



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais



Laboratório de Arquitetura e Redes de Computadores

Plano de Trabalho

Projeto: Teste Público de Segurança (TPS) 2023 e 2025 do Sistema Eletrônico de Votação

Cliente: Tribunal Superior Eleitoral - TSE

Referência: LARC/TSE/01/03.2025

Data: 20/03/2025



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

OBJETIVO

Este plano de trabalho descreve as atividades planejadas no projeto a ser realizado conjuntamente entre o LARC e o Tribunal Superior Eleitoral - TSE.

Este projeto tem por objetivo avaliar a segurança do sistema de votação eletrônico, tanto nos aspectos de hardware, quanto de software e de processo, previamente, durante e após a realização do Teste Público de Segurança (TPS) 2023 e do Teste Público de Segurança (TPS) 2025 do Sistema Eletrônico de Votação. O objetivo desta avaliação é identificar vulnerabilidades, falhas ou potenciais pontos de melhoria em relação às propriedades de integridade ou violação do anonimato dos votos na eleição.

Neste contexto, uma falha significa um evento em que se observa que um sistema violou sua especificação por ter entrado em um estado inconsistente ocasionado por uma imperfeição (defeito) em um *software* ou *hardware* impedindo seu bom funcionamento, sem interferir na destinação e/ou anonimato dos votos dos eleitores.

O conceito de vulnerabilidade tem relação com a possibilidade de fraude, i.e., de que um ato intencional altere informações e/ou cause danos, interferindo na destinação e/ou anonimato dos votos, efetuado de forma a não restarem vestígios prontamente perceptíveis.

Finalmente, pontos de melhoria referem-se a mecanismos que possam dar maior transparência e confiança no processo eleitoral; por exemplo, pode incluir sugestões de processos que visam melhorar a auditabilidade das eleições, ou reduzir a impressão (mesmo que infundada) de fragilidade.

Os resultados deste plano de trabalho serão evidenciados através de relatórios técnicos.

ATIVIDADES PARA O TPS 2023

O processo de eleição eletrônica operado pelo TSE tem produzido resultados importantes nos últimos anos, contribuindo de forma significativa para a democracia brasileira.

A aplicação de um sistema dessa natureza na abrangência do território brasileiro representa um desafio fantástico, que deve ser necessariamente acompanhado por processos seguros, eficientes e eficazes. Inevitavelmente, isso também acaba sendo acompanhado por custos relevantes, devido à amplitude de aplicação do sistema à comunidade de aproximadamente 150 milhões de eleitores.

Como todo sistema eletrônico, ele deve ter a sua evolução pautada pela contínua melhoria dos resultados produzidos, procurando sempre aprimorar a segurança, a



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

integridade, a confiabilidade e a facilidade de uso. O processo de avaliação de segurança procura estabelecer quão efetivamente o sistema atende aos seus requisitos de segurança. Tipicamente, três tipos de atividades são realizados numa avaliação dessa natureza: Teste, Inspeção e Interação.

O objetivo da etapa de teste é exercitar uma ou mais partes do sistema avaliado sob condições específicas, analisando inclusive seu código-fonte, e comparar os resultados obtidos com os esperados. Esta etapa envolve atividades práticas com os elementos que compõem o sistema, buscando identificar vulnerabilidades, e pode ser executada em todo ambiente ou em partes específicas do sistema. A utilização de operações de varredura, técnicas de teste de software, pesquisa de vulnerabilidades apontadas na literatura, e técnicas de penetração, podem fornecer indícios importantes sobre potenciais vulnerabilidades e estimar a probabilidade de um fraudador ou atacante ter sucesso em sua tentativa. Esta etapa permite medir o grau de aderência aos requisitos de segurança do sistema.

A etapa de inspeção é o processo de examinar, revisar, observar, estudar e analisar uma ou mais partes do sistema sendo avaliado com o intuito de facilitar o seu entendimento, conseguindo esclarecer eventuais aspectos críticos e obter evidências de seu comportamento.

A etapa de interação é realizada por meio de entrevistas com indivíduos ou grupos responsáveis pelo desenvolvimento e operação do sistema para facilitar o seu entendimento, obter esclarecimentos sobre seu funcionamento e identificar evidências que poderão ser utilizadas para demonstrar o seu comportamento.

Uma das etapas críticas para um processo de avaliação de segurança é o seu planejamento inicial, que é utilizado para obter as informações necessárias para uma avaliação competente. É desta forma que se consegue identificar claramente os recursos a serem avaliados, as ameaças de interesse contra os recursos avaliados e os controles de segurança a serem utilizados para mitigar tais ameaças.

Uma avaliação de segurança deve ser tratada como qualquer outro projeto com planejamento que endereça os resultados, objetivos, escopo, requisitos e também os papéis e responsabilidades das equipes envolvidas.

A fase de execução da avaliação de segurança tem como seu principal objetivo identificar as eventuais vulnerabilidades e validá-las mediante ações específicas que comprovem a sua presença.

