Relatório de Avaliação Geral do TPS

Execução dos Planos de Testes:
27 de novembro a 1º de dezembro de 2023

Teste de Confirmação:
15 a 17 de maio de 2024

INTRODUÇÃO **4**

SUMÁRIO DOS PLANOS DE TESTES APROVADOS **5**

DESCRIÇÃO DOS PLANOS DE TESTES **8**

PLANO DE TESTE 1: Quebra do sigilo do voto 8

PLANO DE TESTE 2: Fragilizar sigilo do voto 9

PLANO DE TESTE 3: Invadir a mídia de carga da urna eletrônica 9

PLANO DE TESTE 4: Mídia de Resultado: a confiança do(a) cidadão(ã) na urna eletrônica e o coração da democracia 10

PLANO DE TESTE 5: *Fraus Omnia Corrumpit* 10

PLANO DE TESTE 6: *Nihil Autem Absconditum Est, Quod Non Reveletur* 11

PLANO DE TESTE 7: *Qui Duplicat, Videre Suffragio Potest* 12

PLANO DE TESTE 8: *Suffragium Simulata Substantiam Veritas Mutare Possunt* 12

PLANO DE TESTE 9: Extração, verificação e validação do conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis embarcados na urna eletrônica 13

PLANO DE TESTE 10: Execução do JE-Connect utilizando computador com sistema operacional inválido 14

PLANO DE TESTE 11: Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados 14

PLANO DE TESTE 12: USBExploit – acesso a dados da urna através da porta USB 15

PLANO DE TESTE 13: Captura do vídeo transmitido no *display*, com a alteração dos cabos transmissores 15

PLANO DE TESTE 14: Acesso à rede do TSE por intermédio do *software* JE-Connect realizando a execução de *shell* a partir de um dispositivo USB 16

PLANO DE TESTE 15: Adulteração no JE-Connect 16

PLANO DE TESTE 16: Violar a confidencialidade, integridade e disponibilidade das informações no Python do *software* JE-Connect 17

PLANO DE TESTE 17: Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no *software* JE-Connect 18

PLANO DE TESTE 18: Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no *software* JE-Connect 19

PLANO DE TESTE 19: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita do Python no *software* JE-Connect 19

PLANO DE TESTE 20: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita e nas bibliotecas Python no *software* JE-Connect 20

PLANO DE TESTE 21: Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo *KIT* JE, possibilitando comandos a partir de *scripts* em área restrita 20

PLANO DE TESTE 22: Executar código espúrio na urna eletrônica modelo 2020 21

PLANO DE TESTE 23: Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020 22

PLANO DE TESTE 24: Utilizar a chave que cifra/decifra o *kernel* da urna para alterar o Registro Digital de Voto .. 24

PLANO DE TESTE 25: Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI 24

PLANO DE TESTE 26: Alterar dados/programas nos sistemas SIS/GEDAI 25

PLANO DE TESTE 27: Ataque de *cold boot* à urna eletrônica 26

PLANO DE TESTE 28: Tentativa de *Man-in-the-Middle* na comunicação do teclado com Arduíno 26

PLANO DE TESTE 29: Tentativa de reconhecimento das teclas digitadas usando IA 27

PLANO DE TESTE 30: Teste de capacidade do teclado da urna eletrônica em receber múltiplas entradas simultâneas 28

