preenchidos, vide: identificação completa do paciente (nome, sexo, data de nascimento, nome da mãe, naturalidade e endereço), anamnese, exame físico e exames complementares com resultados e/ou hipóteses diagnósticas e tratamento prescrito e evolução diária do paciente.”

## FHIR

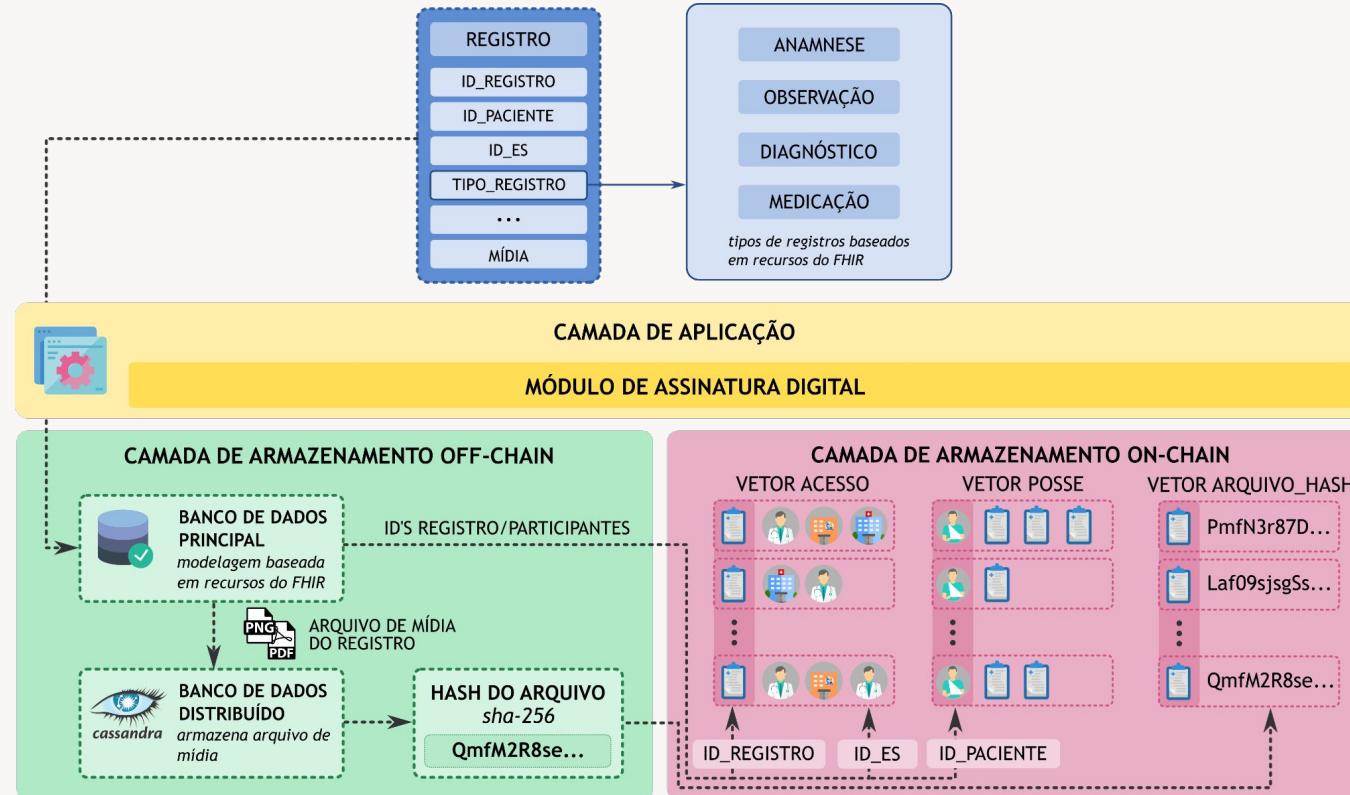
MEDICAÇÃO

OBSERVAÇÃO

DIAGNÓSTICO

QUESTIONÁRIO

# ARQUITETURA DE SOFTWARE E IMPLEMENTAÇÃO

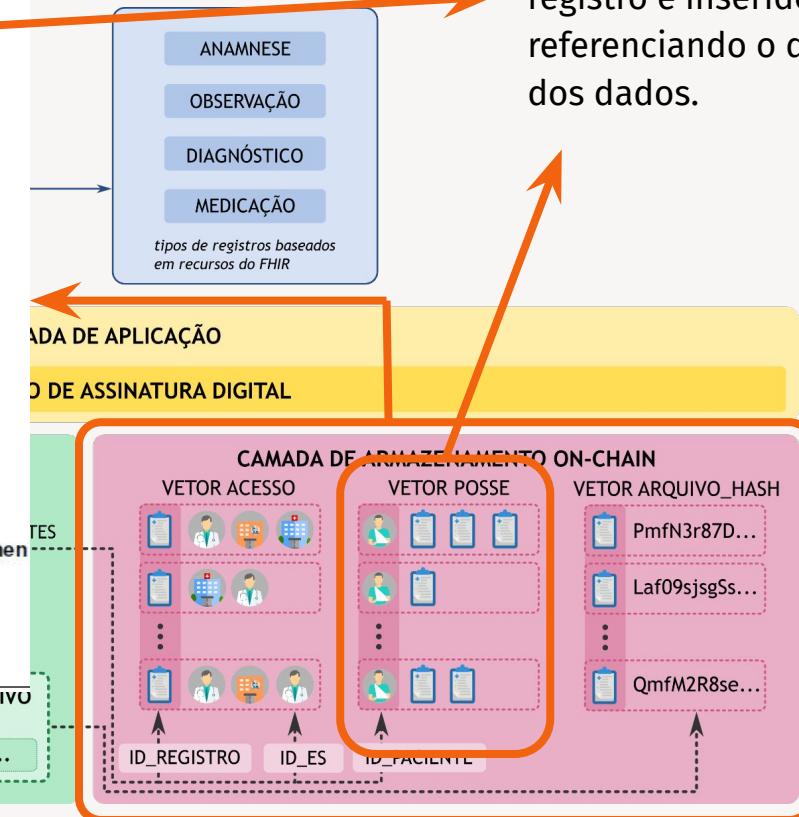


### Algoritmo 1: Contrato Inteligente ControleRegistro

```
1 Função incluirPosse(idRegistro, idPaciente, arquivoHash):  
2   Verifica se msg.sender é diferente de administrador  
3   vetorPosse[idPaciente][idRegistro] = true  
4   inserir hash em vetorArquivoHash[idRegistro]  
5 Fim Função  
6 Função incluirAcesso(idRegistro, idES):  
7   Verifica se msg.sender é diferente de administrador  
8   vetorAcesso[idRegistro][idES] = true  
9 Fim Função  
10 Função removerAcesso(idRegistro, idES):  
11   Verifica se msg.sender é diferente de administrador  
12   vetorAcesso[idRegistro][idES] = false  
13 Fim Função  
14 Função recuperarRegistro(idRegistro, idUser):  
15   Verifica se msg.sender é diferente de administrador  
16   if vetorPosse[idUser][idRegistro] == true || vetorAcesso[idRegistro][idUser] == true then  
17     return vetorArquivoHash[idRegistro]  
18 else return Usuário não tem acesso a esse Registro.  
19 Fim Função
```