A fase de pós-execução tem o seu foco centrado na análise das vulnerabilidades identificadas com o intuito de achar as suas causas raízes e estabelecer recomendações de mitigação, permitindo o desenvolvimento do relatório final.

O processo de avaliação do sistema de votação eletrônica do TSE é composto por quatro etapas realizadas com o ecossistema da Urna Eletrônica (UE): Pré-TPS, Teste Público de Segurança - TPS, Pós-TPS e Teste de Confirmação. Em cada uma dessas



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

etapas deverão ser aplicadas as técnicas pertinentes, obedecendo os preceitos definidos para uma avaliação eficiente e efetiva de segurança.

O escopo geral do trabalho a ser executado pelo LARC, para atender aos objetivos do TPS, abrange os seguintes tópicos, que inclui sistemas, subsistemas e módulos de software e hardware:

- Avaliação do ponto de vista de segurança do software básico e aplicativos da UE, aplicativos de apoio à preparação da UE para a eleição e aplicativos de apoio aos processos de auditoria;
- Avaliação do ponto de vista de segurança dos sistemas de conexão, transporte e recebimento de arquivos da UE, de informação de arquivos da UE e de recebimento de boletim de urna (BU);
- Avaliação do ponto de vista de segurança das bibliotecas de software de integração/interoperabilidade entre os sistemas eleitorais e de interface com os algoritmos criptográficos de assinatura digital e cifração fornecidos pelo Cepesc/Abin;
- Introdução de mecanismos de criptografia White Box nos módulos destinados a transmissão dos dados gerados pelas urnas eletrônicas ao TSE, ao término de uma eleição;
- Avaliação do ponto de vista de segurança e de viabilidade técnica de adição de softwares e/ou módulos da totalização no escopo do TPS, proposição de melhorias do processo de lacração (incluindo procedimentos para garantir um processo de compilação reproduzível), bem como eventuais adições no escopo dos sistemas passíveis de teste pelos investigadores do TPS;
- Avaliação do ponto de vista de segurança da infraestrutura subjacente dos sistemas de transmissão e recebimento de BU e de totalização (se necessário) responsável pela segurança cibernética de tais softwares;
- Participação no TPS – Acompanhamento dos investigadores na execução dos planos de teste, provendo registros que possibilitem a reprodutibilidade dos testes;
- Avaliação da efetividade das correções e melhorias aplicadas sobre os achados do TPS.

Na fase de pré-teste a equipe responsável deve realizar uma avaliação minuciosa dos programas, seus códigos-fonte e processos aplicados pelo sistema com o intuito de identificar eventuais vulnerabilidades, falhas ou pontos de melhoria.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Um dos aspectos fundamentais da etapa de pré-teste é a identificação dos elementos do sistema que devem ser avaliados. Após várias interações com a equipe do TSE, foram identificados os módulos que devem ser avaliados prioritariamente dentro do esforço planejado para a realização do projeto. São eles:

- Software executado na UE;
- Aplicativos de apoio à fase de preparação da UE;
- Aplicativos de apoio aos processos de auditoria;
- Sistemas de conexão, transporte e recebimento de arquivos da UE, de informação de arquivos da UE e de recebimento de boletim de urna (BU);
- Bibliotecas de software de integração/interoperabilidade entre os sistemas eleitorais Java;
- Bibliotecas de software de interface Java com os algoritmos criptográficos de assinatura digital e cifração fornecidos pelo Cepesc/Abin.

Os sistemas e os componentes utilizados nas operações de transporte e recebimento de arquivos da UE a serem avaliados quanto à disponibilidade, à integridade, à confidencialidade e à autenticidade são:

- Transportador;
- RecArquivosUrna;
- InfoArquivosUrna;
- RecBU;
- JEConnect;
- SIS – Subsistema Instalação e Segurança (conjunto de software C e C++);
- Biblioteca de Integração e de segurança:
 - Bibliotecas de software de integração/interoperabilidade entre os sistemas eleitorais Java;
 - Bibliotecas de software de interface Java com os algoritmos criptográficos de assinatura digital e cifração fornecidos pelo Cepesc/Abin.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

- Software da UE:
 - UENUX;
 - Bootloader;
 - Kernel;
 - Drivers e Bibliotecas;
 - Aplicativos de votação: SCUE; GAP; ATUE; VOTA; SA e RED;
 - Aplicativos de auditoria: VPP e Avpart.
- Plataforma Desktop:
 - Aplicativos de preparação de apoio a UE: Gedai-UE; HotSwapFlash; CriptoSevin e Holocron;
 - Aplicativos de auditoria: SAVP-Sorteio; SAVP-votação.
- Eventuais softwares e módulos da totalização adicionados ao escopo do TPS após análise do LARC.

