



Criptografia Aplicada à Conformidade Regulatória e à Proteção de Dados no Open Insurance

Câmara Brasileira de Economia Digital (camara-e.net)

**ANEXO I
PLANO DE TRABALHO**

Coordenação:
Ricardo Felipe Custódio

07/11/2025

1 DADOS CADASTRAIS

Instituição Concedente

Câmara Brasileira da Economia Digital (camara-e.net)

CNPJ: 04.481.317/0001-48

Av. Paulista, 2064. Conjunto 14, (Edifício Paulista)

CEP 01310-928 Consolação – São Paulo/SP

Contato: Maíra Hayashida

Telefone Contato: (11) 9 5342-0289

Instituição Gestora

Fundação de Amparo à Pesquisa e Extensão Universitária - FAPEU

CNPJ: 83.476.911/0001-17

Rua Delfino Conti, s/n

Campus Universitário UFSC

Bairro Trindade - Florianópolis/SC

CEP 88040-370

Contato: Geraldo Morgado Fagundes Filho

Telefone Contato: +55 (48) 3331-7408

E-mail:

Unidade Executora

Laboratório de Segurança em Computação - LabSEC

Parte Integrante do Departamento de Informática e Estatística - INE

Universidade Federal de Santa Catarina - UFSC,

Telefone Contato: (48) 3721-7546 (LabSEC)

E-mail: labsec@inf.ufsc.br

Coordenador do Projeto

Prof. Dr. Ricardo Felipe Custódio

CPF: 485.981.609-97

SIAPE: 1160094

E-mail: ricardo.custodio@ufsc.br

Lotação: Departamento de Informática e Estatística - INE

Telefone Contato: (48) 3721-7546

2 PROJETO DE EXTENSÃO

Título do Projeto: Criptografia Aplicada à Conformidade Regulatória e à Proteção de Dados no Open Insurance

Período de Execução:

O projeto terá duração de 12 meses, contados a partir da data de assinatura do contrato, que marcará o início de sua execução.

Objeto:

Desenvolver um protocolo criptográfico de segurança para o ecossistema brasileiro de Open Insurance que integre criptografia clássica e pós-quântica (PQC), contemplando tecnologias de preservação da privacidade e fortalecendo a soberania tecnológica nacional no setor. O projeto abrangerá desde a modelagem sistemática de ameaças, considerando vetores de ataque clássicos e quânticos aplicáveis ao contexto regulatório brasileiro e aos requisitos da LGPD, até a concepção de uma arquitetura criptográfica híbrida que combine algoritmos clássicos robustos com primitivas pós-quânticas, integrando mecanismos adequados ao compartilhamento seguro de dados sensíveis entre instituições.

O desenvolvimento incluirá a implementação de uma prova de conceito do protocolo proposto, seguida de validação experimental por meio de testes de desempenho e de análise de resistência a ataques conhecidos, com mensuração objetiva dos ganhos de segurança, dos custos computacionais e da viabilidade de implantação no ecossistema real. O projeto prevê ainda ações de transferência de conhecimento, incluindo produção de documentação técnica, especificações abertas e capacitação de profissionais do setor, visando reduzir a dependência de soluções proprietárias estrangeiras e fomentar competências nacionais em criptografia aplicada, contribuindo para o desenvolvimento tecnológico autônomo do Brasil no contexto do Open Insurance e preparando o setor para as ameaças quânticas da próxima década.

Justificativa da Proposição:

O Open Insurance brasileiro representa uma transformação digital fundamental do setor segurador nacional, regulamentado pelas Resoluções CNSP 415/2021 e pela Circular SUSEP 635/2021. A implementação desta plataforma facilita o compartilhamento de dados entre entidades, visando à maior personalização de serviços e ao fomento da competitividade setorial. No entanto, este avanço também traz desafios consideráveis em segurança da informação, especialmente na proteção de dados sensíveis e na garantia de transações seguras.

A atividade proposta é de extrema relevância estratégica para o Brasil, pois aborda a necessidade urgente de desenvolver capacidades tecnológicas nacionais para o Open Insurance. Atualmente, o ecossistema brasileiro depende significativamente de soluções tecnológicas desenvolvidas por fornecedores estrangeiros, criando uma dependência tecnológica crítica em infraestrutura essencial ao sistema financeiro

nacional. O desenvolvimento de protocolos criptográficos nacionais representa um passo fundamental para a soberania tecnológica do país neste setor estratégico.