## TO ON-CHAIN



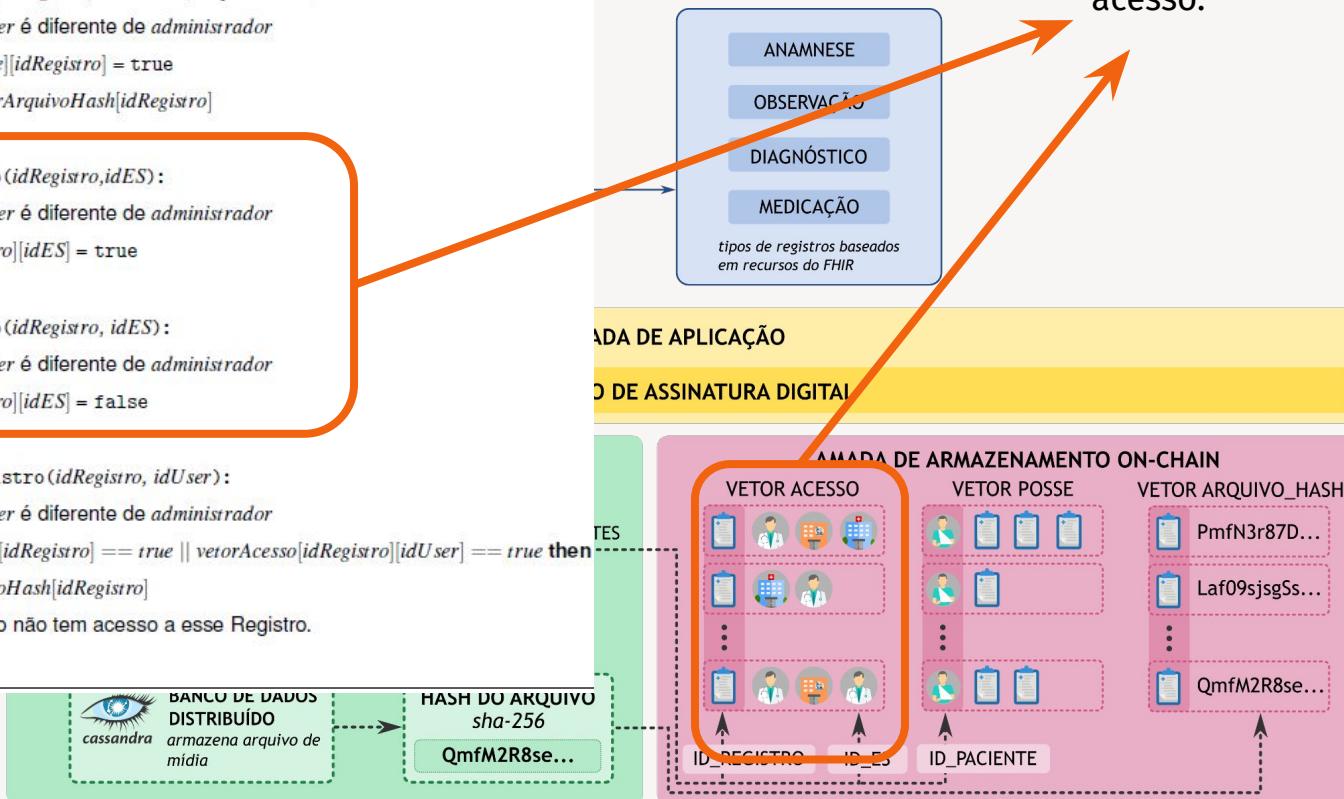
Manipulado quando um registro é inserido, referenciando o detentor dos dados.

### Algoritmo 1: Contrato Inteligente ControleRegistro

```
1 Função incluirPosse(idRegistro, idPaciente, arquivoHash):  
2   Verifica se msg.sender é diferente de administrador  
3   vetorPosse[idPaciente][idRegistro] = true  
4   inserir hash em vetorArquivoHash[idRegistro]  
5 Fim Função  
6 Função incluirAcesso(idRegistro, idES):  
7   Verifica se msg.sender é diferente de administrador  
8   vetorAcesso[idRegistro][idES] = true  
9 Fim Função  
10 Função removerAcesso(idRegistro, idES):  
11   Verifica se msg.sender é diferente de administrador  
12   vetorAcesso[idRegistro][idES] = false  
13 Fim Função  
14 Função recuperarRegistro(idRegistro, idUser):  
15   Verifica se msg.sender é diferente de administrador  
16   if vetorPosse[idUser][idRegistro] == true || vetorAcesso[idRegistro][idUser] == true then  
17     return vetorArquivoHash[idRegistro]  
18   else return Usuário não tem acesso a esse Registro.  
19 Fim Função
```

# TO ON-CHAIN

Associado ao controle de acesso.

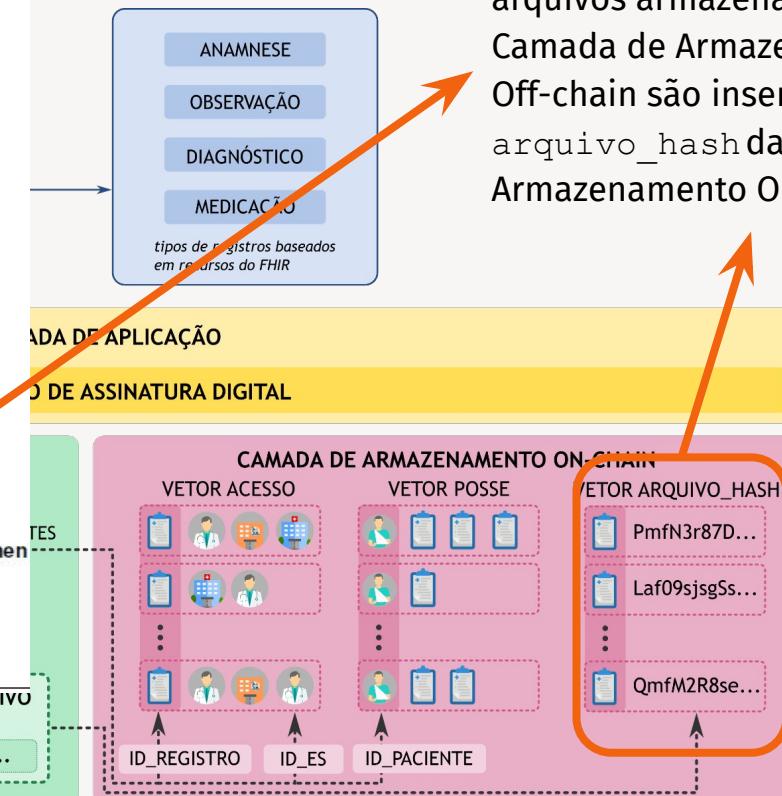


### Algoritmo 1: Contrato Inteligente ControleRegistro

```
1 Função incluirPosse(idRegistro, idPaciente, arquivoHash):  
2   Verifica se msg.sender é diferente de administrador  
3   vetorPosse[idPaciente][idRegistro] = true  
4   inserir hash em vetorArquivoHash[idRegistro]  
5 Fim Função  
6 Função incluirAcesso(idRegistro, idES):  
7   Verifica se msg.sender é diferente de administrador  
8   vetorAcesso[idRegistro][idES] = true  
9 Fim Função  
10 Função removerAcesso(idRegistro, idES):  
11   Verifica se msg.sender é diferente de administrador  
12   vetorAcesso[idRegistro][idES] = false  
13 Fim Função  
14 Função recuperarRegistro(idRegistro, idUser):  
15   Verifica se msg.sender é diferente de administrador  
16   if vetorPosse[idUser][idRegistro] == true || vetorAcesso[idUser][idRegistro] == true then  
17     return vetorArquivoHash[idRegistro]  
18   else return Usuário não tem acesso a esse Registro.  
19 Fim Função
```

