Processo nº 00100.002777/2023-85

II - PLANO DE TRABALHO DO TERMO DE EXECUÇÃO DESCENTRALIZADA Nº 001/2023

PRIMEIRO TERMO ADITIVO

1. DADOS CADASTRAIS DA UNIDADE DESCENTRALIZADORA

a) Unidade Descentralizadora e Responsável

Nome do órgão descentralizador: INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI

Nome da autoridade competente: Enylson Flávio Martinez Camolesi

Número do CPF: [redacted]

Nome da Unidade Responsável pelo acompanhamento da execução do objeto do TED:

CGOPE/DINFRA Identificação do Ato que confere poderes para assinatura: PORTARIAS DE 24 DE OUTUBRO DE 2022, Nº 1229 , Publicada no DOU em: 24/10/2022 | Edição: 202-A | Seção: 2-ExtraA| Página: 1

a) UG SIAFI

Número e Nome da Unidade Gestora - UG que descentralizará o crédito: 203001 - INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Número e Nome da Unidade Gestora - UG Responsável pelo acompanhamento da execução do objeto do TED: Não se aplica

2. DADOS CADASTRAIS DA UNIDADE DESCENTRALIZADA

a) Unidade Descentralizada e Responsável

Nome do órgão ou entidade descentralizada: UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Nome da autoridade competente: IRINEU MANOEL DE SOUZA

Número do CPF: [redacted]

Nome da Secretaria/Departamento/Unidade Responsável pela execução do objeto do TED: Centro

Tecnológico - CTC / Departamento de Informática e Estatística - INE / Laboratório de Segurança em

Computação - LabSEC

b) UG SIAFI

Número e Nome da Unidade Gestora - UG que receberá o crédito: 153163 - UNIVERSIDADE FEDERAL DE SANTA CATARINA

Número e Nome da Unidade Gestora - UG Responsável pela execução do objeto do TED: Não se aplica

3. OBJETO

O objeto do presente Projeto de Pesquisa consiste no estudo para a consolidação das tecnologias de gerenciamento de certificados digitais no Brasil, com ênfase na ameaça que os computadores quânticos representam para a segurança eletrônica.

São propostas implementações de prova de conceito suportando novos algoritmos denominados pós-quânticos, bem como a análise de como estes algoritmos influenciam na certificação digital no contexto da ICP-Brasil.

O projeto também engloba a demanda de aprimoramento, face a eventuais inovações tecnológicas, dos protótipos de Sistemas de Gerenciamento de Certificados (SGC) no escopo da ICP-Brasil, assim como na plataforma de Assinaturas Eletrônicas Avançadas mantida pelo ITI, em parceria junto a SGD, em conformidade com a Lei Nº 14.063, de 23 de setembro de 2020.

Serão realizados estudos de viabilidade com desenvolvimento de artefatos de software e elaborar-se-ão relatórios técnicos para a evolução destas plataformas.

4. DESCRIÇÃO DAS AÇÕES E METAS A SEREM DESENVOLVIDAS NO ÂMBITO DO TED

As atividades desenvolvidas no projeto serão divididas de acordo com os objetivos específicos supracitados. São estabelecidas três trilhas conforme segue. A primeira trata do aprimoramento dos protótipos de Sistemas de Gerenciamento de Certificados (SGC) no âmbito da plataforma de Assinaturas Eletrônicas Avançadas mantida pelo ITI em parceria junto a SGD. A segunda trata do suporte aos novos algoritmos criptográficos pós-quânticos. A terceira trilha lista metas com atividades comuns às demais.

Tabela 1 - Atividades previstas e cronograma

1	Aprimoramento dos componentes/sistemas que integram a Plataforma de Assinatura Eletrônica Avançada.
1.A	Estudo de viabilidade e proposta de inclusão da funcionalidade de compartilhamento de documentos entre cidadãos para assinatura no Portal de Assinatura Eletrônica;
1.B	Estudo sobre viabilidade de adoção de mecanismos para tratar a preservação de assinaturas eletrônicas avançadas;
1.C	Estudo técnico de proxy camada 7 do protocolo TTLV;
1.D	Estudo para implementação de API para assinaturas em lotes usando Certificado Digital Avançado;
1.E	Estudo sobre o fornecimento de uma API compatível com o padrão mundial Cloud Signature Consortium para consumo da Assinatura Avançada;
1.F	Estudo, projeto e implantação de metodologia para realização de deploy seguro dos componentes que integram a solução da Assinatura Eletrônica Avançada;
1.G	Estudo e avaliação da viabilidade técnica e prática do uso de algoritmos criptográficos Pós-Quânticos no contexto das Assinaturas Eletrônicas avançadas;
1.H	Disponibilização de infraestrutura computacional, espaço em DataCenter e conectividade com internet, para desenvolvimento dos estudos, realização de avaliações e demonstrações associadas a Certificados Digitais Avançados;
1.I	Estudar formas de coletar e expor ao cidadão o histórico de assinaturas
1.J	Estudar como expandir a API para permitir que órgãos integrados escolham assinar com PSCs ICP-Brasil ou com a Avançada
2	Suporte aos novos algoritmos criptográficos pós-quânticos.
2.A	Relatório técnico de levantamento de estado da arte de algoritmos pós-quânticos;
2.B	Relatório técnico dos sistemas gerenciadores de certificados (Ywapa, Ywyra e Hawa), bibliotecas e sistemas operacionais que devem ser adaptados para suportar algoritmos pós-quânticos;
2.C	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL 1.1.1-stable;
2.D	Versão Alfa Protótipo dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos;
2.E	Relatório técnico sobre a integração das bibliotecas Pós-quânticas para os aplicativos baseados na linguagem Java;
2.F	Relatório técnico sobre a integração da biblioteca OQS-OpenSSL com a biblioteca Libcryptosec para prover o suporte a algoritmos pós-quânticos (Ywapa, Ywyra, Hawa);

2.G	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL 3.x;
2.H	Protótipo da biblioteca Libcryptosec com suporte a algoritmos pós-quânticos através da integração com a biblioteca OQS-OpenSSL. (Ywapa, Ywyra, Hawa);
2.I	Protótipo Hawa com suporte a algoritmos Pós-quânticos;
2.J	Atualização do sistema operacional do software Ywapa, Ywyra e Hawa para RedHat Enterprise na última versão disponível;
2.K	Protótipo em Beta dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos;
2.L	Relatório técnico sobre formas de autenticação pós-quânticas que podem ser usadas nos softwares Sistemas Gerenciadores de Certificados (SGC - Ywapa, Ywyra e Hawa);
2.M	Relatório sobre a adaptação dos softwares SGC para um ambiente pós-quântico;
2.N	Pacote com a versão atualizada dos protótipos dos programas do SGC com suporte a algoritmos pós-quânticos (Ywapa, Ywyra e Hawa);
3	Atividades Comuns.
3.A	Adaptação normativa;
3.B	Procedimento regular, periódico de transferência de conhecimento e tecnologia, incluindo documentação técnica;
3.C	Suporte técnico e atividades de manutenção corretiva e ajustes

A Tabela 2 descreve os demais entregáveis e seus prazos máximos de entrega. Ressalta-se que os entregáveis no formato de software, no ato da entrega, possuirão nível de maturidade de acordo com o estimado abaixo. O nível é baseado no método TRL (Technology readiness level), padronizado na ISO 16290:2013. A definição acerca da Propriedade Intelectual dos entregáveis será definida em Instrumento Próprio.