2.1 Metas

Número	Meta	Indicador
M1	Mapear os riscos e os tipos de ataque que podem afetar o Open Insurance hoje e no futuro (incluindo a computação quântica).	Documento de riscos revisado e publicado; registro dos encontros de validação com especialistas.
M2	Testar, em protótipo, como técnicas de proteção de dados (ex.: anonimização/pseudonimização) funcionam em conjunto com a criptografia pós-quântica.	Protótipo funcionando e relatório com compatibilidades e impacto em velocidade/uso do sistema publicado.
M3	Producir conhecimento técnico e científico (artigos, relatórios e materiais de capacitação).	Publicações e materiais formativos disponibilizados (com links/DOIs ou registros institucionais).
M4	Estabelecer parcerias com stakeholders do setor público e privado	Reuniões técnicas registradas e memorandos de entendimento/atas assinados.

2.2 Resultados esperados

Número	Resultado esperado
R1	Documento de riscos e ameaças ao Open Insurance (clássicos e quânticos).
R2	Protótipo que integra técnicas de proteção de dados com criptografia pós-quântica.
R3	Materiais de transferência de conhecimento (guia prático/minicurso) para quem vai usar.
R4	Artigos científicos publicados em periódicos e eventos nacionais/internacionais.
R5	Capacitação de pesquisadores e profissionais para atuação em Open Insurance.
R6	Estreitamento de laços entre universidades, SUSEP, seguradoras e empresas de tecnologia.

3 Metodologia

O projeto será conduzido em múltiplas atividades, definidas com base no plano de trabalho. Cada atividade abaixo possui foco direto nas metas e indicadores do plano.

- Atividade 1: Levantamento bibliográfico direcionado; mapeamento regulatório (LGPD/SUSEP) e tecnológico; inventário de ativos e fluxos do Open Insurance; definição dos critérios de aceite (latência, disponibilidade, rastreabilidade) e dos referenciais criptográficos a considerar (clássicos e pós-quânticos);
- Atividade 2: Desenvolvimento do módulo de criptografia pós-quântica (PQC); integração mínima ao fluxo-alvo; coleta de métricas de desempenho (baseline x pós-quântico);
- Atividade 3: Mapeamento dos riscos e dos tipos de ataque que podem afetar o Open Insurance hoje e no futuro (incluindo a computação quântica);
- Atividade 4: Testes, em protótipo, de como técnicas de proteção de dados (ex.: anonimização/pseudonimização) funcionam em conjunto com a criptografia pós-quântica;
- Atividade 5: Produção de conhecimento técnico e científico (artigos, relatórios e materiais de capacitação).

A metodologia seguirá boas práticas internacionais (PRISMA para revisões sistemáticas; metodologias ágeis para desenvolvimento de protótipos; avaliação de usabilidade segundo ISO 9241 e ABNT NBR 9241-210).

4 CRONOGRAMA DE EXECUÇÃO

Número	Fase/etapa	Duração	
		Início	Término
F1	Levantamento de requisitos, mapeamento de ativos e fluxos do Open Insurance e arquitetura preliminar do protocolo híbrido.	Mês 1	Mês 2
F2	Modelagem de riscos e ameaças (clássicos e quânticos) com validação por especialistas e versão revisada do documento.	Mês 3	Mês 5
F3	Protótipo integrando técnicas de proteção de dados (ex.: anonimização/pseudonimização) com primitivas PQC e medição de impacto.	Mês 6	Mês 10
F4	Entrega final, revisão técnica, documentação e publicação dos resultados.	Mês 11	Mês 12

5 Lista de bens e serviços próprios da UFSC utilizados no projeto

Item	Bens / serviços
I1	Laboratório de Segurança em Computação – LabSec/UFSC.
I2	Servidores e storage institucionais da UFSC.
I3	Ambiente de virtualização e containers (Docker/Kubernetes).
I4	Espaços físicos e recursos administrativos da UFSC (salas de reunião, secretaria, apoio técnico) para a gestão e acompanhamento do projeto.

6 – Cronograma de Desembolso (R\$)

O valor total para a execução do projeto fica estabelecido em R\$ 103.800,00 (cento e três mil e oitocentos reais), a ser pago em 12 parcelas mensais de R\$ 8.650,00 (oito mil seiscientos e cinquenta reais), conforme tabela abaixo.

jan/2026	fev/2026	mar/2026	abr/2026	mai/2026	jun/2026
8.650,00	8.650,00	8.650,00	8.650,00	8.650,00	8.650,00
jul/2026	ago/2026	set/2026	out/2026	nov/2026	dez/2026
8.650,00	8.650,00	8.650,00	8.650,00	8.650,00	8.650,00

Prof. Dr. Ricardo Felipe Custódio
Coordenador do Projeto