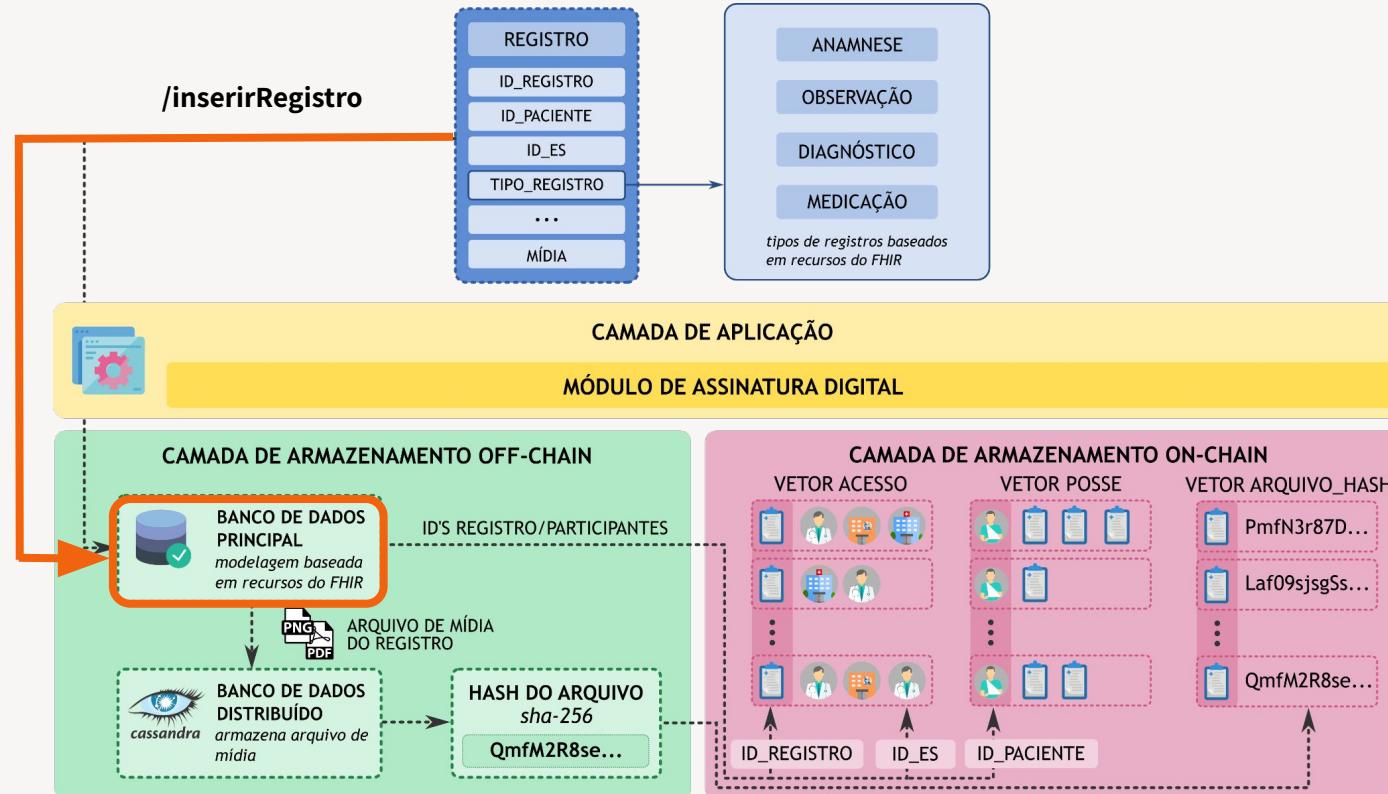


## TO ON-CHAIN

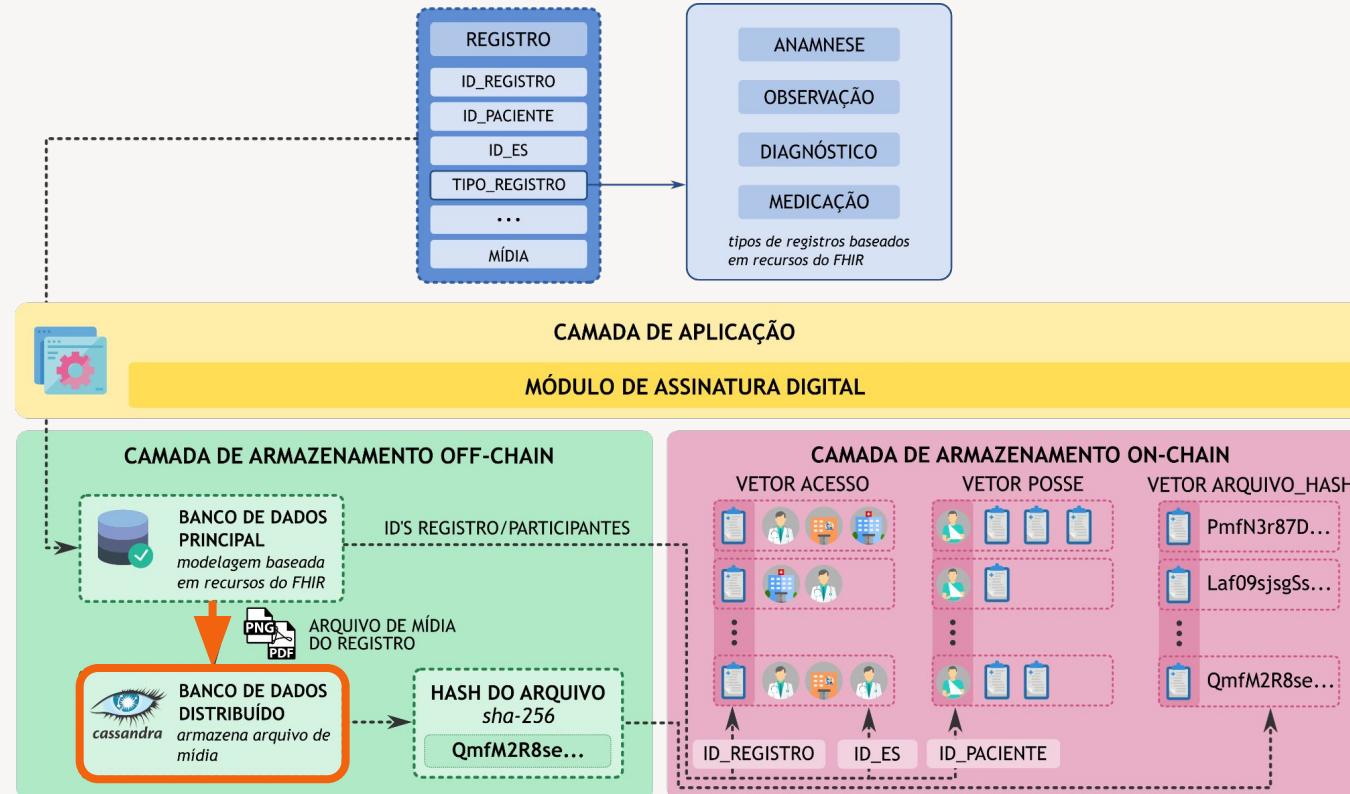


Os hashes referentes aos arquivos armazenados na Camada de Armazenamento Off-chain são inseridos no vetor arquivo\_hash da Camada de Armazenamento On-chain.