Tabela 2: Cronograma dos entregáveis do projeto

Item	Descrição Entrega		Formato
AVANÇADA			
1.A	Estudo de viabilidade e proposta de inclusão da funcionalidade de compartilhamento de documentos entre cidadãos para assinatura no portal	jun./24	Relatório técnico e artefatos de software (TRL 6)
1.B	Estudo sobre viabilidade de adoção de mecanismos para tratar a preservação de assinaturas eletrônicas avançadas	maio./26	Relatório técnico e artefatos de software (TRL 6)
1.C	Estudo técnico de proxy camada 7 do protocolo TTLV	dez./25	Relatório técnico e artefatos de software (TRL 6)
1.D	Estudo para implementação de API para assinaturas em lotes usando Certificado Digital Avançado	abr./26	Relatório técnico e artefatos de software (TRL 6)
1.E	Estudo sobre o fornecimento de uma API compatível com o padrão mundial Cloud Signature Consortium para consumo da Assinatura Avançada	out./25	Relatório técnico e artefatos de software (TRL 6)
1.F	Estudo, projeto e implantação de metodologia para realização de deploy seguro dos componentes que integram a solução da Avançada	jan./25	Relatório técnico e artefatos de software (TRL 6)
1.G	Estudo e avaliação da viabilidade técnica e prática do uso de algoritmos criptográficos Pós Quânticos	ago./25	Relatório técnico e artefatos de software (TRL 3)
1.H	Disponibilização de infraestrutura computacional, espaço em DataCenter e conectividade com internet, para desenvolvimento dos estudos, realização de avaliações e demonstrações associadas a Certificados Avançados	Contínuo	-

1.I	Estudar formas de coletar e expor ao cidadão o histórico de assinaturas	Dez/24	Artefatos de software (TRL 6)
1.J	Estudar como expandir a API para permitir que órgãos integrados escolham assinar com PSCs ICP-Brasil ou com a Avançada	maio/25	Relatório técnico e artefatos de software (TRL 6)
SGC			
2.A	Relatório técnico de levantamento de estado da arte de algoritmos pós-quânticos.	fev./24	Relatório
2.B	Relatório técnico dos sistemas, bibliotecas e sistemas operacionais que devem ser adaptados para suportar algoritmos pós-quânticos. (Ywapa, Ywyra e Hawa)	set./24	Relatório
2.C	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL 1.1.1-stable.	fev./25	Software (TRL-7)
2.D	Versão Alfa Protótipo dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.	fev./25	Software (TRL-3)
2.E	Relatório técnico sobre a integração das bibliotecas Pós-quânticas para os aplicativos baseados na linguagem Java.	set./25	Relatório
2.F	Relatório técnico sobre a integração da biblioteca OQS-OpenSSL com a biblioteca Libcryptosec para prover o suporte a algoritmos pós quânticos. (Ywapa, Ywyra, Hawa)	set./25	Relatório
2.G	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL 3.x.	fev./25	Software (TRL-7)
2.H	Protótipo da biblioteca Libcryptosec com suporte a algoritmos pós-quânticos através da integração com a biblioteca OQS-OpenSSL. (Ywapa, Ywyra, Hawa)	dez./25	Software (TRL-5)
2.I	Protótipo Hawa com suporte a algoritmos Pós-quânticos.	fev./26	Software (TRL-5)
2.J	Atualização do sistema operacional do software Ywapa, Ywyra e Hawa para RedHat Enterprise na última versão disponível.	fev./27	Software (TRL-5)
2.K	Protótipo em Beta dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.	fev./27	Software (TRL-5)
2.L	Relatório técnico sobre formas de autenticação pós-quânticas que podem ser usadas nos softwares SGC. (Ywapa, Ywyra e Hawa)	fev./27	Relatório
2.M	Relatório sobre a adaptação dos softwares SGC para um ambiente pós-quantum.	set./27	Relatório
2.N	Pacote com a versão atualizada dos protótipos dos programas do SGC com suporte a algoritmos pós-quânticos. (Ywapa, Ywyra e Hawa)	set./27	Software (TRL-7)
AVANÇADA / SGC			
3.A	Adaptações normativas.	Contínuo	Software (TRL-7)
3.B	Procedimento regular, periódico de transferência de conhecimento e tecnologia, incluindo documentação técnica.	Contínuo	-
3.C	Suporte técnico e atividades de manutenção corretiva e ajustes	Contínuo	-

No que segue detalha-se para cada uma das atividades previstas, descreve-se, abaixo, o seu respectivo detalhamento.

1.A. Estudo de viabilidade e proposta de inclusão da funcionalidade de compartilhamento de documentos entre cidadãos para assinatura no portal.

Nesta etapa, será realizado um estudo de diferentes estratégias de UX no Portal de Assinaturas da Avançada para viabilizar a coleta de assinaturas em um mesmo documento. Observou-se que há um padrão muito usual nos usuários do Portal de Assinatura, no qual eles sobem um documento, realizam a assinatura, fazem o download, enviam o documento a outra pessoa que repete o processo. Objetiva-se propor uma solução que permita a otimização deste fluxo de compartilhamento de documentos e coleta de assinaturas.

1.B. Estudo sobre viabilidade de adoção de mecanismos para tratar a preservação de assinaturas eletrônicas avançadas.

Nesta etapa será realizado um levantamento de políticas de assinaturas atualmente em uso dentro do contexto da Infraestrutura de Chaves Públicas Qualificadas brasileira (ICP-Brasil), normatizada pelo ITI através do DOC-ICP-15 [16]; assim como perfis padronizados na ETSI TS 102 778 e outros modelos de preservação de documentos eletrônicos relacionados. A partir deste estudo será elaborado parecer sobre aspectos a serem levados em consideração na normatização de mecanismos para tratar da preservação de assinaturas eletrônicas avançadas. Em paralelo, será realizado um estudo sobre a forma de integrar tais mecanismos com o Assinador usado pelo ITI para a Assinatura Eletrônica Avançada. Um protótipo será elaborado para validar a solução proposta através da confecção destas assinaturas no Portal de Assinatura.

1.C. Estudo técnico de proxy camada 7 do protocolo TTLV

A comunicação entre aplicações e HSMs através do protocolo KMIP pode ser realizada utilizando diferentes protocolos de comunicação: JSON, XML, e TTLV. O protocolo TTLV é o que apresenta melhor performance, entretanto elementos de proxy camada 7 não existem para TTLV, sendo necessário recorrer a proxy camada 4. Entretanto proxy camada 4 trabalham a nível de conexão, sendo a distribuição de carga entre HSMs e conexão e desconexão de novos equipamentos não muito adequada. Nesta etapa do projeto, propõem o estudo e propostas sobre como adaptar software e/ou hardware para trabalhar o protocolo KMIP codificado em TTLV em camada 7.

1.D. Estudo para implementação de API para assinaturas em lotes usando Certificado Digital Avançado.

Nesta etapa, será realizado um estudo de diferentes estratégias e APIs para viabilizar o uso de certificado digital avançado para assinatura de mais de um documento simultaneamente. Será realizado um estudo das APIs de assinatura já existentes no DOC ICP-17.01 e CSC e serão propostas alterações e evoluções na API para suportar a assinatura em Lote. Deverá ser considerada a possibilidade da API de assinatura em lote suportar altos volumes sem impactar a operação normal, avaliando-se a possibilidade de uma API de assinatura de lote assíncrona que usará a capacidade ociosa da infraestrutura em horários de subutilização, evitando a deterioração do serviço de assinatura síncrono atualmente fornecido ela API da Assinatura Avançada.