Em especial será feita uma avaliação dos seguintes mecanismos dos sistemas do ecossistema da UE:

- Interface PKCS11 ECDSA P521:
 - Verificação assinatura BIOS;
 - Verificação assinatura Bootloader;
 - Verificação Kernel;
 - Desafio intje;
 - Assinatura da correspondência;
 - Assinatura de todos os arquivos de resultado da UE.
- TRNG:
 - Geração de Chaves;
 - Geração de código de carga;
 - Chave de Kernel: Criptografia da chave de SO (cifração do Kernel do Linux);
 - Derivação de chaves (RDV e envelopes de chaves).



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

- Imagem do Kernel - criptografia com ES-CTR 256 bits:
 - Executáveis, bibliotecas dinâmicas e módulos de Kernel com assinatura ECDSA P521 embutida.
- Assinatura com curvas elípticas de 256 bits (CEPESC) de todos os arquivos de dados que entram na UE:
 - Todos os arquivos de resultados que saem da UE;
 - Kernel e todos executáveis e bibliotecas.
- Assinatura do QR Code do BU com ECDSA (Curve 25519) de 256 bits:
 - Derivação de chaves com HKDF;
 - Criptografia RDV com AES-CBC 256 bits;
 - Envelopes de chave cifradas com AES-CBC 256 bits;
 - Código verificador do BU e do Log baseado em SipHash;
- Uso do TPM na plataforma desktop:
 - Conjugado com driver monitor do ambiente;
 - Criptografia RS 2048 bits para chaveiros;
 - Autoridade certificadora de estações de trabalho;
 - Serviço (daemon) para funções de segurança:
 - Autenticação de aplicações;
 - Serviços de assinatura, cifração e MAC;
 - Guarda de chaves.

Além das atividades acima descritas, pelas diretrizes do TSE para o Teste Público de Segurança (TPS) 2023, o LARC se envolverá nas quatro etapas a seguir:

1) Etapa: Pré-TPS

Duração: 7 meses

Escopo: Avaliação da segurança do Sistema Eletrônico de Votação sob os aspectos de processo, hardware e software, apontando vulnerabilidades, potenciais riscos, e oportunidades de melhoria como preparativos ao Teste Público de Segurança (TPS).



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Esta etapa de avaliação de segurança do sistema de votação eletrônica será feita com o intuito de identificar potenciais vulnerabilidades e pontos de melhoria, juntamente com a identificação de suas causas raízes e recomendações para mitigação dos problemas apontados.

Serão realizadas reuniões de acompanhamento durante esta etapa, para reportar ao TSE, assim que possível, eventuais vulnerabilidades encontradas nas análises conduzidas pela equipe do LARC. Esses apontamentos serão registrados em relatórios parciais na medida da complexidade ou severidade encontradas, permitindo que a equipe técnica do TSE inicie uma investigação célere e aplique o tratamento adequado para o problema.

Participação presencial da equipe do LARC na apresentação dos códigos-fonte pelo TSE, como uma atividade preliminar ao TPS.

O entregável desta etapa será um relatório técnico que compõe todas as observações, sugestões, recomendações relacionadas com as vulnerabilidades, falhas ou pontos de melhoria encontradas e proposição de casos de testes.

2) Etapa: Teste Público de Segurança – TPS 2023

Duração: 1 semana

Escopo: Durante a realização do TPS, a função dos pesquisadores do LARC será acompanhar as atividades planejadas e realizadas pelos investigadores que participarão do TPS. Nesta função de acompanhamento, o objetivo é registrar todas as ações planejadas e realizadas pelos investigadores durante a semana de realização do TPS. Todas estas observações serão registradas num relatório técnico cobrindo as atividades ocorridas no TPS.

A equipe do LARC será composta por pesquisadores experientes na área de segurança da informação. Eles serão coordenados por um gestor responsável por garantir a qualidade e abrangência das observações colhidas e das informações coletadas, garantindo a completa cobertura das atividades ocorridas durante o TPS. O número de pesquisadores alocados nesta atividade dependerá da quantidade de planos de testes aprovados para a respectiva edição do TPS.

Esta etapa será realizada presencialmente no local de execução do TPS (em Brasília), envolvendo custos de deslocamento, hospedagem e diárias.

O entregável desta etapa será um relatório técnico descrevendo todas ocorrências e ações relevantes ocorridas durante a realização do TPS.

3) Etapa: Pós-TPS

Duração: 5 meses



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Escopo: Em função das observações coletadas durante o TPS, uma série de recomendações serão elaboradas com sugestões para mitigar as vulnerabilidades identificadas no TPS, em colaboração com o TSE.

Uma vez implementadas as correções que mitigam as vulnerabilidades identificadas, uma nova análise, agora especificamente sobre as partes modificadas, deve ser realizada para comprovar a efetiva resolução dos problemas sinalizados durante a execução do TPS do Sistema Eletrônico de Votação.

Novamente, os pesquisadores do LARC participarão desta etapa, juntamente com pesquisadores parceiros agregados à equipe do LARC.

Nesta etapa, os esforços se concentrarão nos itens que foram modificados e que são responsáveis pela mitigação das vulnerabilidades encontradas, sem desprezar a interferências que poderão existir como consequências de tais alterações no sistema de votação eletrônica do TSE.

