



Prontuário Eletrônico do Paciente baseado em Blockchain: Uma Análise das Potencialidades e Desafios à Luz dos Requisitos da SBIS e LGPD

Autores: Pamella Soares (UECE - PPGCC), Allysson Allex Araújo (UFC - GESID),
Raphael Saraiva (UECE - PPGCC), Jerffeson Souza (UECE - PPGCC),
George Sousa (UECE - PPCCLIS) e Lúcia Duarte (UECE - PPCCLIS)



UNIVERSIDADE
ESTADUAL DO CEARÁ



Programa de Pós-Graduação
em Ciência da Computação



UNIVERSIDADE
FEDERAL DO CEARÁ



Agenda

- 1. Introdução**
- 2. Análise Preliminar dos Requisitos**
Advindos da SBIS e LGPD
- 3. Considerações Finais**

01. Introdução

INTRODUÇÃO

PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)

“

O Prontuário Eletrônico do Paciente (PEP) é uma **estrutura** que **descreve e registra eventos** e serviços médicos **realizados aos pacientes ao longo de sua vida** (incluindo procedimentos, prescrições e exames executados por profissionais) de forma a facilitar a **tomada de decisões** para definir os devidos tratamentos e processos.

Um ponto crítico a ser observado é a **segurança da informação**, visto que os dados do paciente devem receber tratamento adequado a fim de preservar a **privacidade**.

INTRODUÇÃO

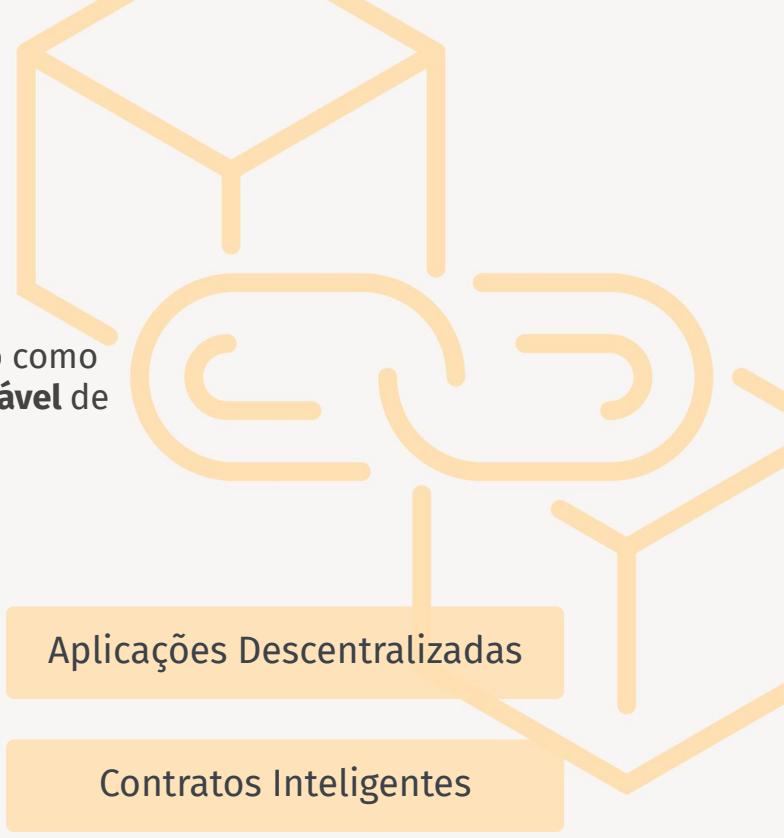
BLOCKCHAIN

O usufruto de blockchain no contexto de PEP tem se posicionado como proeminente tendo em vista a capacidade única de **registro imutável** de **eventos digitais** de forma **transparente, segura e resiliente**.

“

Em suma, o blockchain funciona como um livro-razão distribuído, onde o registro, a verificação, o armazenamento, a manutenção e a transmissão de dados são baseados numa arquitetura distribuída protegida por criptografia, cuja governança e confiança mútua entre os nós da rede é estabelecida de forma descentralizada através de algoritmos de consenso.

[Beck et al. 2017]



INTRODUÇÃO

BLOCKCHAIN E PRONTUÁRIO ELETRÔNICO DO PACIENTE

DESAFIOS

- ❖ Fatores institucionais:
 - Normas e culturas das organizações;
 - Regulamentações e leis existentes;
 - Governança.

[Janssen et al. 2020]

Manual de certificação Sociedade Brasileira de Informática em Saúde (SBIS)

Lei Geral de Proteção de Dados (LGPD)

Identifica-se uma **carência quanto ao alinhamento e discussão** específica do atendimento de tais normas ao utilizar blockchain na implementação de PEPs.