1.E. Estudo sobre o fornecimento de uma API compatível com o padrão mundial Cloud Signature Consortium para consumo da Assinatura Avançada.

Nesta etapa, será realizado um estudo da viabilidade técnica de fornecer um API compatível com o padrão mundial Cloud Signature Consortium para realização de assinaturas avançadas. Isto viabilizará aplicações compatíveis com Cloud Signature Consortium utilizando serviços de assinatura digital com Certificados Digitais Avançados.

1.F. Estudo, projeto e implantação de metodologia para entrega contínua e realização de deploy seguro dos componentes que integram a solução da Avançada.

A solução de Certificação Digital Avançada operada pelo ITI em parceria com a SGD é composta por diferentes componentes de software que se comunicam entre si para fornecimento do serviço ao cidadão. Estes componentes compõem uma arquitetura distribuída complexa, sendo que a evolução segura do projeto, por meio de deploy de novas versões destes componentes é algo bastante complexo. Nesta etapa, será realizado o estudo de cada um dos componentes, e será projeto esteiras automatizadas para gerenciamento do ciclo de vida da solução, desde de sua construção, passando pelo deploy de atualizações em homologação até o deploy no ambiente de produção. Com isso busca-se evitar que erros humanos ocasionam paradas no fornecimento do serviço.

1.G. Estudo e avaliação da viabilidade técnica e prática do uso de algoritmos criptográficos Pós Quânticos.

Com o avanço tecnológico, espera-se que em um futuro algoritmos criptográficos clássicos como RSA e Ed25519 deixem de ser algoritmos seguros. De forma a melhor proteger, propõe-se nessa meta realizar um estudo sobre a viabilidade técnica da confecção de certificados digitais e algoritmos de assinatura usando algoritmos criptográficos pós-quânticos, incluindo avaliação do nível de suporte destes algoritmos nos equipamentos atualmente disponíveis dentro da

infraestrutura do ITI.

1.H. Disponibilização de infraestrutura computacional, espaço em DataCenter e conectividade com internet, para desenvolvimento dos estudos, realização de avaliações e demonstrações associadas à Certificados Avançados.

Como contrapartida da Universidade, durante o desenvolvimento do projeto, será realizada a cessão de espaço físico dentro da sala-cofre operada pela UFSC para correto acondicionamento da estrutura física de hardware HSM e Servidores para hospedagem de:

(1) Ambiente de Testes de Bancada;

(2) Equipamentos HSM para desenvolvimento;

(3) Ambiente de demonstração e validação de protótipo.

Isso envolve:

- espaço físico de racks em ambiente seguro de sala-cofre atendendo aos requisitos devidos de provimento de energia elétrica estabilizada, no-breaks para operação ininterrupta, ambiente climatizado e segurança;

- infraestrutura lógica com conectividade de alta disponibilidade e tolerante à falhas;

- monitoramento do ambiente com equipe dedicada de técnicos.

Além disso, visto a previsão de fornecimento de conectividade com a Internet com alta disponibilidade, redundância e segurança, e os estudos a serem desenvolvidos no contexto do Entregável "C - Estudo técnico de proxy camada 7 do protocolo TTLV", a Universidade prevê adquirir um Firewall de Rede em 2024, por meio de recursos próprios, no montante aproximado de US$ 850.000,00 (oitocentos e cinquenta mil dólares americanos). Com isto, busca-se:

(1) garantir a qualidade da conexão com a Internet em alta velocidade (100 gbps) ao Ambiente de Teste de Bancada, HSMs e Ambiente de Demonstração; e

(2) avaliar características de análise de pacotes em camada L7, em especial o protocolo TTLV.

Ao fim do projeto, o equipamento será integrado à infraestrutura da Universidade para fornecer redundância e alta disponibilidade, viabilizando melhor qualidade de prestação de serviços a toda a comunidade universitária.

1.I. Estudar formas de coletar e expor ao cidadão o histórico de assinaturas

Nesta etapa, será realizado um estudo de como coletar e expor ao cidadão o histórico de assinaturas realizadas com o seu Certificado Avançado e, também, com o Certificados Digitais ICP-Brasil realizadas por meio de Prestadores de Serviços de Confiança. Objetiva-se propor uma solução que permita ao cidadão realizar a consulta de forma simples e intuitiva no Portal para todas as assinaturas realizadas tanto via Portal quanto via API. Essa informação também deve poder ser disponibilizada e consultada por aplicações autorizadas para automação de processos entre ITI e SGD por intermédio de uma API.

1.J. Estudar como expandir a API para permitir que órgãos integrados escolham assinar com PSCs ICP-Brasil ou com a Avançada

Nesta etapa, será realizado um estudo sobre meios disponíveis para alterar a API da Avançada de tal forma que órgãos integrados possam utilizar o fluxo de assinatura do Portal, ou seja, o cidadão possa escolher qual o certificado Digital será usado para realizar a assinatura: o Certificado Avançado ou Certificados disponíveis em Provedores de Serviços de Confiança da ICP-Brasil. Espera-se que seja disponibilizado, desta forma, a mesma experiência disponível no Portal aos Órgãos já integrados via API. Esta API deve ser opt-in, ou seja, o órgão integrador pode escolher entre o fluxo exclusivo da assinatura avançada ou o fluxo integrando o certificado ICP-Brasil dos PSCs.

2.A. Relatório técnico de levantamento de estado da arte de algoritmos pós-quânticos.

Nesta etapa, será realizado um levantamento do estado da arte de diferentes algoritmos de assinatura pós-quântica. Especificamente iremos comparar a viabilidade destes algoritmos nos quesitos: (i) velocidade de geração de par de chaves; (ii) velocidade de geração de assinatura; (iii) velocidade da verificação de assinatura; (iv) tamanho da chave pública; (iv) tamanho da chave privada; (iv) tamanho da assinatura. Objetiva-se aderir aos algoritmos que permitam uma combinação otimizada destes tópicos.

2.B. Relatório técnico dos sistemas, bibliotecas e sistemas operacionais que devem ser adaptados para suportar algoritmos pós-quânticos. (Ywapa, Ywyra, e Hawa).

Realizar um levantamento das possibilidades e necessidades de adaptação de cada um dos componentes dos projetos para utilização do novo algoritmo definido na tarefa 2.B. Para isso, uma busca detalhada nos códigos das bibliotecas utilizadas, bem como no código da própria aplicação, será executada para identificar os pontos em que deverão ser realizadas mudanças.

2.C. Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL *1.1.1-stable*.

Os algoritmos utilizados nos softwares Ywapa, Ywyra, e Hawa C++ são providos pela biblioteca libcriptosec e pelos motores criptográficos dos HSMs, que funcionam como uma ligação entre os sistemas do SGC e a biblioteca de criptografia OpenSSL. Atualmente as aplicações em C++ do SGC utilizam a versão 1.0.2 do OpenSSL. A atualização é necessária devido às melhorias provenientes das versões mais novas do OpenSSL(1.1.1 e 3.0.1). Adicionalmente, este é um passo intermediário necessário para adaptação da biblioteca OpenQuantumSafe-OpenSSL (OQS-OpenSSL), responsável pela implementação otimizada dos algoritmos pós-quânticos.

