Relatório Parcial da Comissão Avaliadora

Primeira Etapa do TPS 2025

Realização: 01 a 05 de dezembro de 2025

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 285, de 26 de junho de 2025, tem como atribuição **validar** a metodologia e os critérios de julgamento definidos pela Comissão Reguladora do Teste Público de Segurança dos Sistemas Eleitorais 2025 (Teste Público de Segurança - TPU), bem como **avaliar** e **homologar** os resultados obtidos durante o TPU 2025, e produzir **relatório conclusivo** contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes porventura identificadas.

A Comissão contou com a presença dos representantes dos seguintes órgãos:

- TSE - Júlio Ferreira de Andrade - Juiz Auxiliar da Presidência;
- Membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:
    - Antonio Esio Marcondes Salgado - Professor Mestre;
    - Osvaldo Catsumi Imamura - Professor Doutor;
    - Roberto Samarone dos Santos Araújo - Professor Doutor;
- MPF - Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas - Assessoria Nacional de Perícias em TIC;
- CFOAB - Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico;
- PF - Leonardo Bueno de Melo - Perito Criminal Federal - Serviço de Perícias em Informática;
- TCU - André Torres Breves Gonçalves - Auditor Federal de Controle Externo;
- SBC - André Ricardo Abed Grégio - Professor Doutor.

2 Metodologia de Avaliação dos Testes

Os Planos de:

- Não executados;
- Executados sem contribuição para melhoria do sistema;
- Executados com contribuição para melhoria do sistema.

3 Planos de Teste Aprovados

A Comissão Reguladora aprovou 38 planos e as propostas e seus objetos são os seguintes:

Plano de Teste 01:

- **Título**: Análise de segurança do Módulo de Segurança Embarcado (MSE) - Geração e uso de chaves privadas
- **Investigador(es)**: ELOISA PETALA APARECIDA VALERIO
- **Resumo do teste**: Este plano propõe a investigação da integridade do Módulo de Segurança Embarcado (MSE) da urna eletrônica UE2022, focando nos algoritmos e circuitos responsáveis pela geração e proteção das chaves eletrônicas privadas. O objetivo é identificar vulnerabilidades que possam vazar informações durante o processo de geração e uso das chaves, comprometendo o sigilo e a destinação dos votos.

Plano de Teste 02:

- **Título**: Exploração de vulnerabilidade na integridade do registro de voto na Mídia Externa da Urna Eletrônica
- **Investigador(es)**: ELOISA PETALA APARECIDA VALERIO
- **Resumo do teste**: O plano propõe a realização de testes na urna eletrônica (modelo UE2022) com o objetivo de identificar eventuais vulnerabilidades ou falhas no processo de registro de votos na mídia de aplicação. O foco é verificar a robustez da assinatura digital e dos mecanismos de integridade que garantem a imutabilidade dos votos armazenados na mídia externa, buscando comprovar a possibilidade de uma fraude que permita a alteração do registro de voto sem deixar vestígios perceptíveis.

Plano de Teste 03:

- **Título**: Falha/Vulnerabilidade na integridade da Mídia de Resultado
- **Investigador(es)**: ELOISA PETALA APARECIDA VALERIO
- **Resumo do teste**: Verificar a integridade e a confidencialidade dos dados de apuração registrados na Mídia de Resultado (MR) durante ou imediatamente após o procedimento de encerramento da votação. O teste visa identificar se há falha ou vulnerabilidade que permita a alteração, corrupção ou perda de informações de apuração (votos e totais) no momento da gravação na Mídia de Resultado.

Plano de Teste 04:

- **Título**: Atitude do Sistema JE-Connect diante da ação de um *rootkit* em sua execução
- **Investigador(es)**: NICHOLAS BARROS DOS SANTOS
- Resumo do teste: O plano de ataque consiste em desenvolver e executar um rootkit num computador onde será utilizado o JE-Connect, com a finalidade de analisar o comportamento do sistema de transmissão de votos, com a finalidade de constatar a confidencialidade, a integridade e a segurança dos votos obtidos durante a realização do pleito, no momento da transmissão dos dados (votos) para o banco de dados do tribunal superior eleitoral, função principal do JE-Connect.

Plano de Teste 05:

- **Título**: Averiguação de conduta da Mídia de Resultado em uma máquina infectada por malware no processo de transmissão de dados
- **Investigador(es)**: NICHOLAS BARROS DOS SANTOS
- **Resumo do teste**: O plano de ataque consiste em desenvolver e executar um malware num computador onde será utilizada a mídia de resultado, com a finalidade de analisar o comportamento do hardware, e constatar a confidencialidade, a integridade e a segurança dos votos obtidos durante a realização do pleito, no momento da transmissão dos dados (votos) para o banco de dados do tribunal superior eleitoral, através do sistema JE-Connect.