OBJETIVO



O presente trabalho visa identificar e avaliar as **potencialidades** e os **desafios** no **desenvolvimento de PEPs baseado em blockchain** por meio de uma **análise documental** no manual de certificação da **SBIS** e na **LGPD**. Respectivamente, esta avaliação considera os requisitos para certificação de PEPs, assim como os princípios de privacidade dos dados sensíveis.

PROCESSO METODOLÓGICO

ANÁLISE 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.

02. Análise Preliminar dos Requisitos Advindos da SBIS e LGPD

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	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.
Grupo 4	Problemas/condições de saúde e outras questões Médico-legal	FUNC.02 FUNC.17			Imutabilidade e operações <i>append-only</i> .

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	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	Integridade	Art. 6º (IV)(VII)	Réplicas dos dados em cada nó da rede. Armazenamento de <i>hash</i> imutável e auditável
Grupo 2	Disponibilidade do RES	NGS1.05	Limitação de armazenamento	- Identificação as partes que interagem com a solução a fim de impedir o acesso de terceiros não-autorizados;	
	Segurança de Dados	NGS1.07	Minimização de dados pessoais	- Controle de acesso e as respectivas entidades habilitadas;	
Grupo 3	Dados clínicos Gerais	ESTR.04 SGED.01	Direito ao esquecimento	- Armazenamento de <i>hashs</i> e identificadores em bancos de dados tradicional ou distribuído;	Imutabilidade e operações <i>append-only</i> .
Grupo 4	Problemas/condições de saúde e outras questões Médico-legal	FUNC.02 FUNC.17		- Modelagem por camadas.	

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	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 Direito ao esquecimento	Art. 15º	Nós da rede se conectam entre si e, assim, mantêm as réplicas das informações de maneira distribuída;
Grupo 4	Problemas/condições de saúde e outras questões Médico-legal	FUNC.02 FUNC.17			<ul style="list-style-type: none"> - Verificar o hash computado (a saída de execução do algoritmo) a um valor de hash conhecido, esperado e inalterado. - Imutabilidade pode garantir que ações de correção ou edição preservem os dados.

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	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	ESTR.04	Limitação de armazenamento	Art. 15º	Estratégia <i>off-chain</i> para armazenamento dos dados brutos.
	Gerais	SGED.01	Minimização de dados - Desafio de escalabilidade em blockchain para armazenar, por exemplo, um arquivo de mídia;		
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02			Imutabilidade e operações <i>append only</i> .
	Médico-legal	FUNC.17		<ul style="list-style-type: none"> - Armazenar o hash do arquivo em blockchain contempla o fato de que deve-se restringir a quantidade de dados a serem apresentados a depender do propósito de uso; - Direito ao esquecimento vs. imutabilidade. 	

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	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 informação Identificação dos responsáveis pelo tratamento	- Armazenamento com registro de tempo. - Transações históricas, que são apenas anexadas, não podem ser excluídas ou modificadas sem invalidar a cadeia de hashes. - Rastreabilidade de informações.	Armazenamento off-chain para privacidade de dados sensíveis.
	Atores	FUNC.18	Integridade	Art. 6º (IV)(VII)	Armazenamento de hash imutável e auditável.
Grupo 2	Disponibilidade do RES	NGS1.05	Limitação de armazenamento	Art. 15º	
	Segurança de Dados	NGS1.07	Minimização de dados pessoais	Art. 6º (1)(2)(3)	Estratégia off-chain para armazenamento dos dados brutos.
Grupo 3	Dados clínicos Gerais	ESTR.04 SGED.01	Direito ao esquecimento	Art. 5º (XIV)	
	Problemas/condições de saúde e outras questões	FUNC.02			Imutabilidade e operações <i>append-only</i> .
Grupo 4	Médico-legal	FUNC.17			

03. Considerações Finais

CONSIDERAÇÕES FINAIS

Por meio deste **estudo preliminar**, compartilha-se, com **acadêmicos e profissionais** envolvidos com **e-health**, um **mapeamento de potencialidades e desafios** ao integrar a tecnologia blockchain para PEP. Assim, oportuniza-se o debate sobre o **uso de blockchain no contexto de PEP de forma alicerçada nos requisitos da SBIS e princípios da LGPD**.



Obrigada!

Dúvidas?

pamella.soares@aluno.uece.br



UNIVERSIDADE
ESTADUAL DO CEARÁ



Programa de Pós-Graduação
em Ciência da Computação



UNIVERSIDADE
FEDERAL DO CEARÁ