PLANO DE TESTE 31: Inconsistência de *software* 29

PLANO DE TESTE 32: *Ab imitio Invalidi, Post Validi* * 30

PLANO DE TESTE 33: *Omnia Invalidi est* * 30

PLANO DE TESTE 34: *Suffragium non est relates* * 31

PLANO DE TESTE 35: Escalação de privilégio no Windows (SIS) * 31

DA REALIZAÇÃO DO TESTE PÚBLICO DE SEGURANÇA DA URNA – EDIÇÃO 2023 33

Da semana de execução dos testes – de 27 de novembro a 02 de dezembro de 2023 33

Do Teste de Confirmação – de 15 a 17 de maio de 2024 34

Resumo das ações implementadas pelas equipes técnicas da STI/TSE 34

RESUMO DOS NÚMEROS DO TESTE PÚBLICO DE SEGURANÇA DA URNA – EDIÇÃO 2023 36

(*) Planos de testes apresentados e aprovados durante a realização do TPS 2023

INTRODUÇÃO

O Teste Público de Segurança de Urna está regulamentado pela Resolução-TSE n° 23.444, de 30 de abril de 2015, e tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação, da apuração e da transmissão dos votos, além de propiciar melhorias no processo eleitoral.

Por meio do TPS, é oportunizado aos(às) participantes a identificação de eventuais vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato do voto, para que essas possam ser corrigidas antes das eleições. O objetivo é contribuir com o desenvolvimento dos sistemas eleitorais.

Nos termos do artigo 2º da Resolução-TSE n° 23.444/2015, os sistemas eleitorais que podem ser objeto do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e recebimento de arquivos, lacrados em cerimônia pública, conforme definido no § 2º do art. 66 da Lei n° 9.504/97, incluindo o *hardware* da urna e seus *softwares* embarcados.

O Teste Público de Segurança de Urna constitui parte integrante do Ciclo de Transparência Democrática – que é composto por várias etapas de fiscalização da fase de desenvolvimento dos sistemas eleitorais – e é oportunizado a qualquer cidadão(ã) brasileiro(a), maior de 18 anos, que, individualmente ou em grupo, preencha os requisitos definidos em edital.

SUMÁRIO DOS PLANOS DE TESTES APROVADOS

ID	Nome	Investigadores		Situação
1	Quebra do sigilo do voto	I-1	Aline Barbosa da Silva	Encerrado sem achados
2	Fragilizar sigilo do voto	I-1	Aline Barbosa da Silva	Encerrado sem achados
3	Invadir a mídia de carga da urna eletrônica	I-1	Aline Barbosa da Silva	Encerrado sem achados
4	Mídia de Resultado: a confiança do(a) cidadão(ã) na urna eletrônica e o coração da democracia	I-2	Érika Maria Rodrigues de Castro	Encerrado sem achados
5	*Fraus Omnia Corrumpit*	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
6	*Nihil Autem Absconditum Est, Quod Non Reveletur*	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
7	*Qui Duplicat, Videre Suffragio Potest*	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
8	*Suffragium Simulata Substantiam Veritas Mutare Possunt*	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
9	Extração, verificação e validação do conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis embarcados na urna eletrônica	I-4	João Benedito dos Santos Junior	Encerrado sem achados
10	Execução do JE-Connect utilizando computador com sistema operacional inválido	I-5	Nicholas Barros dos Santos	Encerrado sem achados
11	Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados	I-5	Nicholas Barros dos Santos	Encerrado sem achados
12	USBExploit – acesso a dados da urna através da porta USB	G-1	Marcos Roberto dos Santos Leandro Caletti (não compareceu) Rafael Noll da Silva Eduardo Bido Rhayra Rodrigues Fiorentin	Encerrado sem achados
13	Captura do Vídeo transmitido no *display*, com a alteração dos cabos transmissores	G-2	Rafael Basso Reis Gabriel Viecili André Izolani Rien (não compareceu) Brayan Vanz de Oliveira Stefano Augusto Mossi	Encerrado sem achados
14	Acesso a rede do TSE por intermédio do *software* JE-Connect realizando a execução de *shell* a partir de um dispositivo USB	G-2	Rafael Basso Reis Gabriel Viecili André Izolani Rien (não compareceu) Brayan Vanz de Oliveira Stefano Augusto Mossi	Encerrado sem achados
15	Adulteração no JE-Connect	G-3	Vitor Aloisio do Nascimento Guia Hitatiana Maria Santiago Ferreira da Silva Guia	Encerrado sem achados
16	Violar a confidencialidade, integridade e disponibilidade das informações no Python do *software* JE-Connect	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado COM achados