Plano de Teste 06:

- **Título**: CT02 - Teste de injeção de caracteres especiais: Avaliação da robustez do *Sanitization* do *Back-end* do RecArquivos.

- **Investigador(es)**: DANIEL GOMES DE ARRUDA

- **Resumo do teste:** Verificar a eficácia das rotinas de limpeza (*sanitization*) do RecArquives contra a injeção de caracteres de controle e null bytes (\x00) em campos de texto. Metodologia: Utilização do Postman para injetar payloads cirúrgicos (como tags malformadas e códigos de escape) diretamente no corpo da requisição POST. O teste visa falhar a lógica de parsing da aplicação. Achado Potencial: Aceitação e armazenamento do caractere proibido (violação da integridade do dado) ou falha de runtime (HTTP 500), classificada como risco Crítico/Alto.

Plano de Teste 07:

- **Título**: CT05 - Teste de robustez sistêmica: Avaliação de concorrência mista e isolamento de falhas (*Thread Management*).

- **Investigador(es)**: DANIEL GOMES DE ARRUDA

- Resumo do teste: Verificar a resiliência do back-end do RecArquivos e sua capacidade de gerenciar múltiplos envios de dados simultaneamente (tráfego concorrente misto). Metodologia: Utilização de ferramenta de desenvolvimento (JMeter) para simular o envio de 20 requisições simultâneas, contendo uma mistura de payloads válidos e falhos. O teste visa garantir o isolamento das falhas. Achado Potencial: O sistema perde ou falha ao registrar dados válidos sob o stress da concorrência, ou ocorre uma interrupção inesperada do processamento, caracterizando uma falha Crítica de Concorrência e Isolamento de Falhas.

Plano de Teste 08:

- **Título**: Teste de Segurança do teclado da Urna Eletrônica utilizando Arduino

- **Investigador(es)**: VITOR ALOISIO DO NASCIMENTO GUIA

- Resumo do teste: Este teste visa avaliar a segurança do processo de votação eletrônica, utilizando um Arduino para simular uma ameaça e tentar comprometer o sigilo do voto.

Plano de Teste 09:

- **Título**: Teste de vulnerabilidade em softwares livres do Kit JE-Connect

- **Investigador(es)**: VITOR ALOISIO DO NASCIMENTO GUIA

- **Resumo do teste**: Este teste visa explorar vulnerabilidades conhecidas em softwares livres utilizados no Kit JE-Connect para avaliar a segurança do sistema e potencialmente comprometer o sigilo ou integridade do voto.

Plano de Teste 10:

- **Título**: Teste de identificação da ordem de votação com modelo de IA
- **Investigador(es)**: VITOR ALOISIO DO NASCIMENTO GUIA
- Resumo do teste: Este teste visa avaliar a capacidade de um modelo de IA em identificar a ordem de votação a partir dos arquivos RDV e Log contidos na mídia de resultado MR, potencialmente comprometendo o sigilo do voto.

Plano de Teste 11:

- **Título**: Operação Camaleão
- **Investigador(es)**: GABRIEL LEONARDO DE SENA SANTOS
- **Resumo do teste**: A Operação Camaleão tem como finalidade testar a possibilidade de alteração mascarada de votos no sistema eletrônico de votação. O procedimento consiste em manipular os arquivos importados pelo sistema VOTAÇÃO, preservando a estrutura da base de dados para que as alterações não sejam detectadas. O teste propõe modificar o código do candidato recebido pela urna eletrônica, mantendo, porém, as demais informações originais (como foto, número, partido e nome do vice). Dessa forma, o eleitor visualiza corretamente os dados do candidato escolhido, mas o voto é computado para outro candidato. Para a simulação, cinco eleitores fictícios — “Hienas de Papai Noel Um”, “Hienas de Papai Noel Dois”, “Hienas de Papai Noel Três”, “Hienas de Papai Noel Quatro” e “Hienas de Papai Noel Cinco” — votaram na mesma seção eleitoral e escolheram a candidata Mamãe Noel. Todos confirmaram ter visto corretamente suas informações na tela da urna. Contudo, ao final da apuração, nenhum voto foi contabilizado para Mamãe Noel, e todos apareceram como votos para o candidato Coelhinho da Páscoa. Não houve votos brancos ou nulos na seção.

Plano de Teste 12:

- **Título**: Operação Camaleão Agregado
- **Investigador(es)**: GABRIEL LEONARDO DE SENA SANTOS
- Resumo do teste: Durante a preparação da eleição, a carga da flash da mídia seria feita em como seção agregada, os dados de uma seção seriam de eleitores reais, já os dados da seção

agregada seriam fictícios, semelhantes aos utilizados nas urnas de treinamento de mesário e a urna presente no museu do voto.