O entregável desta etapa será um relatório técnico avaliando a efetividade das correções realizadas. Será elaborado também um relatório parcial contendo as informações coletadas e analisadas até a metade do prazo desta tarefa.

4) Etapa: Teste de Confirmação

Duração: 3 dias

Escopo: Uma vez feitas as correções recomendadas e validadas na etapa anterior, os investigadores independentes que participarão do TPS são convidados a analisar as correções feitas e comprovar a efetiva solução das vulnerabilidades apontadas durante a fase de execução do TPS. Novamente, a função da equipe do LARC é o acompanhamento do Teste de Confirmação do Sistema Eletrônico de Votação, com o objetivo de registrar todas as observações e sugestões feitas durante a realização deste novo teste do sistema de votação eletrônica.

Esta fase será executada presencialmente no local apontado pelo TSE (em Brasília) com a participação de uma equipe de pesquisadores do LARC que terão a função de anotar e registrar todas as observações e ações pertinentes ao processo de avaliação de segurança.

O número de pesquisadores alocados nesta atividade dependerá da quantidade de planos de testes aprovados para a respectiva edição do TPS.

O entregável desta etapa será um relatório técnico contendo todas essas observações, comentários e sugestões emitidas pelos investigadores sobre o sistema.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

CRONOGRAMA PARA O TPS 2023

Esta fase do projeto terá duração de 24 (vinte e quatro) meses contados da data da assinatura do convênio, conforme cronograma abaixo.

Atividades	Ano 1 (Meses)											
	01	02	03	04	05	06	07	08	09	10	11	12
1) Pré-TPS 2023												
2) Entrega Relatório Pré-TPS 2023						R6						
3) Preparação para o TPS 2023												
4) TPS 2023												
5) Entrega do Relatório do TPS 2023								R8				
6) Pós-TPS 2023												
7) Entrega Relatório Pós-TPS 2023												R12
Interação LARC – TSE												
Relatório de progresso	R1	R2	R3	R4	R5		R7		R9	R10	R11	

Atividades	Ano 2 (Meses)											
	01	02	03	04	05	06	07	08	09	10	11	12
8) Preparação TC TPS 2023												
9) Teste Confirmação (TC) TPS 2023												
10) Entrega Relatório TC TPS 2023		R14										
11) Testes Pós-TC TPS 2023												
12) Relatório Técnico Parcial Testes								R20				
13) Relatório Técnico Final Testes											R23	
14) Avaliação pelo TSE e Ajustes												
Interação LARC – TSE												
Relatório de progresso	R13		R15	R16	R17	R18	R19		R21	R22		



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Detalhamento das atividades:

1. **Pré-TPS 2023:** avaliação da segurança do Sistema Eletrônico de Votação sob os aspectos de processo, hardware e software, apontando vulnerabilidades, potenciais riscos e pontos de melhoria, como preparativos ao Teste Público de Segurança (TPS);
2. **Preparação para o TPS 2023:** preparação para participação no Teste Público de Segurança (TPS) do Sistema Eletrônico de Votação;
3. **TPS 2023:** acompanhamento do Teste Público de Segurança (TPS) do Sistema Eletrônico de Votação;
4. **Pós-TPS 2023:** avaliação das oportunidades de melhoria da segurança do Sistema Eletrônico de Votação resultantes do Teste Público de Segurança (TPS);
5. **Preparação para o Teste de Confirmação (TC) TPS 2023:** preparação para participação no Teste de Confirmação do Sistema Eletrônico de Votação;
6. **Teste de Confirmação (TC) TPS 2023:** acompanhamento do Teste de Confirmação do Sistema Eletrônico de Votação após as correções realizadas pelo TSE com base no que foi evidenciado no Teste Público de Segurança;
7. **Pós-TC TPS 2023:** avaliação das oportunidades de melhoria da segurança do Sistema Eletrônico de Votação resultantes do Teste de Confirmação;
8. **Relatórios Técnicos Parcial e Final dos Testes:** com base em todos os testes, o LARC elaborará um relatório preliminar e um final no Ano 2;
9. **Avaliação pelo TSE e Ajustes:** O TSE avaliará o relatório técnico final e poderá sugerir ajustes que serão efetivados até o final do convênio;
10. **Interação LARC-TSE:** durante todo processo de avaliação serão necessárias diversas interações entre a equipe do LARC e do TSE para esclarecer dúvidas, detalhar procedimentos e fornecer informações adicionais que auxiliem o processo de análise de segurança;
11. **Relatório de progresso:** breve relato enumerando os itens realizados no período e a sinalização de eventuais impedimentos, dificuldades ou problemas encontrados.

ENTREGÁVEIS PARA O TPS 2023

Os entregáveis desta fase do projeto são relatórios de progresso e relatórios técnicos produzidos de acordo com o cronograma, todos validados junto à equipe técnica do TSE.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

EQUIPE PARA O TPS 2023

A equipe do LARC executará todas as atividades previstas nesta fase do projeto, sendo composta por: 5 Bolsistas, 6 Especialistas, 5 Professores Doutores e 1 Gerente de Projeto. Alguns profissionais serão remunerados como serviços de terceiros, por se tratarem de ex-alunos do LARC, não caracterizando terceirização de atividade fim.