2.D. Versão Alfa Protótipo dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.

Entrega de um pacote com todos os protótipos em fase Alfa interoperando para geração de uma cadeia pós-quântica utilizando apenas aplicações SGC no Sistema Operacional RedHat 7.4 usando a versão Alfa da librcryptosec adaptada ao OpenQuantumSafe-OpenSSL (OQS-OpenSSL) na versão 1.1.1 e BouncyCastle com suporte em versão Alfa a algoritmos criptográficos Pós-Quânticos.

2.E. Relatório técnico sobre a integração das bibliotecas Pós-quânticas para os aplicativos baseados na linguagem Java.

Realizar um levantamento das possibilidades e necessidades de adaptação da biblioteca Bouncycastle para sua integração com bibliotecas de gerência de algoritmos pós-quânticos, e então fornecer o suporte fundamental aos softwares do projeto SGC que usufruem da linguagem java. Para isso, será feita uma busca detalhada nos códigos para identificar os pontos em que serão realizadas mudanças.

2.F. Relatório técnico sobre a integração da biblioteca OQS-OpenSSL com a biblioteca Libcryptosec para prover o suporte a algoritmos pós quânticos. (Ywapa, Ywyra, Hawa).

Realizar um levantamento das possibilidades e necessidades de adaptação da biblioteca libcryptosec para sua integração com a OQS-OpenSSL, e então fornecer o suporte aos algoritmos que serão utilizados nos softwares do projeto SGC. Para isso, será executada uma busca detalhada do código para identificar os pontos em que será necessário realizar mudanças.

2.G. Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL *3.x*.

Atualizar a libcryptosec para possibilitar o uso do OpenSSL 3.x é mais um dos passos intermediários necessários para a integração com a OQS-OpenSSL e atingir a finalidade de utilizar algoritmos pós-quânticos. Devido ao processo de atualização do OpenSSL, faz-se necessária a atualização para o OpenSSL 1.1.1 antes da atualização para o OpenSSL 3.x. Adicionalmente, o suporte de algoritmos pós-quânticos na versão OQS-OpenSSL 1.1.1 ainda é maior do que na versão 3.x.

2.H. Protótipo da biblioteca Libcryptosec com suporte a algoritmos pós-quânticos através da integração com a biblioteca OQS-OpenSSL. (Ywapa, Ywyra, Hawa)

A criação de um protótipo é necessária para identificar os problemas e dificuldades da implementação na prática e elaborar diferentes métodos para solucionar eventuais problemas mais complicados que vão além da adaptação de bibliotecas com suporte a algoritmos pós-quânticos. Neste ponto, comparações entre implementações em OQS-OpenSSL 1.1.1 e 3.x também serão feitas e os resultados divulgados em um relatório posteriormente.

2.I. Protótipo Hawa com suporte a algoritmos Pós-quânticos.

Assim como no item 2D, um protótipo da parte da aplicação Hawa feita em Java terá sua versão criada para detecção de possíveis problemas e dificuldades da transição para um cenário pós-quântico. Testes e resultados serão realizados usando este protótipo e divulgados em um relatório posterior.

2.J. Atualização do sistema operacional do software Ywapa, Ywyra e Hawa para RedHat 9.

Como os softwares do projeto SGC são desenvolvidos para um sistema operacional específico, há necessidade de projetá-los com base nas versões e bibliotecas que são disponibilizadas. Deste modo, a utilização de novas versões da biblioteca OpenSSL requer uma atualização de sistema e consequentemente atualização dos softwares para se adaptarem as novas versões das bibliotecas disponibilizadas. Este item requer a atualização de várias bibliotecas usadas pelo SGC. Especificamente, as bibliotecas mais críticas que necessitam de atualização são: (i) PostgreSQL, p11, opensc, e authid.

2.K. Protótipo em Beta dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.

Entrega de um pacote com todos os protótipos interoperando para geração de uma cadeia pós-quântica utilizando apenas aplicações SGC no Sistema Operacional RedHat 7.4 usando a versão Beta da librcryptosec adaptada ao OpenQuantumSafe-OpenSSL (OQS-OpenSSL) na versão 3.0.1 e BouncyCastle com suporte em versão Beta a algoritmos criptográficos Pós-Quânticos.

2.L. Relatório técnico sobre formas de autenticação pós-quânticas que podem ser usadas nos softwares SGC. (Ywapa, Ywyra, e Hawa)

A mudança para um cenário pós-quântico não depende apenas de algoritmos de assinatura, mas de processos presentes nas cerimônias em geral. Atualmente, o processo de autenticação depende de SmartCards. Este relatório detalha o desafio técnico de se implementar uma autenticação pós-quântica através de SmartCards com suporte a algoritmos pós-quânticos e a possibilidade de alternativas que independem de Smart Cards.

2.M. Relatório sobre a adaptação dos softwares SGC para um ambiente pós-quantum.

Nesta etapa será dado início a criação de um documento com detalhes das mudanças realizadas em cada um dos softwares do projeto SGC. Este manual é importante para explicar o novo fluxo das operações, como utilizá-las e esclarecer a necessidade dessas alterações. Este documento explicita todas as mudanças que foram realizadas ao longo do projeto.

2.N. Pacote com a versão atualizada dos protótipos dos programas do SGC com suporte a algoritmos pós-quânticos. (Ywapa, Ywyra, e Hawa)

Após realizar todas as alterações necessárias, tanto nos softwares, quanto no sistema operacional (RedHat 9.x), passar por uma minuciosa etapa de testes e correção de erros, geração de documentos e manuais explicando todas as mudanças realizadas, as novas versões das aplicações estão aptas para serem utilizadas em produção. Para isso, será disponibilizado o pacote para instalação da nova aplicação com todas as dependências necessárias.

3.A. Adaptações Normativas.

Concomitante à atualização dos softwares para suportar algoritmos pós-quânticos, é disponibilizado suporte para os aplicativos já em produção do SGC (Ywapa, Ywyra, e Hawa), com vistas a melhorias e correções necessárias.

3.B. Procedimento regular, periódico de transferência de conhecimento e tecnologia

É previsto durante o desenvolvimento do presente de trabalho, de forma contínua, a realização de workshops para a transferência de conhecimento e tecnologia para a equipe técnica do ITI. Estes Workshops devem ocorrer de forma periódica e regular, a cada 6 (seis) meses, durante o desenvolvimento da TED visando apresentar e discutir os produtos e entregáveis já desenvolvidos e em desenvolvimento. Estes eventos ocorrerão preferencialmente de forma online. Caso haja interesse por parte do ITI, é possível realizar a atividade presencialmente, sendo de responsabilidade do ITI os custos com passagens e diárias referentes ao deslocamento das equipes.

3.C. Suporte técnico e atividades de manutenção corretiva e ajustes

É previsto durante o desenvolvimento do presente de trabalho, de forma contínua, a realização de atividades de suporte técnico às equipes do ITI e da SGD, assim como manutenção corretivas e pequenos ajustes em componentes da solução para resolução de bugs reportados pelo ITI. O resultado da atividade corretiva/ajuste não altera a Propriedade Intelectual do componente alvo da atividade de correção, ou seja, caso o componente que necessite de manutenção seja de propriedade da UFSC, o componente continuará nesta situação. Esta é uma atividade contínua, solicitada sob demanda pelo ITI. Será alocada um máximo de 300 horas-homem para esta atividade durante a vigência do projeto.