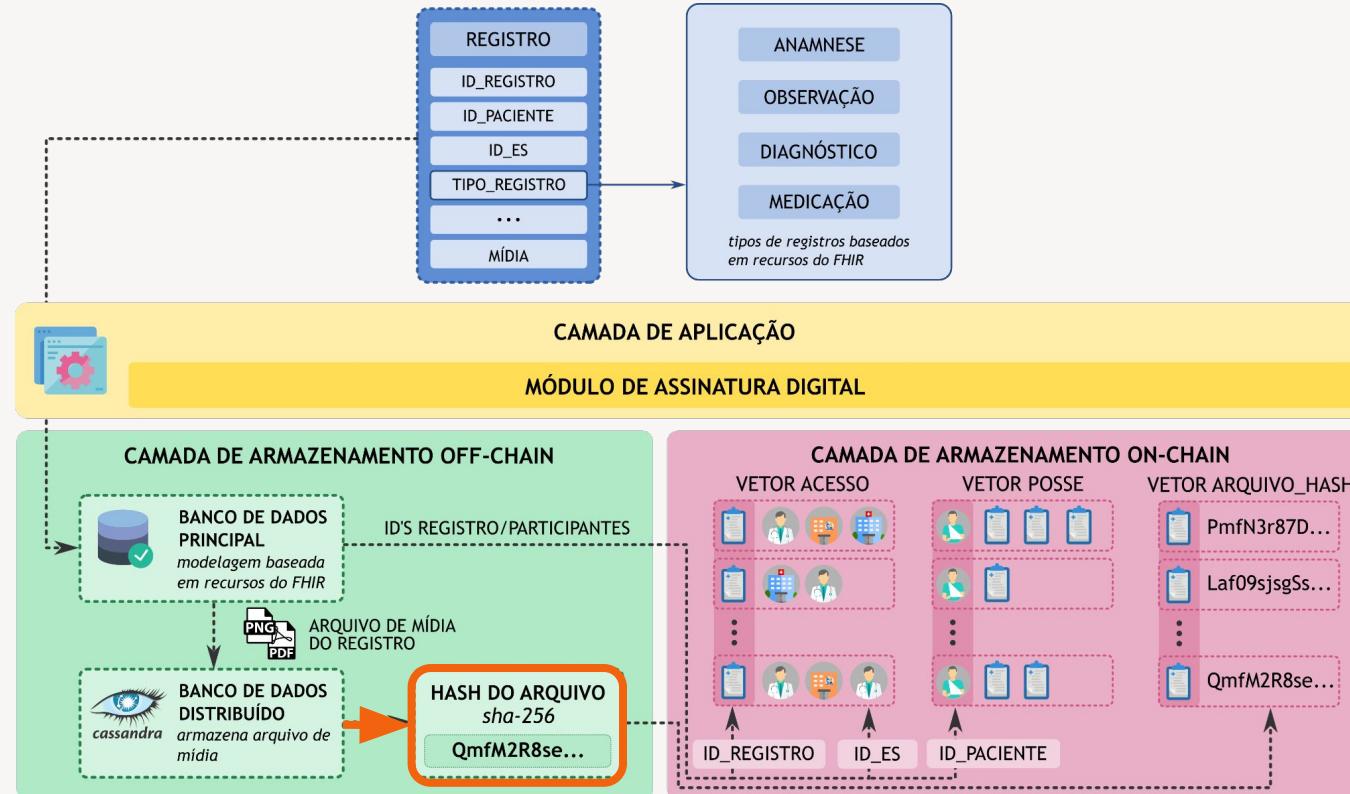
# CAMADA DE ARMAZENAMENTO OFF-CHAIN



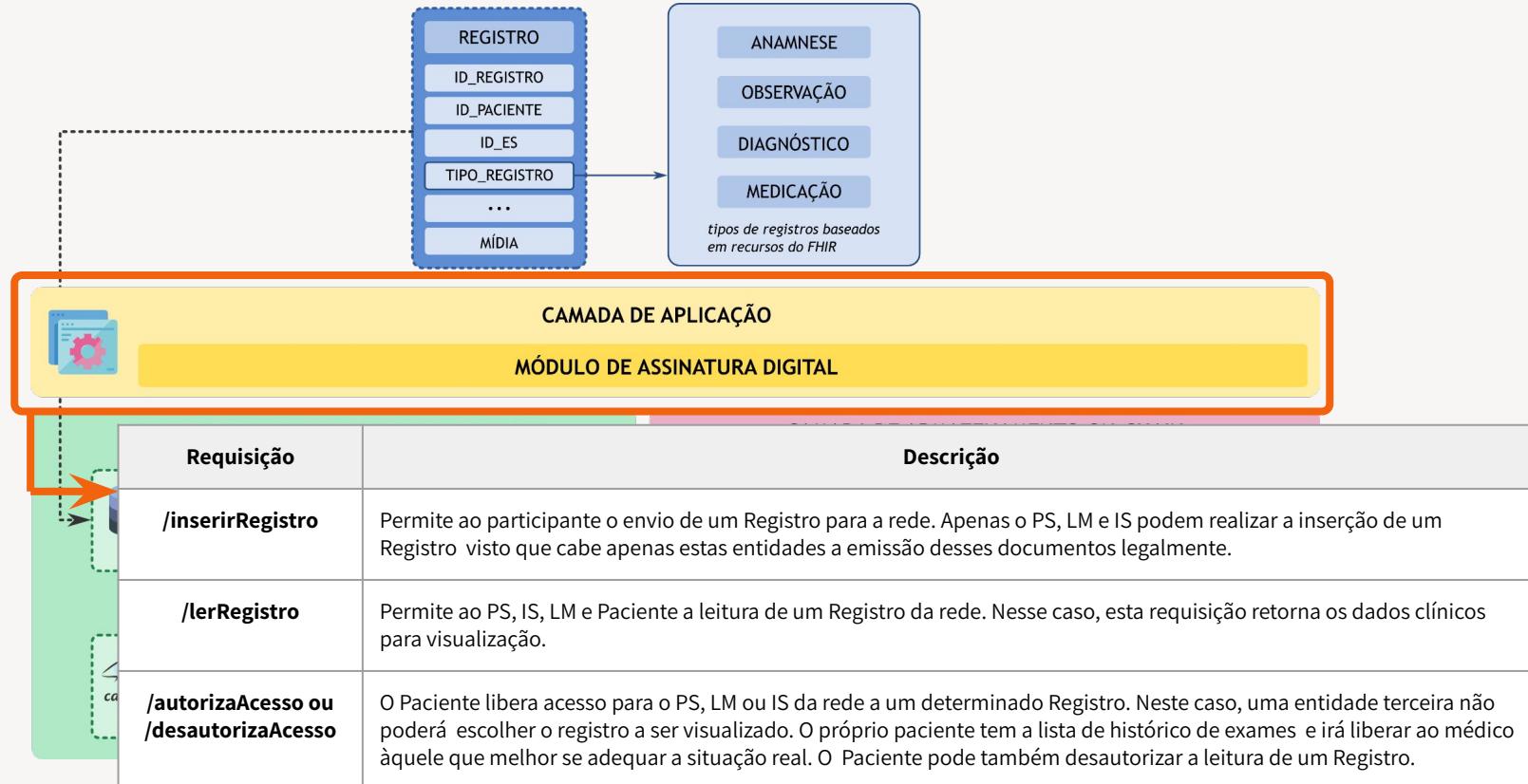
# CAMADA DE ARMAZENAMENTO OFF-CHAIN



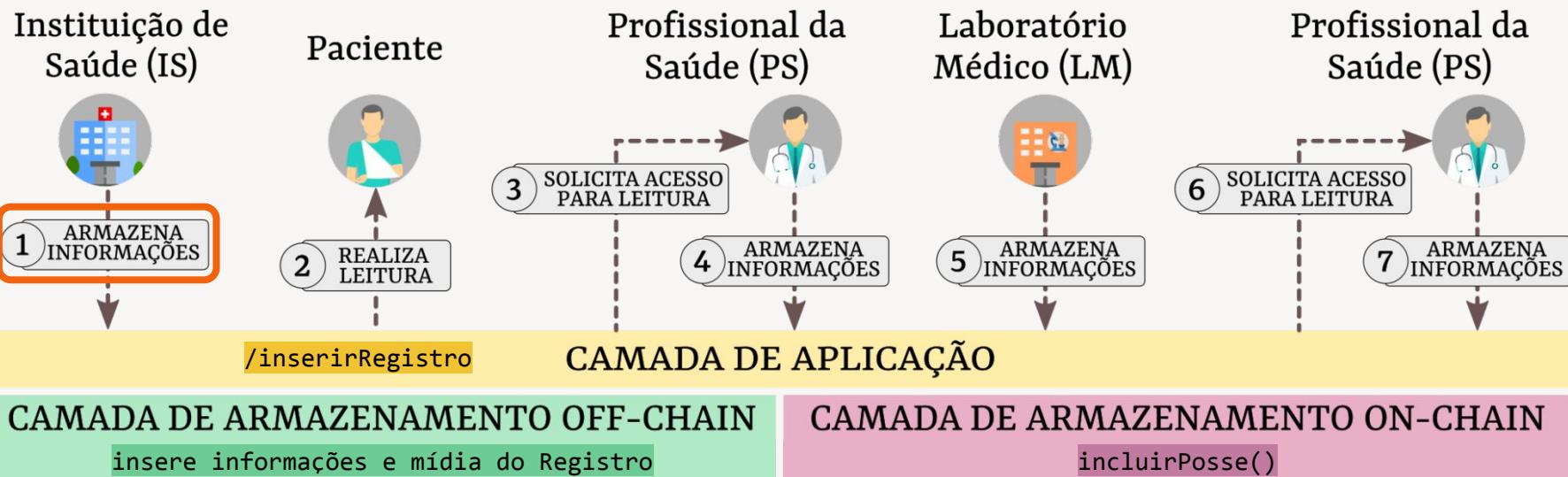
# CAMADA DE ARMAZENAMENTO OFF-CHAIN



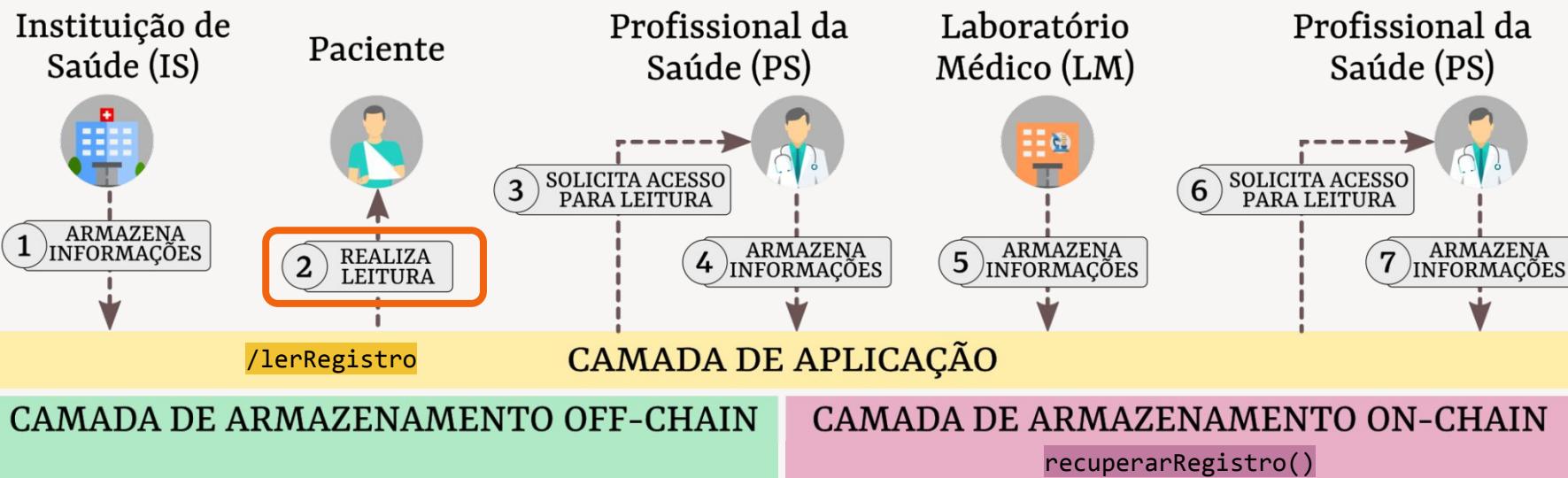
# CAMADA DE APLICAÇÃO



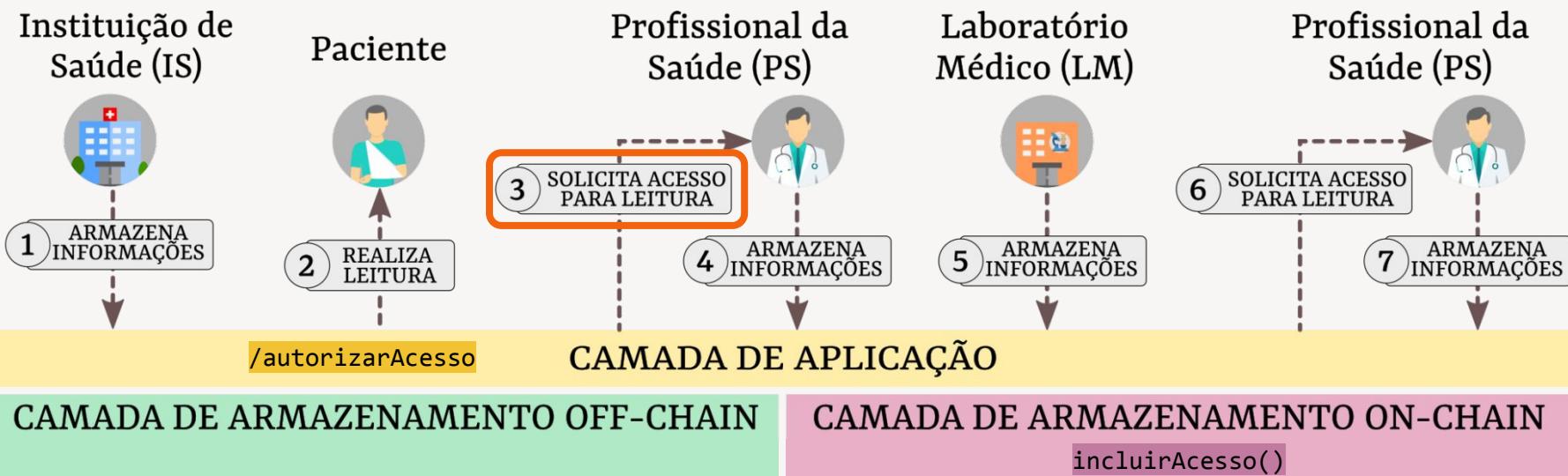
# DEMONSTRAÇÃO DO WORKFLOW ILUSTRATIVO



# DEMONSTRAÇÃO DO WORKFLOW ILUSTRATIVO



# DEMONSTRAÇÃO DO WORKFLOW ILUSTRATIVO



# 06. Avaliação Técnica

# AVALIAÇÃO DE ADERÊNCIA AOS REQUISITOS ADVINDOS DE NORMAS NACIONAIS

## SUBCONJUNTO DOS REQUISITOS DA SBIS SATISFEITOS PELAS ESTRATÉGIAS UTILIZADAS

ID	Requisitos de Conformidade	Descrição
NGS1.02	Identificação e autenticação de pessoas	Permitir que os usuários possam ser identificados e autenticados, além de protegidos contra falhas
NGS1.04	Autorização e controle de acesso	Conceder autorizações para acesso dos dados por terceiros e controlar o acesso de pessoas ao sistema
NGS1.05	Disponibilidade do RES	Garantir que os dados possuam cópia de segurança para manter a integridade dos dados
NGS1.07	Segurança de Dados	Salientar que os dados devem ser armazenados em um Sistema de Gerenciamento de Banco de Dados com validação de acesso aos dados