Plano de Teste 13:

- **Título**: Comprometimento do sistema JE-Connect por dump de chave criptográficas e acesso de *admin* via ataque de força bruta
- **Investigador(es)**: GUSTAVO RODRIGUES GOMES COSTA , JOÃO PEDRO ATALIBA GALVÃO, PEDRO HENRIQUE DE SOUZA
- **Resumo do teste**: Avaliar, a viabilidade de comprometer o acesso do JE-Connect por meio de extração indevida de chaves criptográficas e obtenção de privilégios administrativos por força bruta entre outras técnicas, demonstrando o risco de implantação de softwares maliciosos e manipulação de tráfego/processos do sistema de envio de dados eleitorais. Medir esforço e tempo de exploração, mapear falhas de configuração e lacunas de monitoramento, e produzir recomendações práticas de mitigação (proteção de chaves em hardware, MFA, políticas de bloqueio/*rate limiting*, rotação de credenciais e *hardening*).

Plano de Teste 14:

- **Título**: Geração de dados do votação fraudulentos por ataque de *man in the middle* com hardware especializado no terminal do mesário
- **Investigador(es)**: GUSTAVO RODRIGUES GOMES COSTA, JOÃO PEDRO ATALIBA GALVÃO, PEDRO HENRIQUE DE SOUZA
- **Resumo do teste**: O teste proposto consiste em transmitir, em tempo real, os dados do painel do mesário para uma segunda urna, à distância, previamente carregada com a mesma mídia de carga. Dessa forma, seria possível instaurar uma sessão de votação duplicada, viabilizando o registro de votos fraudulentos. Pretende-se demonstrar, também, como seria realizado o processo de limpeza da primeira urna, em hardware separado, de modo a tornar a fraude irrastreável.

Plano de Teste 15:

- **Título**: Estrutura avançada para análise e exploração de vulnerabilidades de uso após liberação (UAF) em sistemas embarcados críticos.
- **Investigador(es)**: GUSTAVO RODRIGUES GOMES COSTA, JOÃO PEDRO ATALIBA GALVÃO, PEDRO HENRIQUE DE SOUZA

- **Resumo do teste**: O teste visa comprometer a integridade e o controle de execução de módulos críticos do sistema JE-Connect por meio de exploração de vulnerabilidades do tipo *Use-After-Free* (UAF) na biblioteca pyqt6, demonstrando o risco de execução remota de código, elevação de privilégios e manipulação de processos/fluxos internos, abrindo assim brechas para a execução de códigos maliciosos e o possível comprometimento da integridade dos dados eleitorais. Mapear lacunas de proteção de memória e de monitoramento, e produzir recomendações práticas e priorizadas de mitigação (*hardening* de *heap*, proteções de compilação, detecção/monitoramento).

Plano de Teste 16:

- **Título**: Criação de Fuzzer para estruturas de dados (geração de

  Input malformado)

- **Investigador(es)**: KENNEDY ANTONIO VASCONCELOS FERREIRA JUNIOR, MATHEUS AFONSO LOPES CARIANI MATERNA, ROSANGELA EUZEBIO MARQUES

- **Resumo do teste**: O objetivo principal deste teste é verificar a robustez e a segurança de memória do componente de processamento de arquivos .vsu (Registro Digital de Votos), especificamente na rotina responsável por ler e validar a chave/assinatura. O ataque simulado baseia-se na hipótese de que o parser da assinatura possui um buffer de tamanho fixo e carece de validação de limites de entrada. A técnica empregada será a inserção de um payload de dados excessivamente longo no campo da assinatura do arquivo .vsu. Este payload consistirá em múltiplas cópias sequenciais de uma assinatura falsa ou bytes aleatórios, buscando intencionalmente causar um Buffer Overflow no parser ao tentar processar o campo. O brute force será usado na variação dos comprimentos e conteúdo do payload para identificar o ponto exato da falha.

Plano de Teste 17:

- **Título**: Falhas de criptografia/*hashing* em metadados

- **Investigador(es)**: KENNEDY ANTONIO VASCONCELOS FERREIRA JUNIOR, MATHEUS AFONSO LOPES CARIANI MATERNA, ROSANGELA EUZEBIO MARQUES

- **Resumo do teste**: Encontrar um campo de metadados ou dado auxiliar que possa ser alterado sem invalidar o hash ou assinatura digital principal do arquivo, explorando falha de cobertura da integridade.

Plano de Teste 18:

- **Título**: PLANO DE TESTE 1: Aprimoramento do ataque de áudio (Canal Lateral Acústico)

- **Investigador(es)**: KENNEDY ANTONIO VASCONCELOS FERREIRA JUNIOR, MATHEUS AFONSO LOPES CARIANI MATERNA, ROSANGELA EUZEBIO MARQUES

- **Resumo do teste**: Aumentar a acurácia do reconhecimento dos cliques do teclado da urna (dígitos 0-9 e Confirma/Corrige) para acima de 90% usando Machine Learning, provando que a vulnerabilidade acústica (achado anterior) é uma ameaça crítica ao sigilo do voto.