O esforço total estimado da equipe LARC para esta fase do projeto é de 42.000 HH (Horas/Homem) para os 24 meses.

Os bolsistas desta fase do projeto serão remunerados mensalmente conforme as tabelas a seguir:

Bolsas Regulares	Valor Máximo
Iniciação Científica I (IC-I)	R\$ 900,00
Iniciação Científica II (IC-II)	R\$ 1.100,00
Iniciação Científica III (IC-III)	R\$ 1.400,00
Iniciação Científica VI (IC-VI)	R\$ 1.700,00
Iniciação Científica V (IC-V)	R\$ 2.200,00
Mestrado I (MS-I) e Doutorado Direto I (DD-I)	R\$ 4.000,00
Mestrado II (MS-II) e Doutorado Direto II (DD-II)	R\$ 4.500,00
Doutorado I (DR-I) e Doutorado Direto III DD-III)	R\$ 6.500,00
Doutorado II (DR-II) e Doutorado Direto IV (DD-IV)	R\$ 7.000,00
Pós-Doutorado (PD-BR)	R\$ 8.500,00
Pesquisador Colaborador	R\$ 8.500,00

Capacitação de recursos humanos de apoio à pesquisa	Valor Máximo
Treinamento Técnico I (TT-I)	R\$ 600,00
Treinamento Técnico II (TT-II)	R\$ 1.200,00
Treinamento Técnico III (TT-III)	R\$ 1.500,00
Treinamento Técnico IV (TT-IV)	R\$ 4.000,00



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Treinamento Técnico IV-A (TT-IV-A)	R\$ 6.000,00
Treinamento Técnico V (TT-V)	R\$ 8.500,00



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Bolsas de Complementação FAPESP e CAPES/CNPq	Valor Máximo
Bolsa de Complementação para Aluno de Mestrado (BC-M)	R\$ 2.500,00
Bolsa de Complementação para Aluno de Doutorado (BC-D)	R\$ 3.500,00
Bolsa de Complementação para Aluno de Pós-Doc (BC-P)	R\$ 5.000,00

A definição dos valores ficará a critério da coordenação do projeto pelo LARC, que usará como base os critérios da FAPESP e outras instituições de fomento para concessão de bolsas.

Os valores das tabelas poderão ser corrigidos de acordo com o referencial da FAPESP, com formalização pelo LARC, via ofício, com cópia para todas as partes interessadas.

ORÇAMENTO PARA O TPS 2023

O orçamento para execução desta fase do projeto foi estimado em R\$ 7.182.000,00 (sete milhões, cento e oitenta e dois mil reais), considerando, os custos com custeio de equipe, de participação no TPS e no Teste de Confirmação, e em reuniões técnicas, bem como aquisição de equipamentos necessários para a execução de testes, material de consumo, além de todas as taxas e impostos.

Os custos dos acompanhamentos em Brasília do TPS e do Teste de Confirmação incluem passagens, hospedagens e diárias para a equipe do LARC.

O valor total deverá ser pago à FDTE (Fundação para o Desenvolvimento Tecnológico da Engenharia) em 23 parcelas no valor de R\$ 312.260,87, mediante a entrega de relatório de progresso ou relatório técnico, conforme indicado no cronograma.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

ATIVIDADES PARA O TPS 2025

Desde que foram iniciadas as colaborações entre LARC e TSE com foco no TPS, as atividades de análise de segurança e busca de vulnerabilidades realizadas pelo laboratório se pautaram por duas abordagens: a primeira, na direção ativo → vulnerabilidades, consiste na identificação de módulos considerados relevantes do ponto de vista de segurança, seguida da análise detalhada de seu código, de forma manual ou apoiada por ferramentas automatizadas, em busca de eventuais vulnerabilidades, falhas ou pontos de melhoria; a segunda, na direção vulnerabilidade → ativos, envolve a formulação de hipóteses de ataque com base em conhecimento da literatura (e.g., artigos científicos, guias sobre falhas de segurança comuns em sistemas, bases de vulnerabilidades como CVE/CWE, entre outras), para então avaliar se algum dos módulos do sistema poderia viabilizar as hipóteses de ataque formuladas. Ambas as abordagens são aplicadas de forma iterativa, expandindo o escopo das análises a cada iteração, seja expansão sobre a lista de ativos ou sobre a lista de hipóteses de vulnerabilidade.

