

Camila Lúcia Pereira Rio Branco

Título	Resumo	Resultado
Fraude na inicialização da votação	A adoção de sistemas de informação em processos eleitorais trouxe benefícios, como a publicação mais rápida de resultados e a dificuldade na prática de algumas fraudes que dependem do processo manual. Por outro lado, pode introduzir novas vulnerabilidades que podem ser exploradas para a ocorrência de novos tipos de fraudes, até então inexistentes. O teste visa alterar o resultado de uma votação no início, ou seja, alterar as escolhas dos eleitores registradas pela urna.	Reprovado. O plano de teste apresentado visa à utilização dos sistemas Candidaturas e Candex para a sua efetiva realização. Os sistemas Candidaturas e Candex não são objeto de teste para o TPS 2019. Art. 2º Os sistemas eleitorais que serão objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o <i>hardware</i> da urna e seus <i>softwares</i> embarcados.

Fellipe Ribeiro Silva Abib

Título	Resumo	Resultado
Manipulação do boletim de urna	O teste a ser realizado será conhecer o processo da geração dos boletins de urnas, identificar padrões, identificar as falhas, abrir o boletim e identificar a ordem dos eleitores que votaram, para saber quem votou em qual candidato.	Aprovado. A participação no TPS está pendente de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.

Jairo Simão Santana Melo

Título	Resumo	Resultado
Teste da urna Eletrônica baseado em IA e Processamento de Sinais	Escopo do presente plano busca abordar uma avaliação sistêmica da atual configuração da urna eletrônica em uso no processo eleitoral brasileiro, buscando empregar técnicas de aprendizado de máquina e captura de sinais elétricos em um ciclo de treinamento, teste e definição do percentual de acurácia em relação aos dados de entrada.	Aprovado. O grupo de investigadores deverá trazer osciloscópio e <i>notebook</i> para a realização do teste. No ambiente do teste, não há conexão com a internet, o grupo poderá acessar a internet em outro ambiente. Os equipamentos utilizados no teste poderão ficar retidos conforme prevê o edital do TPS, Art. 40, inciso V - os

		equipamentos, dispositivos eletrônicos e materiais citados nos incisos I, II e III deste artigo, quando aprovados, poderão ficar retidos no TSE por até 60 dias após o encerramento da realização do TPS.
--	--	---

José Filipe de Moraes Albano

Título	Resumo	Resultado
Exploração de vulnerabilidades na infraestrutura de rede, sistemas e ativos.	<p>O objetivo da exploração de vulnerabilidades na infraestrutura e nos ativos que compõe a urna eletrônica tem como principal finalidade simular um ataque aos ativos do TSE.</p> <p>Em caso positivo, se encontrada vulnerabilidade, investigar qual o impacto e os sistemas que podem ser afetados, bem como encontrar soluções que possam mitigar os ataques, garantindo o exercício do voto sem ocorrer a sua violação, através dos pilares da segurança da informação, que são eles: a confidencialidade, integridade e disponibilidade da informação.</p>	<p>Aprovado com ressalvas.</p> <p>O Edital do TPS, Art. 2º, estabelece os sistemas eleitorais objeto do TPS.</p> <p>Art. 2º Os sistemas eleitorais que serão objetos do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, incluindo o hardware da urna e seus softwares embarcados.</p> <p>Desta forma, o plano de teste deve realizar ataques apenas aos sistemas apresentados, não sendo permitida a realização de ataques à rede do TSE. Haverá ambiente de teste segregado preparado para o TPS onde o investigador poderá realizar os testes previstos no plano de teste.</p>

Leonardo Cunha dos Santos

Título	Resumo	Resultado
Teste de invasão utilizando análise instantânea de pulso elétrico	O teste constitui-se do uso de reconhecimento de padrões a partir da detecção de pulsos elétricos com a finalidade de compreender	<p>Aprovado.</p> <p>A participação no TPS está pendente de</p>

	comportamentos do equipamento durante a operação de voto.	complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.
--	---	--

Luis Antonio Brasil Kowada

Título	Resumo	Resultado
Tentativa de obtenção de chaves criptográficas	Este teste visa avaliar se os procedimentos e gerenciamento de chaves garantem a confidencialidade e autenticação.	Aprovado.
Verificar vulnerabilidades das bibliotecas do sistema	Este teste visa avaliar a possibilidade de alteração de bibliotecas ou explorar vulnerabilidades de bibliotecas de terceiros.	Aprovado. O grupo de investigadores deverá providenciar instalador para o sistema operacional Kali Linux.