NGS1.12	Privacidade	Garantir o consentimento, por parte do paciente, no compartilhamento de suas informações pessoais de saúde somente para pessoas autorizadas
NGS1.13	Autenticação de usuário utilizando certificado digital	Apresenta os critérios e normas para o uso de certificados digitais em nível de segurança 1
NGS2.01	Certificado digital	Apresenta os critérios e normas para o uso de certificados digitais em nível de segurança 2
NGS2.02	Assinatura digital	Aponta itens de validação e formatos das assinaturas digitais
NGS2.04	Digitalização de documentos	Informar as assinaturas que devem estar presentes nos documentos digitalizados e autorizações que permitam a digitalização desses documentos
ESTR.04	Dados clínicos	Regulamenta como os dados clínicos devem ser tratados
FUNC.02	Problemas/condições de saúde e outras questões	Garantir que os dados de um paciente sejam armazenados de forma cronológica e acessíveis para consultas
FUNC.17	Médico-legal	Trata da manutenção da cronologia de eventos, assegurando que dados retroativos possam ser registrados
FUNC.18	Atores	Delimitação do papel de cada pessoa com autorização para interagir com o sistema com as devidas restrições para cada
SGED.01	Gerais	Trata dos arquivos que devem ser suportados pelo sistema assim como obter os dados clínicos e os métodos de indexação dos arquivos