Para as atividades para o TPS 2025 propõe-se continuar com essa estratégia, e também manter o escopo do TPS 2023 com uma ligeira expansão, de modo a incluir alguns processos adicionais associados à fase de lacração dos códigos da urna. Assim, o escopo proposto para o TPS 2025 deve considerar os seguintes itens:

- Avaliação do ponto de vista de segurança do software básico e aplicativos da UE, aplicativos de apoio à preparação da UE para a eleição e aplicativos de apoio aos processos de auditoria;
- Avaliação do ponto de vista de segurança dos sistemas de conexão, transporte e recebimento de arquivos da UE, de informação de arquivos da UE e de recebimento de boletim de urna (BU);
- Avaliação do ponto de vista de segurança das bibliotecas de software de integração/interoperabilidade entre os sistemas eleitorais e de interface com os algoritmos criptográficos, de assinatura digital e de cifração utilizados no sistema;
- Avaliação do ponto de vista de segurança e de viabilidade técnica de adição de softwares e/ou módulos da totalização no escopo do TPS 2025, bem como eventuais adições no escopo dos sistemas passíveis de teste pelos investigadores do TPS 2025;
- Proposição de melhorias do processo de lacração e nas análises que o precedem, incluindo procedimentos para melhorar a confiança dos auditores sobre a correspondência entre o código analisado, o lacrado, e o efetivamente carregado na urna para execução;



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

- Avaliação do ponto de vista de segurança da infraestrutura subjacente dos sistemas de transmissão e recebimento de BU e de totalização (se necessário) responsável pela segurança de tais softwares;
- Participação no TPS 2025 – Acompanhamento dos investigadores na execução dos planos de teste, provendo registros que possibilitem a reprodutibilidade dos testes em ambiente de laboratório; e,
- Avaliação da efetividade das correções e melhorias aplicadas sobre os achados do TPS 2025.

Dada a similaridade do escopo macro proposto, deve-se atentar para que as análises a serem realizadas complementem (em vez de meramente repetir) os esforços passados. Assim, embora considere-se que todos os sistemas e componentes específicos listados para as análises para o TPS 2023 permaneçam parte do escopo, deve ser dada maior prioridade a elementos específicos que: (1) sejam considerados prioritários devido a mudanças realizadas desde as últimas eleições; (2) embora importantes, não tenham até então recebido prioridade suficiente para serem avaliados em detalhes na abordagem ativo → vulnerabilidades; ou (3) sejam identificados como prioritários durante uma nova avaliação na abordagem vulnerabilidade → ativos. Adicionalmente, tendo em vista as atividades em andamento pela equipe da USP, enumeram-se a seguir alguns elementos que não se encontravam na lista original para o TPS 2023, mas que são considerados relevantes para a continuidade das análises:

- Software da UE: BIOS; firmware do MSE;
- Softwares utilizados no processo de lacração;
- Elementos de comunicação da UE (e.g., comunicação entre TE e TM, comunicação entre placa-mãe e teclado); e,
- Leitor Biométrico.

Além das atividades acima descritas, pelas diretrizes do TSE para o Teste Público de Segurança (TPS) 2025, o LARC se envolverá nas quatro etapas a seguir:

1) Etapa: Pré-TPS 2025

Duração: 4 meses



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Escopo: Avaliação da segurança do Sistema Eletrônico de Votação sob os aspectos de processo, hardware e software, apontando vulnerabilidades, potenciais riscos, e oportunidades de melhoria como preparativos ao TPS 2025.

Esta etapa de avaliação de segurança do sistema de votação eletrônica será feita com o intuito de identificar potenciais vulnerabilidades e pontos de melhoria, juntamente com a identificação de suas causas raízes e recomendações para mitigação dos problemas apontados.

Serão realizadas reuniões de acompanhamento durante esta etapa, para reportar ao TSE, assim que possível, eventuais vulnerabilidades encontradas nas análises conduzidas pela equipe do LARC. Esses apontamentos serão registrados em relatórios parciais na medida da complexidade ou severidade encontradas, permitindo que a equipe técnica do TSE inicie uma investigação célere e aplique o tratamento adequado para eventuais problemas.

O entregável desta etapa serão relatórios técnicos contemplando todas as observações, sugestões, casos de teste e recomendações relacionadas às vulnerabilidades, falhas ou pontos de melhoria encontrados.

2) Etapa: Participação no TPS 2025

Duração: 1 semana

Escopo: Durante a realização do TPS 2025, a função dos pesquisadores do LARC será acompanhar as atividades planejadas e realizadas pelos investigadores que participarão do TPS. Nesta função de acompanhamento, o objetivo é registrar todas as ações planejadas e realizadas pelos investigadores durante a semana de realização do TPS. Todas essas observações serão registradas num relatório técnico cobrindo as atividades ocorridas no TPS.

A equipe do LARC será composta por pesquisadores experientes na área de segurança da informação. Eles serão coordenados por um gestor responsável por garantir a qualidade e abrangência das observações colhidas e das informações coletadas, garantindo a completa cobertura das atividades ocorridas durante o TPS. O LARC alocará 17 pesquisadores nesta atividade presencialmente em Brasília.

Esta etapa será realizada presencialmente no local de execução do TPS (em Brasília), envolvendo custos de deslocamento, hospedagem e diárias já previstos no orçamento deste projeto.

