



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 Alex Araújo (UFC - GESID),
Raphael Saraiva (UECE - PPGCC), Jerffeson Souza (UECE - PPGCC),
George Sousa (UECE - PPCCLIS) e Lúcia Duarte (UECE - PPCCLIS)



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]

Aplicações Descentralizadas

Contratos Inteligentes

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 <i>design</i>
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 pessoais	Art. 6º (1)(2)(3)	
			Direito ao esquecimento	Art. 5º (XIV)	
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02			Imutabilidade e operações <i>append-only</i> .
	Médico-legal	FUNC.17			

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de <i>design</i>
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. 6º (1)(2)(3)	Estratégia <i>off-chain</i> para armazenamento dos dados brutos.
	Gerais	SGED.01	Minimização de dados pessoais	Art. 6º (XVI)	
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02	Direito ao esquecimento	Art. 18º (XV)	Imutabilidade e operações <i>append-only</i> .
	Médico-legal	FUNC.17			

- Identificação as partes que interagem com a solução a fim de impedir o acesso de terceiros não-autorizados;
- Controle de acesso e as respectivas entidades habilitadas;
- Armazenamento de *hashs* e identificadores em bancos de dados tradicional ou distribuído;
- Modelagem por camadas.

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de <i>design</i>	
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. Imutabilidade e operações <i>append-only</i> .	
	Gerais	SGED.01	Minimização de dados Direito ao esquecimento	Art. 16º (V) Art. 17º		
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02	<div><ul style="list-style-type: none">- Nós da rede se conectam entre si e, assim, mantêm as réplicas das informações de maneira distribuída;- 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.</div>			
	Médico-legal	FUNC.17				

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de <i>design</i>
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. Imutabilidade e operações <i>append-only</i> .
	Gerais	SGED.01	Minimização de dados	Art. 15º Desafio de escalabilidade em blockchain para armazenar, por exemplo, um arquivo de mídia;	
Grupo 4	Problemas/condições de saúde e outras questões	FUNC.02	Direito ao esquecimento	Art. 15º Direito ao esquecimento vs. imutabilidade.	
	Médico-legal	FUNC.17			

ANÁLISE PRELIMINAR DOS REQUISITOS ADVINDOS DA SBIS E LGPD

	Requisitos da SBIS	Ref.	Princípios da LGPD	Ref.	Estratégias de <i>design</i>
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 Identificação dos responsáveis pelo tratamento	Art. 18º	
	Atores	FUNC.18			
Grupo 2	Disponibilidade do RES	NGS1.05	Integridade	Art. 6º (IV)(VII)	Estratégia <i>off-chain</i> para privacidade de dados sensíveis.
	Segurança de Dados	NGS1.07			
Grupo 3	Dados clínicos	ESTR.04	Limitação de armazenamento	Art. 15º	Armazenamento de <i>hash</i> imutável e auditável.
	Gerais	SGED.01	Minimização de dados pessoais	Art. 6º (1)(2)(3)	
Grupo 4			Direito ao esquecimento	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			

- 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.

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