Plano de Teste 19:

- **Título**: PLANO DE TESTE 5: Condição de corrida (TOCTOU)

- **Investigador(es)**: KENNEDY ANTONIO VASCONCELOS FERREIRA JUNIOR, MATHEUS AFONSO LOPES CARIANI MATERNA, ROSANGELA EUZEBIO MARQUES

- **Resumo do teste**: Explorar uma *race condition* (TOCTOU: *Time-of-Check to Time-of-Use*) para alterar um arquivo crítico após sua validação de integridade, mas antes de ser usado pelo sistema.

Plano de Teste 20:

- **Título**: Mídias adulteradas - violação do sigilo do voto

- **Investigador(es)**: LUCAS PAVÃO DE CARVALHO XAVIER

- **Resumo do teste**: Uso de mídias com hardware alterado para permitir registro oculto de dados, sequência de armazenagem e consulta para violação do sigilo do voto.

Plano de Teste 21:

- **Título**: Interrupção fraudulenta do processo de gravação do voto

- **Investigador(es)**: LUCAS PAVÃO DE CARVALHO XAVIER

- **Resumo do teste**: Interrupção remota do processo de gravação do voto por meio de dispositivo adicionado dentro da UE que provocará reset diretamente no processador.

Plano de Teste 22:

- **Título**: Clonagem do sinal de vídeo da tela da Urna Eletrônica UE2022 via cabo e transmissão UHF.

- **Investigador(es)**: CARLOS HENRIQUE FERRÃO, DANIEL MACHADO BORGES, RAFAEL BASSO REIS

- **Resumo do teste**: O plano visa testar a possibilidade de obter uma cópia em tempo real (clonagem) da imagem exibida na tela da urna eletrônica usando uma conexão física por cabo a um transmissor UHF, com o objetivo de exibir o voto de cada eleitor em uma TV externa, comprometendo o sigilo do voto.

Plano de Teste 23:

- **Título**: Avaliação da mídia de carga e tentativa de injeções por canal USB — Urna Eletrônica
- **Investigador(es)**: CARLOS HENRIQUE FERRÃO, DANIEL MACHADO BORGES, RAFAEL BASSO REIS
- **Resumo do teste**: Este plano descreve um teste autorizado e controlado que avalia a reação da urna eletrônica à inserção de dispositivos USB que se anunciam como teclado (HID) e à interação da mídia de carga com o processo de inicialização. O objetivo é observar pontos do boot e do sistema que aceitam entrada por teclado ou dependem da mídia de carga, identificar falhas de proteção/validação e avaliar a capacidade de detecção e resposta. Testes serão realizados em laboratório isolado, mediante autorização escrita, imagens forenses prévias e medidas de *rollback*. Resultados servirão para recomendar controles técnicos e processuais específicos para urnas.

Plano de Teste 24:

- **Título**: Inserção de Mídia de Carga maliciosa: Alteração de dados de Zona/Seção e candidatos para manipulação de votos.
- **Investigador(es)**: CARLOS HENRIQUE FERRÃO, DANIEL MACHADO BORGES, RAFAEL BASSO REIS
- **Resumo do teste**: A alteração do plano de teste vai ser tentar injetar o Raspberry Pi 4 ou o Arduino dentro da placa mãe da urna eletrônica, vimos que tinha um espaço USB 3.0 com a pinagem de 19 pinos sobrando e queremos solicitar o pedido de alteração do plano de teste, iremos tentar fazer com que a urna inicialize com o rasp/arduino e consiga injetar comandos para acessar GRUB e outros serviços, através do protocolo hid.

Plano de Teste 25:

- **Título**: Teste controlado de *Buffer Overflow* no software de votação de Urna Eletrônica utilizando Raspberry Pi e Kali Linux

- **Investigador(es)**: CARLOS HENRIQUE FERRÃO, DANIEL MACHADO BORGES, RAFAEL BASSO REIS

- **Resumo do teste**: Este plano descreve a execução de um teste controlado com o objetivo de identificar vulnerabilidades do tipo *buffer overflow* no software de votação da urna eletrônica do Tribunal Superior Eleitoral durante o teste público de segurança de 2026. O ambiente será simulado por meio de uma Raspberry Pi com Kali Linux para emulação das condições reais de ataque, visando aprimorar a robustez do sistema contra-ataques clássicos de transbordamento de dados.

Plano de Teste 26:

- **Título**: Contornar proteção ZipSlip

- **Investigador(es)**: LUCIO SANTOS DE SA

- **Resumo do teste**: Durante a análise dos códigos-fonte, foi encontrada a implementação de uma proteção ao ataque ZipSlip no Transportador, RecArquivos e InfoArquivos. Esta, por sua vez, não protege de forma efetiva todas as possibilidades desta classe de ataque.