ID	Nome	Investigadores		Situação
17	Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no *software* JE-Connect	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado sem achados
18	Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no *software* JE-Connect	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado sem achados
19	Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita do Python no *software* JE-Connect	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado sem achados
20	Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita e nas bibliotecas Python no *software* JE-Connect	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado sem achados
21	Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo *KIT* JE, possibilitando comandos a partir de *scripts* em área restrita	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado sem achados
22	Executar código espúrio na urna eletrônica modelo 2020	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Encerrado COM achado
23	Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Encerrado COM achado
24	Utilizar a chave que cifra/decifra o *kernel* da urna para alterar o Registro Digital de Voto	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Não executado
25	Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Encerrado COM achado
26	Alterar dados/programas nos sistemas SIS/GEDAI	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Não executado
27	Ataque de *cold boot* à urna eletrônica	G-5	Galileu Batista de Sousa Maria Isabel Vasconcelos Lima Breno Rangel Borges Marchetti João Paulo Vieira Almeida João Vitor de Sá Hauck	Não executado

ID	Nome	Investigadores		Situação
28	Tentativa de *Man-in-the-Middle* na comunicação do teclado com Arduíno	G-6	Luis Antonio Brasil Kowada Gabriel Cardoso de Carvalho Caubi de Souza Loureiro Rosa Camila Ferreira Alves	Encerrado sem achados
29	Tentativa de reconhecimento das teclas digitadas usando IA	G-6	Luis Antonio Brasil Kowada Gabriel Cardoso de Carvalho Caubi de Souza Loureiro Rosa Camila Ferreira Alves	Encerrado COM achados
30	Teste de capacidade do teclado da urna eletrônica em receber múltiplas entradas simultâneas	G-7	André Mário dos Reis dos Santos Alexandre Zago Boava Diego Vergaças de Sousa Carvalho	Encerrado COM achado
31	Inconsistência de *Software*	G-8	Avelino Francisco Zorzo (não compareceu) Ariel Rossetto Ril Daniel Dalalana Bertoglio	Encerrado sem achados
32	*Ab imitio Invalidi, Post Validi* *	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
33	*Omnia Invalidi est* *	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
34	*Suffragium non est relatus* *	I-3	Guilherme Henrique dos Santos	Encerrado sem achados
35	Escalação de privilégio no Windows (SIS) *	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho	Encerrado COM achados

(*) Planos de testes apresentados e aprovados durante a realização do TPS 2023

DESCRIÇÃO DOS PLANOS DE TESTES

PLANO DE TESTE 1: Quebra do sigilo do voto		
	Investigadora:	Aline Barbosa da Silva
	Apoio técnico:	Andrea Erina Komo (USP)
	Objetivo:	Testar se a mídia de resultados contabiliza o voto sem que a votação na seção tenha sido encerrada pelo terminal do mesário.
	Etapas Propostas:	1. Inicia-se votação na urna eletrônica; 2. Primeiro o(a) eleitor(a) hipotético(a) realiza o voto do início ao fim; 3. Investigadora retira a mídia de resultado sem encerrar a seção; 4. No computador com o JE-Connect, investigadora transfere os arquivos da urna; 5. Investigadora verifica se o voto foi computado antes de terminar a seção; 6. Com o voto transferido da mídia de resultado, investigadora quebra o sigilo desse único voto.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de *kit*/senha do JE-Connect e usuário/senha do SIS.
	Considerações técnicas:	Nesse teste, a investigadora propôs a leitura da mídia de resultado do primeiro e único eleitor da seção sem que esta fosse encerrada no terminal do mesário. Ao longo do teste, a investigadora concluiu que era necessário encerrar a seção para acessar as informações na mídia de resultados. Considerando essa alteração no plano de teste, a investigadora encerrou a seção e consultou a mídia de resultado. Dado que havia apenas um único voto computado, ela concluiu que o sigilo desse voto havia sido quebrado. Porém, tal situação apresentada não configura uma quebra do sigilo do voto por uma falha ou brecha no sistema da urna eletrônica. A situação relatada já foi discutida e está registrada no Acórdão-TSE, da sessão de 2/9/2010, Processo Administrativo n° 1089-06.2010.6.00.0000/DF, cujo relator é o Ministro Marco Aurélio. No voto, o ministro descreve que a situação retratada é de ocorrência improvável, mas, caso ocorra, há de garantir o direito à cidadania (manifestação da vontade), ainda que haja o risco de identificação do voto do(a) eleitor(a). Além disso, foi explicado para a investigadora que a recomendação do TSE é que o(a) primeiro(a) eleitor(a) não seja liberado(a) até que o(a) segundo(a) da mesma seção conclua o voto.