5. JUSTIFICATIVA E MOTIVAÇÃO PARA CELEBRAÇÃO DO TED:

Visão Geral

Este documento, elaborado pelo Laboratório de Segurança em Computação (LabSEC) [1] da Universidade Federal de Santa Catarina (UFSC), apresenta uma proposta de pesquisa e desenvolvimento com o objetivo de buscar soluções para o aprimoramento da plataforma de Assinaturas Eletrônicas Avançadas mantida pelo ITI, em parceria junto a SGD, em conformidade com a Lei Nº 14.063, de 23 de setembro de 2020, bem como para melhorar a usabilidade do conjunto de Sistemas de Gerenciamento de Certificados Digitais da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), chamados Ywapa, Ywyra, e Hawa.

Adicionalmente, entre os objetivos deste projeto está a preparação para o eventual cenário pós-quântico para o qual a ICP-Brasil deve estar preparada antes que o mesmo aconteça.

Em linhas gerais, objetiva-se a análise da adição de algoritmos pós-quânticos nos aplicativos SGC, a avaliação de eventuais adaptações normativas para acompanhamento fiel das

atividades propostas, bem como o estudo de utilização de alternativas pós-quânticas nos processos e cerimônias usadas na ICP-Brasil.

O LabSEC é reconhecido como um dos maiores centros de pesquisa científica e tecnológica na área de certificação digital no país. Desde a sua criação em 1999, já foram desenvolvidos mais de 150 trabalhos de conclusão de curso de graduação, dissertações de mestrado e teses de doutorado relacionados ao tema certificação digital e suas aplicações [2, 3, 4, 5]. Foram mais de 50 artigos científicos publicados nos mais renomados eventos e periódicos científicos, nacionais e internacionais. O LabSEC tem participado dos dois maiores esforços acadêmicos em atividades relacionadas ao desenvolvimento de tecnologia nacional para a gestão do ciclo de vida de chaves criptográficas: projetos ICPEDU [6] e João de Barro [7].

O LabSEC desenvolveu e mantém um sistema acadêmico aberto de gerenciamento de certificados digitais e o software para a gestão de chaves criptográficas para módulo de segurança criptográfica (ASI-HSM) [8, 9, 10, 11]. Estes sistemas são utilizados no projeto ICPEDU. A solução desenvolvida, fruto de trabalhos acadêmicos, está sendo usada por mais de 20 universidades em todo o país.

Cabe citar o Programa João de Barro, responsável pelo desenvolvimento do Sistema de Gerenciamento de Certificados Digitais - SGCs - tanto para a Autoridade Certificadora Raiz Brasileira quanto para as autoridades certificadoras intermediárias. Nesse programa também foi desenvolvido o SGC para emissão de certificados digitais a usuários finais, conhecido como Hawa. Estes SGCs estão hoje em uso por várias autoridades certificadoras no âmbito da Infraestrutura de Chaves Públicas Brasileira. Fruto de etapas anteriores do projeto, com a participação de dezenas de alunos de graduação e pós-graduação, a ICP-Brasil conta nestes softwares com os mais modernos algoritmos criptográficos [12, 13], bem como melhorias significativas em diversos subsistemas. Destaca-se, portanto, a relevância de dar continuidade na colaboração entre as instituições envolvidas para o benefício de todas as partes. Principalmente referente ao desenvolvimento científico-tecnológico e na formação de mão de obra profissional especializada e acadêmica no Brasil.

Este histórico no expertise em certificação digital, criptografia, infraestrutura de chaves públicas coloca a UFSC e o Labsec em posição ímpar para auxiliar o ITI e SGD na evolução da Plataforma de Assinatura de Documentos. É fundamental a participação da Universidade no fomento, geração de conhecimento, e transferência tecnológica para o Governo e Sociedade, auxiliando a fornecer aos cidadãos brasileiros acesso a tecnologias de ponta no que tange à Assinatura de Documentos digitais.

Sobre os SGCs, cita-se que suas funções principais são efetuadas usando algoritmos clássicos disponibilizados por bibliotecas como Bouncycastle, OpenSSL, e Libcryptosec, bem como através de hardware chamado de Módulo de Segurança Criptográfico - MSC. A adaptação destes SGCs para utilização de recursos pós-quânticos envolve a atualização destas bibliotecas, fluxos, sistemas aplicativos e sistemas operacionais. Além disso, a escolha do modelo de certificação e respectivos algoritmos pós-quânticos deve ser feita com cuidado, sendo que cada particularidade presente nos respectivos SGCs deverá ser estudada cuidadosamente.

Além disso, é fundamental que este estudo e a adaptação dos softwares sejam feitos o quanto antes para que informações possam ser cifradas e protegidas contra os futuros ataques quânticos. Além da necessidade de se proteger a comunicação no momento em que um computador quântico que tenha a capacidade de quebrar os algoritmos clássicos seja criado, informações sigilosas devem ser cifradas muito antes para proteger usuários de ataques que coletam informações cifradas para serem decifradas no futuro.

Estado da arte

Shor mostrou que os problemas matemáticos usados atualmente para a segurança de comunicações podem ser quebrados através de operações executadas em computadores quânticos [14]. Para tratar essa ameaça pós-quântica, novos algoritmos de assinatura foram desenvolvidos e estão sendo testados e avaliados [15, 16, 17]. Tais algoritmos têm as suas características que impactam a certificação digital de vários modos. Para que a transição aconteça de forma não abrupta, certificados híbridos foram propostos [18, 19, 20]. Tais certificados contém algoritmos clássicos e pós-quânticos, protegendo a informação da quebra de um dos algoritmos, o algoritmo clássico protege da quebra do pós-quântico e o algoritmo pós-quântico protege da quebra do clássico.

Computadores quânticos já existem, entretanto, seu potencial computacional ainda é limitado e ainda não são capazes de quebrar tais algoritmos. A proteção dos meios de comunicação de forma híbrida deve estar pronta antes dos computadores quânticos atingirem o nível em que a quebra de algoritmos clássicos se torne realidade. Pesquisas de como os algoritmos pós-quânticos impactam na certificação digital estão sendo realizados de modo que os algoritmos usados são modificados [21, 22]. Bibliotecas como Bouncycastle e o projeto Open Quantum Safe provêm tais algoritmos para pesquisa e experimentação.

Vários gerenciadores de certificados digitais já provêm a possibilidade de criar certificados digitais com algoritmos híbridos e pós-quânticos. Amazon Web Services usam protocolos

híbridos para comunicações TSL. O Sectigo disponibiliza um kit de prova de conceito onde usuários podem criar certificados pós-quânticos para autoridades certificadoras raiz, intermediárias e finais. Digicert disponibiliza um kit de ferramentas para testes de certificados híbridos para TLS.