Plano de Teste 27:

- **Título**: Contornar restrições adicionadas ao Firefox do JE-Connect

- **Investigador(es)**: LUCIO SANTOS DE SA

- **Resumo do teste**: Contornar restrições adicionadas ao Firefox do JE-Connect para obter acesso às partes privilegiadas do sistema.

Plano de Teste 28:

- **Título**: O som do teclado e do fone de ouvido - Quebra de sigilo do voto por meio de sensor ultrassônico posicionado na mesa do mesário.

- **Investigador(es)**: ERIKA MARIA RODRIGUES DE CASTRO

- **Resumo do teste**: Posicionar um sensor ultrassônico na mesa do mesário para verificar a possibilidade de identificar variações ao eleitor pressionar as teclas e também do som emitido no fone de ouvido no caso de uso por deficiente. Havendo a possibilidade de variações similares para as teclas verificar se é possível identificar o número digitado e a partir disso identificar ou não se é possível a identificação e quebra do sigilo do voto. E identificar se o som emitido pela urna no fone de ouvido do deficiente pode ser ouvido.

Plano de Teste 29:

- **Título**: USB Fuzzing sobre a Urna Eletrônica
- **Investigador(es)**: LEANDRO DE SOUZA OLIVEIRA, RODRIGO BONIFACIO DE ALMEIDA
- **Resumo do teste**: Propomos um plano de avaliação das interfaces USB perante ataques de USB Fuzzing. Objetivos: Identificar potenciais pontos de entrada; Evoluir para um ataque de execução remota de código (RCE), dominando o software que é executado pela urna.

Plano de Teste 30:

- **Título**: Análise total do Kit JE-Connect: Estudo de elevação de privilégio e riscos de LOL Bins
- **Investigador(es)**: CARLOS ALBERTO DA SILVA, IAN MARTINEZ ZIMMERMANN, MATHEUS VIANNA SILVEIRA
- **Resumo do teste**: Realizar, em ambiente de homologação fornecido pelo time de desenvolvimento, uma avaliação *white-box* do Kit JE-Connect visando identificar vetores de elevação de privilégio partindo de um usuário padrão até acesso root. Embora o JE-Connect seja um sistema fechado e sem terminais habilitados em operação normal, a análise de código fonte e de binários de suporte indicou que mecanismos de shell e funcionalidades inerentes ao sistema não foram completamente desativados a nível de código. Este teste buscará, de modo controlado e autorizado, validar se técnicas de abuso de utilitários confiáveis do sistema (LOLBins) e manipulação de parâmetros em runtime permitem contornar a restrição de terminal e, subsequentemente, comprometer a integridade do subsistema de transmissão e de arquivos. Todos os testes ocorrerão exclusivamente em VM de homologação com acesso root cedido para testes. O intuito é simular um cenário onde um desenvolvedor com acesso ao sistema, prepare um *exploit* que servirá para exploração do ambiente real, sem acesso root, ou seja, um kit JE-Connect normal, porém para isso, o desenvolvedor *insider* deve ter conhecimento prévio do ambiente, e iremos simular nesse período, em ambiente de homologação, possíveis escapes do kit JE-Connect para exploração em massa de qualquer KIT JE-Connect, se bem sucedido o ataque, avançar com o objetivo de afetar a integridade dos votos.

Plano de Teste 31:

- **Título**: Sanitização e validação do Kit JE-Connect
- **Investigador(es)**: CARLOS ALBERTO DA SILVA, IAN MARTINEZ ZIMMERMANN, MATHEUS VIANNA SILVEIRA
- **Resumo do teste**: Reproduzir e validar o comportamento das funções vulneráveis sob o ambiente Windows, avaliando se o interpretador trata parâmetros e formatos incorretos com exceções controladas, sem travar ou encerrar o processo no kit JE-Connect. Exemplos em

anexo, são automatização destes testes de módulos padrão de entradas de dados, mas podem ser testados manualmente.

Plano de Teste 32:

- **Título**: Comprometimento de Integridade via GEDAI: Uso indevido de credenciais/chaves de assinatura para injeção de dados na urna.

- **Investigador(es)**: CARLOS ALBERTO DA SILVA, IAN MARTINEZ ZIMMERMANN, MATHEUS VIANNA SILVEIRA

- **Resumo do teste**: Simular um atacante interno com acesso administrativo de suporte em um TRE e avaliar se, por meio do GEDAI-UE (executando sob políticas do SIS), é possível gerar/assinar mídias de carga/votação de modo a adulterar para que a urna aceite dados manipulados, afetando integridade (alteração silenciosa de configurações/dados de eleição) e, secundariamente, confidencialidade (se a adulteração incluir mecanismos de exfiltração/violação do sigilo).