# AVALIAÇÃO DE ADERÊNCIA AOS REQUISITOS ADVINDOS DE NORMAS NACIONAIS

## SUBCONJUNTO DOS PRINCÍPIOS DA LGPD SATISFEITOS PELAS ESTRATÉGIAS UTILIZADAS

Princípio	Resumo	LGPD	GDPR
Minimização de dados	Os dados devem ser relevantes e necessários para o efeito.	Art. 6º (1) (2) (3)	Art. 5º (1) lit c; Art. 25º
Anonimização	Implementação e utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.	Art. 5º (3) (11); Art. 12º	Art. 5º; Art. 32; Art. 34; Recital 26
Limitação de armazenamento	Os dados devem ser armazenados em uma forma que permita a identificação do titular dos dados não mais do que o tempo necessário.	Art. 15º	Art. 5º (1) lit e;
Integridade e confidencialidade	Os dados devem ser processados de forma a garantir a segurança e proteção adequadas contra o processamento não autorizado.	Art. 6º (IV) (VII); Art. 46º	Art. 5º (1) lit f;
Consentimento	O tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular.	Art. 5º (VII); Art. 8º	Art. 4º (11); Art. 6º (1) lit a; Art. 7º
Direito ao esquecimento	O titular dos dados pode obter do controlador a exclusão de dados pessoais, quando, e. g. os dados não são mais necessários, o titular dos dados retira seu consentimento ou os dados pessoais foram coletados ilegalmente.	Art. 5º (XIV)	Art. 17º
Direito de acesso	Fornecer ao titular acesso aos seus dados pessoais, garantindo a portabilidade desses dados a um outro controlador.	Art. 18º	Art. 15º
Direito à informação	Garantir ao titular a visibilidade em torno do que venha a ser realizado com os seus dados pessoais.	Art. 18º	Art. 13º
Portabilidade de dados	O titular dos dados tem o direito de receber seus dados pessoais em um formato estruturado, comumente usado e legível por máquina e de transmitir esses dados a outro controlador.	Art. 18º	Art. 20º

# AVALIAÇÃO DE ADERÊNCIA AOS REQUISITOS ADVINDOS DE NORMAS NACIONAIS

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de design
Grupo 1	Identificação e autenticação de pessoas	NGS1.02	Anonimização	Art. 5º (3)(11); Art. 12º	Regra de acesso por meio da manipulação de estruturas de dados implementadas nos CI.
	Autorização e controle de acesso	NGS1.04	Confidencialidade e Consentimento	Art. 5º (VII); Art. 8º Art. 46º	
	Privacidade	NGS1.12	Direito de acesso   Direito à informação   Identificação dos responsáveis pelo tratamento	Art. 18º	Estratégia <i>off-chain</i> para privacidade de dados sensíveis.
	Atores	FUNC.18			
Grupo 2	Disponibilidade do RES	NGS1.05	Integridade	Art. 6º (IV)(VII)	Réplicas dos dados em cada nó da rede.
	Segurança de Dados	NGS1.07			Armazenamento de <i>hash</i> imutável e auditável.
Grupo 3	Dados clínicos Gerais	ESTR.04 SGED.01	Limitação de armazenamento Minimização de dados pessoais Direito ao esquecimento	Art. 15º Art. 6º (1)(2)(3) Art. 5º (XIV)	Estratégia <i>off-chain</i> para armazenamento dos dados brutos.
	Problemas/condições de saúde e outras questões	FUNC.02			
	Médico-legal	FUNC.17			Imutabilidade e operações <i>append-only</i> .

# AVALIAÇÃO DE DESEMPENHO

## CONFIGURAÇÃO DO EXPERIMENTO COMPUTACIONAL

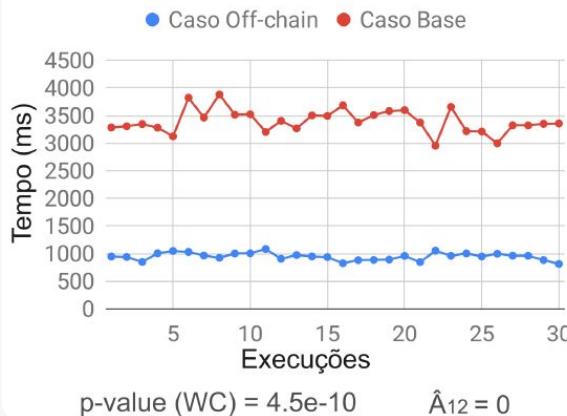
- ❖ Implementação da Prova de Conceito de um dApp;
- ❖ Testes aplicados sobre duas funções do contrato inteligente:
  - **inserirRegistro;**
  - **lerRegistro.**
- ❖ Para fins de comparação foram criados dois tipos de casos:
  - **Caso Base;**
  - **Caso Off-chain.**

- ❖ Simulação com tamanhos de arquivos:
  - 1000 *bytes* à 2000 *bytes*;
  - 2000 *bytes* à 4000 *bytes*;
  - 4000 *bytes* à 7000 *bytes*;
- ❖ Métricas analisadas:
  - Tempo de Publicação;
  - Tempo de Busca.
- ❖ Configuração da máquina:
  - 16 GB de memória RAM, SSD de 256 GB, processador Intel Core i7

# AVALIAÇÃO DE DESEMPENHO

## RESULTADOS TEMPO DE PUBLICAÇÃO

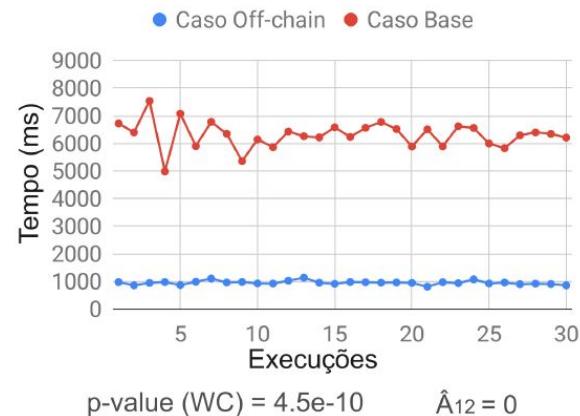
(a) Arquivos de tamanho entre 1KB à 2KB



**3397 ms**

**1082 ms**

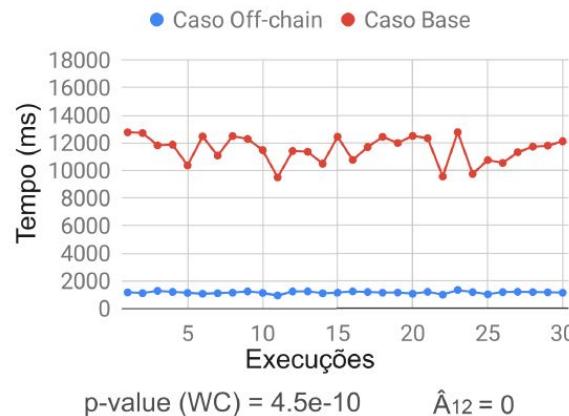
(b) 2KB a 4KB



**6307 ms**

**1133 ms**

4KB a 7KB



**11543 ms**

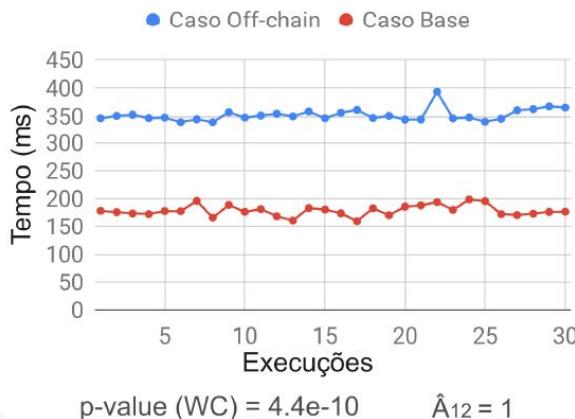
**1141 ms**

- Para todas as situações, existem evidências estatísticas que mostram que o tempo de publicação do Caso Base é significantemente maior que o do Caso Off-chain em 100% das execuções para todos os tamanhos de arquivos, visto que o p-value mostra-se inferior à 0,5 e o  $\hat{\Delta}_{12}$  equivale à 0.