Luis Fernando de Almeida

Título	Resumo	Resultado
Tentativa de mapeamento de rotina aleatória por meio de algoritmos de reconhecimento de padrão	Para fins de garantir a confidencialidade dos votos, sua na urna eletrônica utiliza do recurso de rotinas pseudoaleatórias para proporcionar que um voto seja armazenado em posições ao acaso dentro do arquivo. Atualmente, nota-se a crescente aplicação de rotinas inteligentes baseadas em <i>Machine Learning</i> aplicadas ao problema de Reconhecimento de Padrão. A literatura apresenta casos de sucesso destas rotinas em problemas de regressão e modelo preditivos. Diante deste contexto, o teste em questão pretende analisar a possibilidade de rotinas inteligentes serem capazes de criarem um modelo capaz de mapear a geração dos números aleatórios e, conseqüentemente, comprometer o sigilo do voto.	Aprovado.

Paulo César Herrmann Wanner

Título	Resumo	Resultado
Extração de dados e configurações do Kit JE Connect.	<ol style="list-style-type: none"> 1. Obter senhas e configuração da VPN a partir de uma mídia do JE Connect. 2. A partir dos dados obtidos, tentar se conectar diretamente à rede do TSE. 3. Verificar existência de vulnerabilidades 	Aprovado. O grupo de investigadores deverá providenciar o disco rígido ou HDD externo USB de tamanho compatível para

	no RecArquivos utilizando técnicas de <i>fuzzing</i> . 4. Verificar possibilidade de acesso direto ao banco de dados e às suas rotinas.	copiar as imagens Interface USB/SATA. O grupo de investigadores deverá providenciar instalador para o sistema operacional Kali Linux.
Extração do conteúdo do disco criptografado do SIS	1. Obter acesso físico ao disco do computador com o GEDAI instalado para retirar o disco criptografado e buscar a chave no registro do Windows. 2. Inicializar o disco em uma máquina virtual para obter um <i>dump</i> de memória. 3. Extrair a chave a partir do <i>dump</i> e comparar com as informações obtidas no registro para estabelecer processo de formação da chave. 4. Montar o disco cifrado e extrair os dados presentes neste disco. 5. Verificar, no disco cifrado, informações sensíveis para o processo eleitoral.	Aprovado. O TSE providenciará material para abertura do gabinete do computador a ser utilizado no plano de teste. O grupo de investigadores deverá providenciar o disco rígido ou HDD externo USB de tamanho compatível para copiar as imagens Interface USB/SATA e mídia removível de alta capacidade (64gb ou superior).
Instalação e execução de código arbitrário em uma máquina do GEDAI para implante de dados falsos na Urna Eletrônica.	1. Obter acesso físico ao computador com o GEDAI instalado para fazer uma imagem completa do disco. 2. Inicializar o disco em uma máquina virtual. 3. Subverter o sistema de inicialização para viabilizar o <i>boot</i> sem a carga do SIS. 4. Acessar e modificar programas de criação e preparação de dados a serem gravados nas urnas eletrônicas. 5. Criar um cartão de inicialização da urna com dados espúrios.	Aprovado. O TSE providenciará material para abertura do gabinete do computador a ser utilizado no plano de teste. O grupo de investigadores deverá providenciar o disco rígido ou HDD externo USB de tamanho compatível para copiar as imagens Interface USB/SATA e mídia removível de alta capacidade (64gb ou superior).

Roberto Miyano Neto

Título	Resumo	Resultado
CT001 – Integridade do Arquivo Executável da Urna - VOTA	Verificar que o arquivo executável assinado somente é executado após verificação da assinatura	Aprovado com ressalvas. A participação no TPS está pendente de

		complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.
CT002 – Integridade da Coleta de Votos	Verificar se o processo de coleta de votos gera provas de integridade para cada voto obedecendo aos requisitos funcionais de sigilo do voto, definidos pela constituição brasileira.	Aprovado com ressalvas. A participação no TPS está pendente de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.
Integridade do Arquivo de VOTOS	Verificar se o arquivo de votos contem a lista de votantes e os votos armazenados fora de ordem, garantindo o sigilo constitucional, porém com provas de integridade por voto, e com integridade entre a quantidade de votantes e votos. Verificar ainda se tal arquivo é assinado com chave privada única por urna, conhecida pelo TSE, armazenada em HSM.	Aprovado com ressalvas. A participação no TPS está pendente de complementação de informações. O investigador deverá entrar em contato com o TSE para sanar a pendência.