Plano de Teste 33:

- **Título**: Elevação de privilégio no SIS para impacto em confidencialidade e integridade dos votos

- **Investigador(es)**: CARLOS ALBERTO DA SILVA, IAN MARTINEZ ZIMMERMANN, MATHEUS VIANNA SILVEIRA

- **Resumo do teste**: Avaliar se um usuário comum (operacional) em um posto com SIS consegue, por falha de configuração/arquitetura, elevar privilégios a administrativo, e então usar o novo nível para executar ações de software que: (a) exponham segredos (quebra de confidencialidade, p.ex. chaves/segredos de preparação), ou (b) adulterem artefatos/processos de preparação (quebra de integridade). O plano varre módulos e implementações do SIS (serviços, drivers, mecanismos de atualização, políticas, *whitelists*, verificação de assinatura e auditoria) e, em caso de sucesso de LPE, prossegue para provas controladas de impacto nos pilares de confidencialidade e integridade dos votos.

Plano de Teste 34:

- **Título**: Avaliação da mídia de carga e tentativa de injeções por canal USB.

- **Investigador(es)**: EDUARDO MARAGNO, MARCOS ROBERTO DOS SANTOS, RICARDO CALDERAM ZANANDREA

- **Resumo do teste**: Este plano visa analisar, em ambiente controlado e com autorização, o processo de inicialização (boot) da urna eletrônica quando uma mídia de carga é inserida,

desde o reconhecimento da mídia pelo firmware/UEFI até as etapas que precedem a carga do sistema operacional ou aplicação. Serão inspecionados os artefatos presentes na mídia e monitorada a interação do boot loader com a mídia, com foco em identificar vetores que possibilitem injeção de conteúdo, quebra de integridade ou comportamentos de interposição (MITM) capazes de alterar valores ou dados transitórios durante a inicialização.

Plano de Teste 35:

- **Título**: Comprometimento da integridade e confidencialidade por dispositivos USB de captura (*Keygrabber*) em mídias removíveis usadas na votação.

- **Investigador(es)**: JOAO VITOR BASTOS DOS SANTOS, PEDRO BOHNEN SEGATTO, VITALINO PITT

- **Resumo do teste**: Simulação controlada de um ataque físico onde um dispositivo USB do tipo *keygrabber* / USB *keylogger* com capacidade de cópia e transmissão via Wi-Fi é usado para interceptar e copiar dados gravados em pendrives utilizados no processo de votação, avaliando impactos na integridade dos dados e na confidencialidade do processo, e testando a capacidade do ambiente e dos procedimentos de detectar, mitigar e responder ao incidente.

Plano de Teste 36:

- **Título**: Bypass de TPM de hardware no GEDAI/SIS via virtualização e emulação para interceptação de chaves

- **Investigador(es)**: RENATA MEYER HOBOLD, VICTOR ZACARIAS

- **Resumo do teste**: Utilizar técnicas de evasão de anti-virtualização para executar a estação GEDAI/SIS em uma plataforma de máquina virtual. Realizar dumps/snapshots de memória volátil da VM para extrair a chave de volume do Bitlocker. Subsequentemente, inicializar o sistema operacional convidado com um TPM 2.0 virtual, permitindo a interceptação, registro e manipulação das chaves criptográficas de assinatura e dos comandos enviados pelo GEDAI ao TPM durante a geração da Mídia de Carga, visando a criação de uma mídia alterada e assinada com chaves válidas.

Plano de Teste 37:

- **Título**: Análise de protocolo e fuzzing dos servidores de recebimento de arquivos do TSE via VPN do JE-Connect

- **Investigador(es)**: RENATA MEYER HOBOLD, VICTOR ZACARIAS

- **Resumo do teste**: Obter os certificados de cliente e configurações da VPN privada do TSE através da virtualização e engenharia reversa do sistema JE-Connect. Mapear a superfície de ataque da rede interna permitida ao JE-Connect através da captura e análise de tráfego (PCAP) de uma transmissão legítima de Boletim de Urna (BU). Por fim, conectar-se à VPN a partir de um ambiente não controlado e executar um ataque de fuzzing de protocolo direcionado aos servidores de recebimento de arquivos (RecArquivos/Sistot), visando encontrar vulnerabilidades.

Plano de Teste 38:

- **Título**: Acesso ao voto de cada eleitor através da porta USB da Mídia de Resultado
- **Investigador(es)**: HARON RANE SACRAMENTO CAMPELO
- **Resumo do teste**: Quebrar o sigilo do voto através de uma mídia externa no ato da votação.

4 Planos de Teste não executados

Para tornar os trabalhos de avaliação consistentes com o preparo do ambiente, o andamento das investigações e com os registros efetuados pela Equipe de Apoio Técnico do TPU 2025, constituída para acompanhar as atividades, registram-se a seguir os planos de teste não executados:

- Plano de teste 28: não executado por desistência do investigador;
- Planos de teste 11 e 12: o investigador proponente não compareceu ao evento.

5 Avaliação dos Planos de Teste

Os planos de teste apresentados em consequência ao edital de Testes Públicos de Segurança do Sistema Eletrônico de Votação foram todos avaliados pela Comissão Avaliadora. Os resultados da execução dos planos são apresentados a seguir.