O entregável desta etapa será um relatório técnico descrevendo todas ocorrências e ações relevantes ocorridas durante a realização do TPS 2025.

3) Etapa: Pós-TPS 2025

Duração: 5 meses



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Escopo: Em função das observações coletadas durante o TPS, será elaborada uma série de recomendações e sugestões para mitigar as vulnerabilidades identificadas no TPS, em colaboração com o TSE.

Uma vez implementadas as correções que mitigam as vulnerabilidades identificadas, uma nova análise, agora especificamente sobre as partes modificadas, deve ser realizada para comprovar a efetiva resolução dos problemas sinalizados durante a execução do TPS do Sistema Eletrônico de Votação.

Novamente, os pesquisadores do LARC participarão desta etapa, juntamente com pesquisadores parceiros agregados à equipe do LARC.

Os esforços se concentrarão nos itens que foram modificados e que são responsáveis pela mitigação das vulnerabilidades encontradas, sem desprezar a interferências que possam existir como consequências de tais alterações no sistema de votação eletrônica do TSE.

O entregável desta etapa será um relatório técnico avaliando a efetividade das correções realizadas. Será elaborado também um relatório parcial contendo as informações coletadas e analisadas até a metade do prazo desta tarefa.

4) Etapa: Participação no Teste de Confirmação

Duração: 3 dias

Escopo: Uma vez feitas as correções recomendadas e validadas na etapa anterior, os investigadores independentes que participarão do TPS são convidados a analisar as correções feitas e comprovar a efetiva solução das vulnerabilidades apontadas durante a fase de execução do TPS. Novamente, a função da equipe do LARC é o acompanhamento do Teste de Confirmação do Sistema Eletrônico de Votação, com o objetivo de registrar todas as observações e sugestões feitas durante a realização deste novo teste do sistema de votação eletrônica.

Esta fase será executada presencialmente no local apontado pelo TSE (em Brasília) com a participação de uma equipe de pesquisadores do LARC que terão a função de anotar e registrar todas as observações e ações pertinentes ao processo de avaliação de segurança.

O número de pesquisadores alocados nesta atividade dependerá da quantidade de planos de testes aprovados para o Teste de Confirmação.

O entregável desta etapa será um relatório técnico contendo todas essas observações, comentários e sugestões emitidas pelos investigadores sobre o sistema.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

CRONOGRAMA PARA O TPS 2025

Esta fase do projeto terá duração de 24 (vinte e quatro) meses contados da data da assinatura do termo aditivo ao convênio, conforme cronograma abaixo.

Atividades	Ano 3 (Meses)											
	01	02	03	04	05	06	07	08	09	10	11	12
1) Pré-TPS 2025												
2) TPS 2025												
3) Entrega do Relatório do TPS 2025					R28							
4) Pós-TPS 2025												
5) Teste de Confirmação (TC)												
6) Entrega do Relatório do TC											R34	
Interação LARC – TSE												
Relatório de progresso e/ou técnicos	R24	R25	R26	R27		R29	R30	R31	R32	R33		R35

Atividades	Ano 4 (Meses)											
	01	02	03	04	05	06	07	08	09	10	11	12
7) Testes pré-lacração de sistemas												
8) Lacração sistemas para eleições												
9) Acompanhamento das eleições												
10) Avaliação de segurança												
11) Execução de testes												
12) Relatório técnico final											R46	
Interação LARC – TSE												
Relatório de progresso e/ou técnicos	R36	R37	R38	R39	R40	R41	R42	R43	R44	R45		



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Detalhamento das atividades:

1. **Pré-TPS 2025:** Avaliação da segurança do Sistema Eletrônico de Votação sob os aspectos de processo, hardware e software, apontando vulnerabilidades, potenciais riscos e pontos de melhoria, como preparativos ao Teste Público de Segurança (TPS);
2. **TPS 2025:** Acompanhamento do Teste Público de Segurança (TPS) do Sistema Eletrônico de Votação;
3. **Entrega do Relatório do TPS 2025:** Relatório consolidado da participação do LARC no TPS 2025, com o detalhamento dos planos executados pelos investigadores, achados, melhorias identificadas e estatísticas sobre o evento.
4. **Pós-TPS 2025:** Avaliação das oportunidades de melhoria da segurança do Sistema Eletrônico de Votação resultantes do Teste Público de Segurança (TPS);
5. **Teste de Confirmação (TC):** Acompanhamento do Teste de Confirmação do Sistema Eletrônico de Votação após as correções realizadas pelo TSE com base no que foi evidenciado no Teste Público de Segurança;
6. **Entrega do Relatório do TC:** Relatório consolidado da participação do LARC no Teste de Confirmação, com o detalhamento dos planos executados pelos investigadores, achados, melhorias identificadas e estatísticas sobre o evento;
7. **Testes pré-lacração de sistemas:** Realização de testes previamente ao evento de lacração dos sistemas para as eleições de 2026;
8. **Lacração sistemas para eleições:** Acompanhamento da cerimônia de compilação e lacração dos sistemas para as eleições de 2026;
9. **Acompanhamento das eleições:** Acompanhamento do processo eleitoral em algumas escolas de São Paulo-SP e do teste de integridade;
10. **Avaliação de segurança:** Avaliações e estudos técnicos de segurança descritos no preâmbulo das atividades para o TPS 2025;
11. **Execução de testes:** Execução de testes descritos no preâmbulo das atividades para o TPS 2025;
12. **Relatório técnico final:** Relatório técnico final do projeto contemplando a Fase do TPS 2025;