Resultados esperados

Cumprindo ao preceito da indissociabilidade de ensino, pesquisa e extensão da Universidade Federal de Santa Catarina, o principal resultado esperado é a disseminação do conhecimento sobre certificação digital, algoritmos pós-quânticos, criptografia, assinatura digital e documentos eletrônicos para toda a sociedade, isto se dá com a eventual incorporação dos artefatos de pesquisa desenvolvidos no contexto do presente projeto na Plataforma de Assinatura GovBR, através do qual a tecnologia será disponibilizada a toda a população brasileira. O mesmo ocorre com a elaboração de aplicações que permitem ao usuário final gerar e gerenciar certificados digitais pós-quânticos para a execução de testes. Através das aplicações desenvolvidas, o gerenciamento de cadeia de certificação pós-quânticas será disponibilizado. Além dos aplicativos, a biblioteca open source Libcryptosec será atualizada para permitir a fácil manipulação de certificados tradicionais e pós-quânticos.

Ademais, espera-se que trabalhos acadêmicos no formato de monografias e artigos científicos sejam produzidos como consequência deste projeto, contribuindo para o estado da arte sobre certificação digital, criptografia pós-quântica, e assinaturas digitais, para estudantes futuros e consequentemente para a sociedade. Tais pesquisas têm motivação baseada em atuais problemas teóricos e técnicos em relação à adaptação de um ecossistema clássico, para um ambiente suscetível a ataques provenientes de um computador quântico. Ainda contribuindo para a produção, sistematização e socialização do saber científico e tecnológico, seguindo a missão da Universidade, serão realizadas internamente no LabSEC e em eventos abertos, oficinas sobre o projeto e assuntos semelhantes.

Metodologia

Para alcançar os objetivos acima, propõe-se o seguinte método:

i. Revisão bibliográfica e manutenção de uma base de dados com trabalhos relacionados a certificação digital, assinatura digital, documentos eletrônicos e infraestrutura de chaves públicas dentro e fora do contexto e regulamentação brasileira;

ii. Elaboração de relatórios técnicos contendo propostas a serem entregues ao ITI para guiar a evolução das plataformas desenvolvidas;

iii. Elaboração de protótipos funcionais para validar as propostas descritas nos relatórios técnicos apresentados, assim como seu código fonte;

iv. Revisão bibliográfica e manutenção de base de dados de trabalhos relacionados a certificados híbridos e pós-quânticos dentro e fora do Brasil;

v. Estudo da criação e gerenciamento de artefatos de certificação digital com algoritmos pós-quânticos, com base no item (iv);

vi. Elaboração de uma prova de conceito para o gerenciamento de certificados digitais híbridos e pós-quânticos, de acordo com o item (iv);

vii. Estudo da transição de um cenário clássico para um cenário pós-quântico, com base nos itens (iv) e (v).

Referências

[1] LabSEC, "Laboratório de Segurança em Computação (LabSEC)" http://www.labsec.ufsc.br, 2023, acessado em 11/04/2023.

[2] L. Ferraro, "Assinatura digital de documentos eletrônicos" Mestrado em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2011.

[3] J. E. Martina, "Projeto de um provedor de serviços criptográficos embarcado para infra-estrutura de chaves públicas e suas aplicações" Mestrado em Computação, Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Santa Catarina, Florianópolis, 2005.

[4] M. C. Carlos, "Topologias dinâmicas de infra-estrutura de chaves públicas" Mestrado em Computação, Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Santa Catarina, Florianópolis, 2007.

[5] T. C. S. d. Souza, "Aspectos técnicos e teóricos da gestão do ciclo de vida de chaves criptográficas no openhsm" Mestrado em Computação, Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Santa Catarina, Florianópolis, 2008.

[6] RNP, "Infraestrutura de chaves públicas para ensino e pesquisa (ICPEdu)" https://portal.rnp.br/web/servicos/icpedu, 2016, acessado em 08/11/2016.

[7] ITI, "Programa Joao de Barro," http://www.iti.gov.br/programas/programa-joao-de-barro, 2016, acessado em 08/11/2016.

[8] J. E. Martina, T. C. S. de Souza, and R. F. Custodio, “Openhsm: An open key life cycle protocol for public key infrastructure hardware security modules” in European Public Key Infrastructure Workshop. Springer, 2007, pp. 220–235.

[9] T. C. S. de Souza, J. E. Martina, and R. F. Custodio, “Audit and backup procedures for hardware security modules” in Proceedings of the 7th Symposium on Identity and Trust on the Internet. ACM, 2008, pp. 89–97.

[10] J. E. Martina, T. C. S. de Souza, and R. F. Custodio, “Ceremonies design for pki’s hardware security modules” in Proc. of the 9th Brazilian Symposium on Information and Computer System Security (NDSS 2009), 2009, pp. 115–128.

[11] J. E. Martina, T. C. S. de Souza, and R. F. Custodio, “Ceremonies formal analysis in pki’s context” in Computational Science and Engineering, 2009. CSE’09. International Conference on, vol. 3. IEEE, 2009, pp. 392–398.

[12] M. Lochter and J. Merkle, “Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation” RFC 5639 (Informational), Internet Engineering Task Force, Mar. 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5639.txt

[13] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, “RFC 8083 – edwards-curve digital signature algorithm (eddsa),” 2017, ”https://tools.ietf.org/html/rfc8032”.

[14] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

[15] Kumar, Manoj, and Pratap Pattnaik. "Post quantum cryptography (PQC)-An overview." 2020 IEEE High Performance Extreme Computing Conference (HPEC). IEEE, 2020.

[16] Alagic, Gorjan, et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST 2 (2020).

[17] Raavi, Manohar, et al. "Security comparisons and performance analyses of post-quantum signature algorithms." Applied Cryptography and Network Security: 19th International Conference, ACNS 2021, Kamakura, Japan, June 21–24, 2021, Proceedings, Part II. Cham: Springer International Publishing, 2021.

[18] Bindel, Nina, et al. "X. 509-compliant hybrid certificates for the post-quantum transition." *Journal of Open Source Software* 4.40 (2019): 1606.

[19] M. Raavi, P. Chandramouli, S. Wuthier, X. Zhou and S. -Y. Chang, "Performance Characterization of Post-Quantum Digital Certificates," *2021 International Conference on Computer Communications and Networks (ICCCN)*, Athens, Greece, 2021, pp. 1-9.

[20] Bindel, Nina, et al. "Transitioning to a quantum-resistant public key infrastructure." *Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8*. Springer International Publishing, 2017.

[21] Jinnan Fan , Fabian Willems , Jafar Zahed , John Gray , Serge Mister , Mike Ounsworth and Carlisle Adams. "Impact of post-quantum hybrid certificates on PKI, common libraries, and protocols." Published online: September 24, 2021. pp 200-211

[22] Sergey E. Yunakovsky, Maxim Kot, Nikolay Pozhar, Denis Nabokov, Mikhail Kudinov, Anton Guglya, Evgeniy O. Kiktenko, Ekaterina Kolycheva, Alexander Borisov, Aleksey K. Fedorov. “Towards security recommendations for public-key infrastructures for production environments in the post-quantum era.” EPJ Quantum Technol. 8 (1) 14 (2021)

6. SUBDESCENTRALIZAÇÃO

A Unidade Descentralizadora autoriza a subdescentralização para outro órgão ou entidade da administração pública federal?

( ) Sim

(X) Não

7. FORMAS POSSÍVEIS DE EXECUÇÃO DOS CRÉDITOS ORÇAMENTÁRIOS:

A forma de execução dos créditos orçamentários descentralizados poderá ser:

(X) Direta, por meio da utilização da capacidade organizacional da Unidade Descentralizada.

( ) Contratação de particulares, observadas as normas para contratos da administração pública.