PLANO DE TESTE 2: Fragilizar sigilo do voto		
	Investigadora:	Aline Barbosa da Silva
	Apoio técnico:	Andrea Erina Komo (USP)
	Objetivo:	Testar se as teclas, ao serem acionadas pelo(a) eleitor(a), são realmente criptografadas e não há nenhuma vulnerabilidade no teclado da urna eletrônica.
	Etapas Propostas:	1. Instalar, na saída de áudio da urna eletrônica (habilitada para deficientes visuais), um dispositivo com fio auxiliar conectado a uma caixinha de som para testar as teclas; 2. Ao pressionar uma tecla, sua identificação será transmitida pela caixinha de som.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de *kit*/senha do JE-Connect, usuário/senha do SIS, fone de ouvido da investigadora e disponibilização de um microfone e uma caixinha de som pelo TSE.
	Considerações técnicas:	Nesse teste, a investigadora propôs uma eventual quebra do sigilo do voto do(a) eleitor(a) em virtude de um vazamento de áudio durante a votação. O teste não apresentou achados, pois os passos e as justificativas apresentadas apenas demonstraram que o sistema de acessibilidade da urna eletrônica, via áudio, funciona corretamente. Só haveria um vazamento do áudio se o(a) próprio(a) eleitor(a) quisesse quebrar seu sigilo.

PLANO DE TESTE 3: Invadir a mídia de carga da urna eletrônica		
	Investigadora:	Aline Barbosa da Silva
	Apoio técnico:	Andrea Erina Komo (USP)
	Objetivo:	Invadir a mídia de carga da urna eletrônica fazendo a limitação de votos aos(às) candidatos(as) de uma seção.
	Etapas Propostas:	1. Conectar a mídia de carga em um computador; 2. Tentar invadir a mídia de carga; 3. Limitar os votos aos(às) candidatos(as) da mídia de carga; 4. Testar a mídia de carga limitada instalando na urna.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS.
	Considerações técnicas:	O teste proposto visava limitar o número de votos de algum(a) candidato(a) alterando a mídia de carga. A investigadora tentou alterar a mídia de carga, sem conhecer as proteções existentes, não conseguindo realizar qualquer alteração na mídia de carga.

PLANO DE TESTE 4: Mídia de Resultado – a confiança do(a) cidadão(ã) na urna eletrônica e o coração da democracia	
Investigadora:	Érika Maria Rodrigues de Castro
Apoio técnico:	Luís Fernando Schauren (TRE/RS)
Objetivo:	Averiguar a segurança jurídica da mídia de resultado, desde sua inserção na urna eletrônica; e o processo de transmissão dos dados até a divulgação, tentando identificar possíveis vulnerabilidades ou falhas que possam interferir na integridade ou na quebra do sigilo dos votos em uma eleição.
Etapas Propostas:	1. Inserção da mídia de resultado na urna eletrônica (hipótese de troca por uma mídia vazia) para verificar o funcionamento; 2. Inserção de uma mídia de resultado comum para verificar o encaixe físico e a necessidade de uma porta física proprietária com pinagem diferenciada; 3. Testagem da possibilidade de inserção de novos dados na mídia de resultados, após o encerramento da votação e antes da emissão do boletim de urna; 4. Simulação de extravio de uma mídia de resultado, com adulteração do RDV, simulando quebra de integridade ou violação do sigilo do voto; 5. Gravação, em vídeo, da tela da urna eletrônica durante a votação.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento do usuário/senha do SIS.
Considerações técnicas:	O teste proposto visava limitar o número de votos de algum(a) candidato(a) alterando a mídia de carga. A investigadora tentou alterar a mídia de carga, mas, sem conhecer as proteções existentes, não conseguiu realizar qualquer alteração.