5.1 Planos de teste executados e finalizados sem contribuições

Todos os planos de teste que não registraram supostos achados de vulnerabilidades foram executados de acordo com o planejamento dos investigadores presentes.

Os planos de teste que não registraram supostos achados de vulnerabilidades foram: 1, 2, 3, 4, 5, 6, 7, 8, 10, 13, 14,1 5, 16, 17, 18, 19, 20, 21, 22, 23, 24,25, 27, 29, 30, 32, 34, 35, 36, 37 e 38.

5.2 Planos de teste executados com contribuição

Os planos de teste que apresentaram resultados de avanço nos objetivos propostos foram: 9, 26, 31 e 33.

Plano de Teste 9:

- **Título**: Teste de vulnerabilidade em softwares livres do Kit JE-Connect
- **Resumo do teste**: Este teste visa explorar vulnerabilidades conhecidas em softwares livres utilizados no Kit JE-Connect para avaliar a segurança do sistema e potencialmente comprometer o sigilo ou integridade do voto.
- **Descrição do teste**: Verificação documental das atualizações efetuadas em bibliotecas de software.
- **Resultado obtido**: Constatação de vulnerabilidades conhecidas em três bibliotecas do Kit Je-Connect disponibilizado nos testes.

Parecer da Comissão Avaliadora:

- A equipe executora constatou o uso de três bibliotecas de versões anteriores, que continham vulnerabilidades conhecidas, no Kit JE-Connect disponibilizado nos testes.
- O investigador constatou também que existem bibliotecas mais recentes que não apresentam as mesmas vulnerabilidades, mas a verificação foi essencialmente documental e não foi realizado nenhum teste nos sistemas investigados.
- Tendo em vista que o problema já havia sido identificado, corrigido e documentado pela equipe técnica do TSE, não há necessidade de retorno do investigador para verificação por ocasião de novo ciclo de testes.

Plano de Teste 26:

- **Título**: Contornar proteção *ZipSlip*
- **Resumo do teste**: Durante a análise dos códigos-fonte, foi encontrada a implementação de uma proteção ao ataque *ZipSlip* no Transportador, RecArquivos e InfoArquivos. Esta, por sua vez, não protege de forma efetiva todas as possibilidades desta classe de ataque.
- **Resultado obtido**: A biblioteca infra-devsec-java-25.8.2-rc.jar possui uma falha no método validarSegurancaZipSlip, pois realiza uma verificação insuficiente contra o ataque *ZipSlip*,

limitando-se a buscar padrões como ".." ou "./" em vez de validar corretamente os caminhos extraídos. Essa abordagem pode ser facilmente burlada com caminhos absolutos (como /etc/... em Unix ou C:\ no Windows), permitindo que arquivos sejam extraídos fora do diretório esperado. Como consequência, identifica-se um risco de segurança pois a falha pode permitir escrita e execução arbitrária de arquivos.

Parecer da Comissão Avaliadora:

- Foi identificada uma falha real de segurança (*ZipSlip*) que não está plenamente mitigada na implementação atual.

- Contudo, deve-se considerar que o cenário de ataque proposto é condicional: ele depende da quebra de camadas anteriores de segurança que não foram superadas pelo investigador.

- Os riscos associados à falha identificada podem comprometer a integridade do processo e os quesitos de confiabilidade do software especificado no teste. A comissão entende que a falha foi identificada, mas não explorada efetivamente.

- O investigador deverá ser convidado a retornar e verificar as eventuais correções. O TSE deverá prover condições suficientes para que essas correções sejam testadas.

Plano de Teste 31:

- **Título**: Sanitização e validação do Kit JE-Connect

- **Resumo do teste**: Reproduzir e validar o comportamento das funções vulneráveis sob o ambiente Windows, avaliando se o interpretador trata parâmetros e formatos incorretos com exceções controladas, sem travar ou encerrar o processo no kit JE-Connect.

- **Resultado obtido**: Foi identificado um problema no software JE-Connect relacionado ao uso da tecla "ESC" (Escape). Ao utilizar a opção ”Ações” ⇒ "Acompanhar Log" duas vezes e pressionar "ESC" para fechar a janela de Log, o sistema apresenta comportamento anômalo. Na primeira vez, a tecla "ESC" fecha corretamente apenas a janela de Log, retornando à tela principal. Na segunda vez, pressionar "ESC" faz com que tanto a janela de Log quanto a janela principal sejam fechadas inesperadamente. Após esse evento, o software fica inutilizável, sem interface visível ou opções, sendo necessário reiniciar o JE-Connect para retomá-lo.

Parecer da Comissão Avaliadora:

- O procedimento descrito é determinístico, reproduzível e não depende de privilégios especiais ou de contorno de segurança.