# AVALIAÇÃO DE DESEMPENHO

## RESULTADOS TEMPO DE BUSCA

(a) Arquivos de tamanho entre 1KB à 2KB



**179 ms**

**352 ms**

(b)

- Nessas duas situações os casos são significativamente diferentes, com o Caso Off-chain tendo maiores valores de tempo de busca em 100% das execuções em relação ao Caso Base.
  - Na Figura b o Caso Off-chain obteve um tempo maior em 14% das execuções em relação ao Caso Base.
- 
- Scatter plot (b) showing search time (ms) vs. executions for files between 1KB and 2KB. The y-axis ranges from 0 to 1800 ms, and the x-axis ranges from 5 to 30 executions. Blue dots represent 'Caso Off-chain' and red dots represent 'Caso Base'. The 'Caso Off-chain' data is consistently higher than 'Caso Base'.
- | Execuções | Caso Off-chain (ms) | Caso Base (ms) |
|-----------|---------------------|----------------|
| 5         | 340                 | 170            |
| 10        | 340                 | 170            |
| 15        | 340                 | 170            |
| 20        | 340                 | 170            |
| 25        | 340                 | 170            |
| 30        | 340                 | 170            |

# 07. Avaliação Social

# AVALIAÇÃO SOCIAL

## RESULTADOS

- ❖ Através da análise de conteúdo sobre a discussão dos Grupos Focais, foi possível identificar:
  - 5 temas;
  - 20 subtemas;
- ❖ Ocorrência de Subtemas nos Grupos Focais:
  - GF 1 discutiu 90% de todos os subtemas encontrados;
  - GF 2 discutiu 75% de todos os subtemas encontrados;

Tema	Subtema	Ocorrência nos Grupos Focais	
		1	2
Uso atual do PEP	Falta de integralidade e interoperabilidade das informações entre diferentes unidades	✓	✓
	Registro de todas as informações possíveis sobre o paciente é muito relevante e comum entre os profissionais de saúde	✓	✓
	Controle de acesso às informações do paciente entre os profissionais e entidades de saúde	✓	✓
	Fluxo e hierarquia de atividades nos registros dos pacientes entre os profissionais de saúde		✓
	Armazenamento e gerenciamento atual de registros por parte do paciente	✓	✓
Modelo 4C	Compartilhamento e visualização de informações do paciente por parte dos profissionais	✓	✓
	Disponibilidade e prevenção de perda das informações sobre o segmento do paciente	✓	
	Conscientização dos profissionais de saúde / Interprofissionalidade	✓	✓
PEP & Blockchain	Imutabilidade, rastreabilidade e auditoria das informações aumenta segurança de todas as partes	✓	✓
	Alterações de informações dentro do prontuário		✓
	Acesso e facilidade na disponibilidade das informações	✓	✓
Melhoria da Qualidade	Controle de acesso e segurança da informação do paciente	✓	
	Qualidade de processos e do trabalho	✓	✓
	Controle de acesso e LGPD	✓	✓
	Liberdade de acesso por profissionais de saúde para agirem em situações de emergência	✓	
	Dificuldade de lidar com a tecnologia	✓	✓
Lições Aprendidas e Oportunidades	Dificuldade de implantação	✓	
	Integração com sistemas automatizados	✓	✓
	Registro dos acessos a uma prescrição específica	✓	
	Nível de assistência médica	✓	✓

# USO ATUAL DO PEP

**Falta de integralidade e interoperabilidade das informações entre diferentes unidades.**

“nunca tem essa integralidade registrada, porque eu não sei o que o outro profissional faz (...) Eu não via evolução de pacientes nem de outros postos da região, nem de especialistas” (PS 1)

Dificuldade observada mais em instituições públicas.

**Registro de todas as informações possíveis sobre o paciente é muito relevante e comum entre os profissionais e entidades de saúde.**

“[...] se dá muito por escrito em termos de parecer” (PS 2)  
“a forma da gente comprovar o nosso serviço que a gente tá fazendo com o paciente, é a partir da anotação do registro” (IS 1)

Deve-se ter meios eficazes de integrá-las entre os profissionais e entre instituições diferentes a fim de mitigar problemáticas relacionadas à interoperabilidade e organização das informações.

**Controle de acesso às informações do paciente entre os profissionais e entidades de saúde.**

“não tem nenhuma privacidade pra quem trabalha no hospital” (PS 1)  
“solicita uma assessoria médica” (LM 1)

Até que ponto o paciente tem o controle de seus dados armazenados por um hospital ou um laboratório?

Maior burocracia para os LMs.

# USO ATUAL DO PEP

## Fluxo e hierarquia de atividades nos registros dos pacientes entre profissionais de saúde.

“[...] pode haver mudanças em que o médico ali faz a mudança e comunica ao enfermeiro para que apraza. O técnico, em seguida, executa alguma medicação que deve ser administrada” (IS 2).

Existe uma certa “coordenação” de algumas atividades entre os diferentes tipos de profissionais da saúde

## Armazenamento e gerenciamento atual de registros por parte do paciente.

“[...] até hoje eu ainda tenho guardado o envelope, porque pra onde eu for, em questão de saúde, eu fico levando” (Paciente 1).

“não faço uma gestão muito elaborada [...] Por exemplo, exames eu guardo por um tempo, depois eu descarto” (Paciente 2)

O prontuário em papel ainda se faz presente em muitas instituições.

Lacunas no histórico do paciente.

Poucos sistemas de gerenciamento de acesso aos registros.

Baixa conscientização de pacientes pela própria privacidade.

# MODELO 4C

**Compartilhamento e visualização de informações do paciente por parte dos profissionais.**

“iria ficar muito mais fácil mesmo, e a gente não iria perder a informação do paciente” (PS1)

“ [...] ajuda a equipe demais se essa interação vier com o diálogo correto e, dessa forma que a gente tá pondo, isso é excepcional na realidade” (PS2)

**Disponibilidade e prevenção de perda das informações sobre o segmento do paciente.**

“ [...] informações que às vezes o paciente não lembra, às vezes, perdeu um exame ou não leva” (PS 1)

**Conscientização dos profissionais de saúde / Interprofissionalidade.**

“ [...] ajuda muito nessa questão da comunicação. Porque, infelizmente, os profissionais de saúde não conseguem ainda atuar nessa questão da interprofissionalidade, que é algo urgente, desde sempre, acredito” (IS 1)

O IS1 informou que um médico pode prescrever informações para um enfermeiro, por exemplo, este, por sua vez, deve realizar procedimentos conforme o que foi prescrito.

A única forma de se obter indícios do sucesso da **comunicação** é através do discurso e das ações (e reações) do receptor.

Uso de blockchain permite o compartilhamento de forma segura e minimiza a perda de informações.

Padrões de interoperabilidade, legibilidade, passagem de plantões.

Minimização da perda de informações visto que as informações são armazenadas em réplicas. Melhoria de acesso por parte do paciente e médicos.

Interprofissionalidade depende da **colaboração e cooperação** entre os profissionais que manuseiam as informações do paciente, de forma que possam desenvolver o trabalho em conjunto.

O pilar **coordenação** pode apresentar também interdependência de atividades, o que significa que a equipa são mutuamente interdependentes.