(X) Descentralizada, por meio da celebração de convênios, acordos, ajustes ou outros instrumentos congêneres, com entes federativos, entidades privadas sem fins lucrativos, organismos internacionais ou fundações de apoio regidas pela Lei nº 8.958, de 20 de dezembro de 1994.

8. CUSTOS INDIRETOS (ART. 8, §2°)

A Unidade Descentralizadora autoriza a realização de despesas com custos operacionais necessários à consecução do objeto do TED?

(X) Sim

( ) Não

O pagamento será destinado aos seguintes custos indiretos, até o limite de 20% do valor global pactuado:

1. Centro Tecnológico (CTC/UFSC), totalizando 1% (um por cento) do valor bruto do projeto (R$31.154,67);

2. Departamento de Informática e Estatística (INE/UFSC), totalizando 2% (dois por cento) do valor bruto do projeto (R$62.309,33);

3. Fundo de Desenvolvimento Institucional, totalizando 4% (quatro por cento) do valor bruto do projeto (R$124.618,67);

4. Programa de Apoio às Atividades de Pesquisa (PAAP/UFSC), totalizando 3% (três por cento) do valor bruto do projeto (R$93.464,00);

5. Os custos indiretos acima estão de acordo com o Art. 12 da Resolução Normativa Nº 47/CUn/2014, de 16 de dezembro de 2014 da Universidade Federal de Santa Catarina. O valor total dos custos indiretos definido em 10% totalizando R$311.546,67

9. CRONOGRAMA FÍSICO-FINANCEIRO

As tabelas abaixo resumem os custos do projeto para cada um dos quatro anos de execução do projeto. São previstas bolsas para o Coordenador do Projeto, para Professores Pesquisadores, para equipe de servidores técnicos-administrativos da UFSC, sendo que parte atuará na administração e acompanhamento interno do projeto, e parte atuará como Pesquisadores e auxiliarão no atendimento das metas do Projeto.

São previstas bolsas para alunos de graduação e de pós-graduação. A UFSC descentralizará recursos diretamente na forma de bolsas para discentes e servidores. Vale ressaltar que, como contrapartida, para atendimento ao entregável E.8, a Universidade irá, por meio de recursos próprios, adquirir equipamento de rede Firewall.

Tabela 3 : Custo do projeto para o primeiro ano - Avançada

Descrição	Valor (ano 1)	Pessoas	Total (ano 1)
Coordenação Avançada	R$ 34.200,00	1	R$ 34.200,00
Professores	R$ 24.000,00	2	R$ 48.000,00
Servidores técnico-administrativo (Valores determinados de acordo com a atividade realizada)	R$ 23.236,36	11	R$ 255.600,00
Pesquisador júnior (pós-graduação)	R$ 44.400,00	2	R$ 88.800,00
Pesquisador júnior (graduação)	R$ 24.600,00	5	R$ 123.000,00
		Custo total para pagamentos	R$ 549.600,00
		Ressarcimento UFSC (10%):	R$ 61.066,67
		Total bruto:	R$ 610.666,67

Tabela 3.1: Custo do projeto para o primeiro ano - SGC

Descrição	Valor (ano 1)	Pessoas	Total (ano 1)
Coordenação SGC	R$ 55.200,00	1	R$ 55.200,00

Servidor técnico-administrativo	R$ 7.800,00	1	R$ 7.800,00
Pesquisador júnior (pós-graduação)	R$ 44.400,00	2	R$ 88.800,00
Pesquisador júnior (graduação)	R$ 24.600,00	5	R$ 123.000,00
		Custo total para pagamentos	R$ 274.800,00
		Ressarcimento UFSC (10%):	R$ 30.533,33
		Total bruto:	R$ 305.333,33

Tabela 4: Custo do projeto para o segundo ano - Avançada

Descrição	Valor (ano 2)	Pessoas	Total (ano 2)
Coordenador	R$ 36.000,00	1	R$ 36.000,00
Professores	R$ 26.400,00	2	R$ 52.800,00
Servidores técnico-administrativo (Valores determinados de acordo com a atividade realizada)	R$ 24.872,73	11	R$ 273.600,00
Pesquisador júnior (pós-graduação)	R$ 48.000,00	2	R$ 96.000,00
Pesquisador júnior (graduação)	R$ 26.400,00	5	R$ 132.000,00
		Custo total para pagamentos	R$ 590.400,00
		Ressarcimento UFSC (10%):	R$ 65.600,00
		Total bruto:	R$ 656.000,00

Tabela 4.1: Custo do projeto para o segundo ano - SGC

Descrição	Valor (ano 2)	Pessoas	Total (ano 2)
Coordenador (professor)	R$ 59.400,00	1	R$ 59.400,00
Servidor técnico-administrativo	R$ 8.400,00	1	R$ 8.400,00
Pesquisador júnior (pós-graduação)	R$ 48.000,00	2	R$ 96.000,00
Pesquisador júnior (graduação)	R$ 26.400,00	5	R$ 132.000,00
		Custo total para pagamentos	R$ 295.800,00
		Ressarcimento UFSC (10%):	R$ 32.866,67
		Total bruto:	R$ 328.666,67

Tabela 5 : Custo do projeto para o terceiro ano - Avançada (8 meses)

Descrição	Valor (8 meses)	Pessoas	Total (8 meses)
Coordenador	R$ 25.920,00	1	R$ 25.920,00
Professores	R$ 19.200,00	2	R$ 38.400,00
Servidores técnico-administrativo (Valores determinados de acordo com a atividade realizada)	R$ 18.000,00	11	R$ 198.000,00
Pesquisador (pós-graduação)	R$ 34.800,00	2	R$ 69.600,00
Pesquisador (graduação)	R$ 19.200,00	5	R$ 96.000,00

Custo total para pagamentos	R$ 427.920,00
Ressarcimento UFSC (10%):	R$ 47.546,67
Total bruto:	R$ 475.466,67

Tabela 5.1: Custo do projeto para o terceiro ano - SGC

Descrição	Valor (ano 2)	Pessoas	Total (ano 2)
Pesquisador sênior (professor)	R$ 64.200,00	1	R$ 64.200,00
Servidor técnico-administrativo	R$ 9.000,00	1	R$ 9.000,00
Pesquisador júnior (pós-graduação)	51.600,00	2	R$ 103.200,00
Pesquisador júnior (graduação)	R$ 28.800,00	5	R$ 144.000,00
Custo total para pagamentos			R$ 320.400,00
Ressarcimento UFSC (10%):			R$ 35.600,00
Total bruto:			R$ 356.000,00

Tabela 6: Custo do projeto para o quarto ano - SGC

Descrição	Valor (ano 4)	Pessoas	Total (ano 4)
Pesquisador sênior (professor)	R$ 69.000,00	1	R$ 69.000,00
Servidor técnico-administrativo	R$ 9.600,00	1	R$ 9.600,00
Pesquisador júnior (pós-graduação)	R$ 55.200,00	2	R$ 110.400,00
Pesquisador júnior (graduação)	R$ 31.200,00	5	R$ 156.000,00
Custo total para pagamentos:			R$ 345.000,00
Ressarcimento UFSC (10%):			R$ 38.333,33
Total bruto:			R$ 383.333,33