- Não caracteriza uma vulnerabilidade de segurança no sentido clássico (como elevação de privilégio, execução remota ou *bypass* de autenticação). Porém, o erro pode afetar a continuidade de operação e causar interrupção indesejada do serviço.

- O defeito ocorre em um módulo acessório e não interfere no processamento de votos nem em funcionalidades críticas do processo eleitoral.

- O investigador deverá ser convidado para retornar no teste de confirmação, dado que a falha está documentada e reprodutível.

Plano de Teste 33:

- **Título**: Elevação de privilégio no SIS para impacto em confidencialidade e integridade dos votos

- **Resumo do teste**: Avaliar se um usuário comum (operacional) em um posto com SIS consegue, por falha de configuração/arquitetura, elevar privilégios a administrativo, e então usar o novo nível para executar ações de software que: (a) exponham segredos (quebra de confidencialidade, p.ex. chaves/segredos de preparação), ou (b) adulterem artefatos/processos de preparação (quebra de integridade). O plano varre módulos e implementações do SIS (serviços, drivers, mecanismos de atualização, políticas, *whitelists*, verificação de assinatura e auditoria) e, em caso de sucesso de LPE, prossegue para provas controladas de impacto nos pilares de confidencialidade e integridade dos votos.

- **Resultado obtido**: Durante o teste, foi possível identificar uma vulnerabilidade no sistema de abertura de arquivos do GEDAI-UE. Foi identificado que a interface executa com acesso Administrativo, e ao clicar no botão "Importar processo eleitoral de local alternativo", o acesso a essa janela foi tratado, com o objetivo de trazer maior segurança, impedindo que seja possível que o usuário consiga acessar pastas de maior privilégio, essas estão ocultas dessa janela. No entanto, durante o teste, foi possível identificar um *bypass* que possibilita o acesso a essas pastas que estão desabilitadas.

  O GEDAI-UE executa com privilégio administrativo por padrão, porém, o usuário comum, não pode ter acesso aos arquivos do sistema. Portanto, essas pastas estão desabilitadas do

sistema, o que impossibilitaria o usuário realizar a navegação e visualização de arquivos do sistema.

OBS.: O *bypass* cria um atalho no sistema, uma vez que há um controle por barras no sistema. Assim, se o atacante colocar "\" não irá funcionar. Caso seja colocado apenas C:Seguranca, é realizado um *alias* direto ao arquivo do sistema. Por meio desse *bypass*, o atacante consegue ter acesso às seguintes pastas protegidas:

* C:\Seguranca
* C:\Windows
* D:*
E a qualquer outra pasta ou arquivo protegida pelo sistema.

Parecer da Comissão Avaliadora:

- O achado é tecnicamente válido, explorado e demonstrou um comportamento inesperado da interface de importação de arquivos do GEDAI-UE.

- A limitação do impacto (somente listagem, sem execução ou modificação direta) reduz o risco de segurança, mas não elimina a necessidade de correção.

- Em sistemas que lidam com artefatos sensíveis e operam com privilégios elevados, falhas de visibilidade de caminho já configuram brechas relevantes, pois facilitam engenharia reversa, reconhecimento do ambiente e preparação de ataques futuros.

- No entanto, a presença de *bypass* funcional explorável dentro de um sistema com privilégios elevados exige resposta técnica preventiva.

- Recomenda-se correção da falha no diálogo de abertura de arquivos, com sanitização robusta do caminho e validação também no backend da aplicação, impedindo acessos indiretos por alias.

- O investigador deverá ser convidado para retornar no teste de confirmação, visto que a falha foi confirmada, documentada e seu impacto é conhecido e limitado.

6 Considerações sobre as observações realizadas pela Comissão Avaliadora

O TPU 2025 apresentou um novo cenário em que um maior número de planos de testes foram propostos, avaliados e aceitos para execução conforme o Edital do Teste Público de Segurança.

A complexidade, a segurança e maturidade dos sistemas e dos processos eleitorais foram constatadas pelo volume de esclarecimentos solicitados pelos candidatos e investigadores selecionados para identificar e conhecer os cenários de testes.

Os resultados alcançados pelos investigadores não comprometam a integridade, o sigilo do voto e o resultado das eleições. A mitigação dos riscos associados pode contribuir para o processo de melhoria contínua dos sistemas associados à votação eletrônica, tornando as eleições mais seguras e os sistemas e processos mais robustos e verificáveis.

O investigador do Plano de Teste 9 recomendou somente a atualização das versões das bibliotecas utilizadas por ter constatado que os documentos apresentados registravam novas versões e as devidas correções. A Comissão Avaliadora considera desnecessário o retorno do mesmo nos Testes de Confirmação.

A Comissão avaliadora recomenda que os investigadores dos testes 26, 31 e 33 sejam convidados para participarem dos Testes de Confirmação e realizarem uma verificação dos achados e examinarem as soluções propostas pela equipe técnica do TSE.