# PEP BASEADO EM BLOCKCHAIN

**Imutabilidade, rastreabilidade e auditoria das informações aumenta segurança de todas as partes.**

“garante a segurança do paciente e a atuação do profissional. O respaldo do profissional [...] Porque o registro é informação, é o respaldo do seu trabalho” (IS 1)

[...] às vezes, dá problema, o paciente pode dizer que informou uma coisa e não tá registrado, ou o contrário, o médico dizer que registrou e não tá lá escrito”. (PS 2)

**Alterações de informações dentro do prontuário.**

“profissional tem acesso a mudar uma determinada questão dentro do prontuário, o médico faz a prescrição, uma enfermeira apraza” (IS 2)

**Acesso e facilidade na disponibilidade das informações.**

“independente do que acontecer, aquilo vai tá disponível nos outros membros da rede” (Paciente 1)

“é importante esse registro digital [...] por exemplo, depois de 10 anos, o SUS não tem mais que ter aquele registro no papel, o papel pode ser eliminado, pode ir pra um arquivo, então isso vai mudar né, quando eu tenho esse registro”. (IS 2)

**Controle de acesso e segurança da informação do paciente.**

O Paciente 1 informa que a possibilidade de liberar e negar acesso é uma etapa importante que pode influenciar na segurança de dados do paciente.

Gera rastreabilidade nas ações dos registros dos pacientes.

Aumenta a eficiência das auditorias.

Evidências digitais e órgãos judiciais.

Histórico de alterações sobre diferentes versões de um mesmo documento.

Vincular identidade de quem realiza as alterações.

Registro da evolução do paciente.

Minimiza perda de informações.

Segurança dos dados do paciente.

Desafios dependendo do contexto.

# MELHORIA NA QUALIDADE

## Qualidade de Processos e do Trabalho.

“os laboratórios vão ter um pouco mais de cautela, fazerem, liberarem esses resultados, que deveria ser o normal. O normal é que já tenha cautela. Mas, é, isso deixa escrita eternamente e facilitando o acesso ao paciente a esse erro” (LM 1).

“talvez até na maneira que você coloca as perguntas pra gente preencher, tem como melhorar a própria qualidade da anamnese principalmente dependendo do contexto” (PS 2).

Impactos no gerenciamento de atendimento ao cliente, processos internos, verificações de segurança.

Comprovação de serviços e trabalho dos profissionais.

Melhoria na qualidade das informações pelo acesso à dados completos.

Confiabilidade de forma a impactar na satisfação do paciente.

Melhoria nos recursos de auditoria e relatório das organizações.

# LIÇÕES APRENDIDAS E OPORTUNIDADES

**Controle de acesso pelo paciente e a LGPD.**

**Liberdade de acesso por profissionais de saúde para agirem em situações de emergência.**

**Dificuldade de lidar com tecnologia.**

**Dificuldade de implantação.**

“[...] suponhamos que o(a) Paciente 2 não autorizou ninguém a olhar os dados dele(a), então de repente ele(a) está lá na emergência, faz uma dipirona e convulsiona, né? Eu não tenho o histórico dela porque ela não autorizou” (IS2).

“[...] teria esses dois pontos: de ele tá inconsciente e de ele também está consciente, mas não saber mexer, não saber trabalhar com a tecnologia que ele tem em mãos”. (Paciente 2)

“nem todo paciente vai entender esse fluxo” (PS 1)  
“existem também alguns profissionais que têm dificuldades” (IS 1)

“[...] isso soluciona totalmente essa problemática, mas quando você investe toda essa solução do ponto de vista tecnológico, não vai ser completamente perfeito” (Paciente 1)

Dificuldade de uso da solução em situações de emergência.

Novos contratos com funções administrativas.

Envio de contratos formais em blockchain no âmbito da equipe multiprofissional ou instituição.

Tal problemática se faz presente em muitos setores, áreas e domínios onde ocorre uma transformação digital.

Necessidade de políticas públicas.

Esforço do profissional e constante atualização tecnológica é essencial.

Fatores institucionais, normas e cultura das organizações.

# LIÇÕES APRENDIDAS E OPORTUNIDADES

## Integração com sistemas automatizados.

“[...] envia esses resultados para o servidor de interfaceamento e o servidor pega esses resultados do paciente e manda pro sistema hospitalar”. (LM 1)

Módulos para comunicação com outros serviços podem ser adicionados na Camada de Aplicação.

## Registro dos acessos a uma prescrição específica.

“[...] a gente pode auditar aquilo ali e ver quem foi a última pessoa que teve acesso” (LM 1)

Log de inserções com gravação do *timestamp*.

Registro de novas ações.

## Níveis de assistência médica.

“paciente eletivos [...] que são aqueles que periodicamente vão e voltam ao hospital, né. Ele se encaixa perfeito nele”. (LM 1)

Nível de assistência básica.

Pacientes eletivos.

Comunicação entre diferentes instituições.

# 08. Ameaças à Validade

# AMEAÇAS À VALIDADE

## AMEAÇAS INTERNAS

- ❖ Na avaliação computacional foram utilizados **dados gerados aleatoriamente**;
  - Representado pela codificação base64.
  - Apresentar carga de trabalho.
- ❖ **Longa duração** do experimento social;
  - Experimento piloto possibilitou a eliminação de etapas redundantes.
- ❖ Situações especiais podem gerar **alteração comportamental** (Efeito Hawthorne)

## AMEAÇAS EXTERNAS

- ❖ Na avaliação computacional, arquivos de **tamanhos 1KB à 7KB**;
- ❖ **Generalização da avaliação de aderência** à normas técnicas pode ser prejudicada para outros países;
  - Análise para GDPR.
- ❖ No experimento social, **número reduzido de participantes e GFs**;
  - Tamanho ótimo de um GF deve permitir a participação efetiva;
  - Convergência dos temas.

# AMEAÇAS À VALIDADE

## AMEAÇAS DE CONCLUSÃO

- ❖ Na avaliação computacional, **alterações de latências dos diferentes instantes** de tempo avaliados.
  - 30 execuções em cada cenário e tamanho de arquivo;
- ❖ No experimento social, **GFs realizados virtualmente**.
  - Grupo com especialidades diferentes e aptos para executar os fluxos através da interface web.

## AMEAÇAS DE CONSTRUÇÃO

- ❖ **Poucas métricas** referentes às características internas da blockchain.
  - Métricas utilizadas podem impactar na experiência do usuário.
- ❖ Alguns participantes com **conhecimento em computação**.

# 09. Considerações Finais

# CONSIDERAÇÕES FINAIS

## CONTRIBUIÇÕES

- ❖ Análise do arcabouço regimental para adequação do uso de blockchain em PEPs;
- ❖ Proposta de arquitetura de software;
- ❖ Metodologia sociotécnica multi-método;
- ❖ Implementação da PoC.

# CONSIDERAÇÕES FINAIS

## LIMITAÇÕES

- ❖ Comparação com sistemas existentes;
- ❖ Funcionalidades da PoC restringidas pelo escopo do trabalho pode ter limitado novos *insights*;
- ❖ Múltiplas métricas computacionais e de usabilidade;
- ❖ Total integração com padrões de interoperabilidade.

# CONSIDERAÇÕES FINAIS

## TRABALHOS FUTUROS

- ❖ Introdução de novas blockchains;
- ❖ Novos algoritmos de consenso;
- ❖ Utilização de novas métricas para o experimento computacional e introdução de novos conceitos para avaliação de novos constructos colaborativos, como o *Technology Acceptance Model*.
- ❖ Integração da solução com APIs de padrões de interoperabilidade, como o FHIR.
- ❖ Inclusão de novos cenários no experimento com pessoas;
- ❖ Inclusão de novos papéis de usuários, como entidades que representam Farmácias, por exemplo.



# Obrigada!

## Dúvidas?



UNIVERSIDADE  
ESTADUAL DO CEARÁ



Programa de Pós-Graduação  
em Ciência da Computação