Interação LARC-TSE: Durante todo processo de avaliação serão necessárias diversas interações entre a equipe do LARC e do TSE para esclarecer dúvidas, detalhar procedimentos e fornecer informações adicionais que auxiliem o processo de análise de segurança;

Relatório de progresso e/ou técnico: Breve relato enumerando os itens realizados no período e a sinalização de eventuais impedimentos, dificuldades ou problemas



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

encontrados, bem como relatórios técnicos específicos, abrangendo aspectos particulares dos testes realizados.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

ENTREGÁVEIS PARA O TPS 2025

Os entregáveis desta fase do projeto são relatórios de progresso e relatórios técnicos produzidos de acordo com o cronograma, todos validados junto à equipe técnica do TSE.

EQUIPE PARA O TPS 2025

A equipe do LARC executará todas as atividades previstas nesta fase do projeto, sendo composta por: 5 Bolsistas, 6 Especialistas, 5 Professores Doutores e 1 Gerente de Projeto. Alguns profissionais serão remunerados como serviços de terceiros, por se tratarem de ex-alunos do LARC ou profissionais com larga experiência, não caracterizando terceirização de atividade fim.

O esforço total estimado da equipe LARC é de 42.000 HH(Horas/Homem) para os 24 meses desta fase do projeto.

Os bolsistas desta fase do projeto serão remunerados mensalmente conforme as tabelas a seguir:

Bolsas Regulares	Valor Máximo
Iniciação Científica I (IC-I)	R\$ 1.100,00
Iniciação Científica II (IC-II)	R\$ 1.500,00
Iniciação Científica III (IC-III)	R\$ 1.800,00
Iniciação Científica VI (IC-VI)	R\$ 2.200,00
Pré-mestrado (PMS)	R\$ 3.000,00
Mestrado I (MS-I) e Doutorado Direto I (DD-I)	R\$ 5.600,00
Mestrado II (MS-II) e Doutorado Direto II (DD-II)	R\$ 6.000,00
Doutorado I (DR-I) e Doutorado Direto III DD-III)	R\$ 6.800,00
Doutorado II (DR-II) e Doutorado Direto IV (DD-IV)	R\$ 7.000,00
Pós-Doutorado (PD-BR)	R\$ 12.000,00
Pesquisador Colaborador	R\$ 12.000,00



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais

Capacitação de recursos humanos de apoio à pesquisa	Valor Máximo
Treinamento Técnico I (TT-I)	R\$ 700,00
Treinamento Técnico II (TT-II)	R\$ 1.300,00
Treinamento Técnico III (TT-III)	R\$ 1.800,00
Treinamento Técnico IV (TT-IV)	R\$ 4.500,00
Treinamento Técnico IV-A (TT-IV-A)	R\$ 7.000,00
Treinamento Técnico V (TT-V)	R\$ 10.000,00

Bolsas de Complementação FAPESP e CAPES/CNPq	Valor Máximo
Bolsa de Complementação para Aluno de Mestrado (BC-M)	R\$ 3.000,00
Bolsa de Complementação para Aluno de Doutorado (BC-D)	R\$ 4.000,00
Bolsa de Complementação para Aluno de Pós-Doc (BC-P)	R\$ 6.000,00

A definição dos valores ficará a critério da coordenação do projeto pelo LARC, que usará como base os critérios da FAPESP, FUSP e outras instituições de fomento para concessão de bolsas.

Os valores das tabelas poderão ser corrigidos de acordo com o referencial da FAPESP e da FUSP, com formalização pelo LARC, via ofício, com cópia para todas as partes interessadas.

ORÇAMENTO PARA O TPS 2025

O orçamento para execução desta fase do projeto foi estimado em R\$ 7.889.427,00 (sete milhões, oitocentos e oitenta e nove mil, quatrocentos e vinte e sete reais), considerando, o custeio de equipe, da participação no TPS, no Teste de Confirmação e em reuniões técnicas, bem como aquisição de equipamentos necessários para a execução de testes, material de consumo, além de todas as taxas e impostos.

Os custos dos acompanhamentos em Brasília do TPS e do Teste de Confirmação incluem passagens, hospedagens e diárias para a equipe do LARC.

O valor total deverá ser pago à FDTE (Fundação para o Desenvolvimento Tecnológico da Engenharia) em 23 parcelas no valor de R\$ 343.018,56, mediante a entrega de relatório de progresso e/ou relatório técnico, conforme indicado no cronograma.



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
Departamento de Engenharia de Computação e Sistemas Digitais