Tabela 7: Custo das metas

Metas	Descrição	Unidade de Medida	QTD	Valor Unitário (R$)	Valor Total (R$)	Início	Fim
AVANÇADA							
1.A	Estudo de viabilidade e proposta de inclusão da funcionalidade de compartilhamento de documentos entre cidadãos para assinatura no portal.	Meses	1	21.948,22	21.948,22	jun./24	jun./24
1.B	Estudo sobre viabilidade de adoção de mecanismos para tratar a preservação de assinaturas eletrônicas avançadas.	Meses	13	10.125,90	131.636,36	maio./25	maio./26
1.C	Estudo técnico de proxy camada 7 do protocolo TTLV.	Meses	12	13.297,00	159.564,03	dez./24	dez./25

1.D	Estudo para implementação de API para assinaturas em lotes usando Certificado Digital Avançado.	Meses	6	21.939,39	131.636,36	nov./25	abr./26
1.E	Estudo sobre o fornecimento de uma API compatível com o padrão mundial Cloud Signature Consortium para consumo da Assinatura Avançada.	Meses	6	21.939,39	131.636,36	maio./25	out./25
1.F	Estudo, projeto e implantação de metodologia para realização de deploy seguro dos componentes que integram a solução da Avançada.	Meses	10	13.163,64	131.636,36	abr./24	jan./25
1.G	Estudo e avaliação da viabilidade técnica e prática do uso de algoritmos criptográficos Pós Quânticos.	Meses	18	21.939,39	394.909,09	ago./24	ago./25
1.H	Disponibilização de infraestrutura computacional, espaço em DataCenter e conectividade com internet Desenvolvimento dos Estudo e Realização de Avaliações e Demonstrações associadas a Certificados Avançados.	Contrapartida institucional Infraestrutura disponibilizada durante Vigência do projeto (48 meses)				out./23	set./25
1.I	Estudar formas de coletar e expor ao cidadão o histórico de assinaturas	Meses	1	59.433,33	59.433,33	dez./24	dez./24
1.J	Estudar como expandir a API para permitir que órgãos integrados escolham assinar com PSCs ICP-Brasil ou com a Avançada	Meses	6	59.433,33	356.599,98	dez./24	maio/25
SGC							
2.A	Relatório técnico de levantamento de estado da arte de algoritmos pós-quânticos.	Meses	6	7.800,00	46.800,00	out./23	mar./24
2.B	Relatório técnico dos sistemas, bibliotecas e sistemas operacionais que devem ser adaptados para suportar algoritmos pós-quânticos. (Ywapa, Ywyra, e Hawa)	Meses	4	5.312,50	21.250,00	jul./24	out./24
2.C	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL .1.1-stable.	Meses	18	4.150,00	74.700,08	out./23	mar./25
2.D	Versão Alfa Protótipo dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.	Meses	18	9.366,67	168.600,00	out./23	mar./25
2.E	Relatório técnico sobre a integração das bibliotecas Pós-quânticas para os aplicativos baseados na linguagem Java.	Meses	2	3.850,00	7.700,00	set./25	out./25
2.F	Relatório técnico sobre a integração da biblioteca OQS-OpenSSL com a biblioteca Libcryptosec para prover o suporte a algoritmos pós quânticos. (Ywapa, Ywyra, Hawa)	Meses	5	8.780,00	43.900,00	jun./25	out./25
2.G	Atualização da biblioteca Libcryptosec utilizada pelo Ywapa, Ywyra e Hawa para a versão OpenSSL 3.x.	Meses	7	4.357,14	30.500,00	set./25	mar./26
2.H	Protótipo da biblioteca Libcryptosec com suporte a algoritmos pós-quânticos através da integração com a biblioteca OQS-OpenSSL. (Ywapa, Ywyra, Hawa)	Meses	4	10.900,00	43.600,00	out./25	jan./26
2.I	Protótipo Hawa com suporte a algoritmos Pós-quânticos.	Meses	13	12.269,23	159.500,00	mar./25	mar./26
2.J	Atualização do sistema operacional do software Ywapa, Ywyra e Hawa para RedHat 9.	Meses	13	10.646,16	138.400,08	mar./26	mar./27
2.K	Protótipo dos softwares Ywapa, Ywyra e Hawa com suporte a algoritmos Pós-quânticos.	Meses	13	14.407,69	187.300,00	mar./26	mar./27

2.L	Relatório técnico sobre formas de autenticação pós-quânticas que podem ser usadas nos softwares SGC. (Ywapa, Ywyra, e Hawa)		Meses	6	4.600,00	27.600,00	out./26	mar./27
2.M	Relatório sobre a adaptação dos softwares SGC para um ambiente pós-quantum.		Meses	2	4.641,67	9.283,33	ago./27	set./27
2.N	Pacote com a versão atualizada dos protótipos dos programas do SGC com suporte a algoritmos pós-quânticos. (Ywapa, Ywyra, e Hawa)		Meses	7	12.400,00	86.800,00	mar./27	set./27
SGC e Avançada								
3.A	Adaptação normativa	SGC	Meses	48	4.320,83	207.399,84	Contínuo	
		Avançada	Meses	24	4.320,83	103.699,92		
3.B	Transferência de tecnologia ao ITI Eventos/workshops de transferência	SGC	Meses	8	30.000,00	120.000,00	a definir	
		Avançada	Meses	4	15.000,00	60.000,00		
3.C	Suporte técnico e atividades de manutenção corretiva e ajustes	Avançada e SGC	Horas	300	198,11	59.433,33	dez./24	set./27

10. CRONOGRAMA DE DESEMBOLSO

MÊS/ANO	OBJETO ESPECÍFICO	VALOR	VALOR TOTAL
Outubro 2023	Avançada	R$ 610.666,67	R$ 1.160.366,67
	SGC	R$ 549.700,00	
Novembro/2024	Avançada	R$ 328.000,00	R$ 506.225,00
	SGC	R$ 178.225,00	
Abril/2025	Avançada	R$ 328.000,00	R$ 506.225,00
	SGC	R$ 178.225,00	
Outubro/2025	SGC	R$ 406.900,00	R$ 406.900,00
Abril/2026	Avançada	R$ 475.466,67	R$475.466,67
Outubro/2026	SGC	R$ 60.283,33	R$ 60.283,33
VALOR TOTAL DA DESCENTRALIZAÇÃO:			R$ 3.115.466,67

11. PLANO DE APLICAÇÃO CONSOLIDADO - PAD

CÓDIGO DA NATUREZA DA DESPESA	CUSTO INDIRETO	VALOR PREVISTO
33.90.39 (Ressarcimento UFSC)	*Sim*	R$311.546,67
33.90.18 (Bolsas de Pesquisas para Discentes)	*Não*	R$1.558.800,00
33.90.20 (Bolsa de Pesquisa Docentes e TAE)	*Não*	R$1.245.120,00

12. PROPOSIÇÃO

Florianópolis, **Irineu Manoel de Souza** **REITOR** **Universidade Federal de Santa Catarina (UFSC)**
13. APROVAÇÃO
Brasília, **Enylson Flávio Martinez Camolesi** **Diretor-Presidente** **Instituto Nacional de Tecnologia da Informação (ITI)**

sei! assinatura eletrônica	Documento assinado eletronicamente por **IRINEU MANOEL DE SOUZA**, **Usuário Externo**, em 11/06/2025, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.
sei! assinatura eletrônica	Documento assinado eletronicamente por **Enylson Flávio Martinez Camolesi**, **Presidente**, em 12/06/2025, às 11:34, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.
	A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0734928** e o código CRC **BF28077D**.