PLANO DE TESTE 5: *Fraus Omnia Corrumpit*	
Investigador:	Guilherme Henrique dos Santos
Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
Objetivo:	Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do(a) eleitor(a), e, com isso, alterar a disposição dos votos.
Etapas Propostas:	1. Conectar outra fonte de vídeo para a tela do terminal do eleitor; 2. Aplicar um adesivo de fundo preto e números brancos sobre as teclas 123 e 789, então apresentando as teclas 789, 456 e 123; 3. Apresentar *feedback* visual na tela que apresente teclar inverso ao realmente teclado.
Resultado:	Executado sem achados.

	Flexibilizações de segurança:	Nenhum.
	Considerações técnicas:	O investigador não conseguiu realizar o seu teste por possuir componentes inapropriados para implementar a sua prova de conceito. Apesar da ausência de execução, foi aberta uma discussão sobre as suas preocupações ao ter proposto tal teste. O investigador sugeriu então fortalecer a gaiola de *faraday* interna da urna, para atenuar/bloquear sinais de/para dentro da urna e impedir qualquer iniciativa de controle remoto ou exfiltração de dados, e enfatizou a sugestão de melhoria feita sobre cifrar o canal de comunicação da tela.

PLANO DE TESTE 6: *Nihil Autem Absconditum Est, Quod Non Reveletur*		
	Investigador:	Guilherme Henrique dos Santos
	Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
	Objetivo:	Obter o conteúdo do RDV, em mídia alternativa; inserir em urna de contingência; e, a partir da comparação da diferença entres os arquivos e da ordem de eleitores(as) habilitados(as), violar o sigilo do voto.
	Etapas Propostas:	1. Inserir cabo *splitter* USB na saída para mídia e acoplar 2 mídias; 2. Iniciar a votação; 3. Retirar uma mídia e colocar na urna de contingência; 4. Tentar variações do procedimento, alternando a ordem de inserção e duplicação da mídia de resultados; 5. Simultaneamente, anotar o fluxo de habilitação; 6. Habilitar mais um(a) eleitor(a) na urna oficial e, após seu voto, encerrar a votação em ambas as urnas; 7. Comparar os resultados entre a votação oficial e a advinda da mídia duplicada na urna de contingência; 8. Se não obtiver sucesso, repetir os passos usando um *laptop* para duplicação do conteúdo da mídia de votação.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Concedido livre acesso ao SIS/GEDAI para geração de mídias.
	Considerações técnicas:	O investigador reconheceu a inviabilidade do procedimento apresentado de violação do sigilo do voto contra todos(as) os(as) eleitores(as) da seção. Ele argumentou que é um cenário válido somente para o caso de violação do sigilo do voto do(a) último(a) eleitor(a). Há uma decisão do Ministro Marco Aurélio sobre o significado da quebra de sigilo do voto do(a) último(a) eleitor(a), que, sendo uma possibilidade já conhecida pelo TSE, é tomada como risco aceito. O investigador sugeriu que fossem impedidas cópias binárias de mídias de aplicação, apesar de reconhecer o aumento do custo associado.

PLANO DE TESTE 7: *Qui Duplicat, Videre Suffragio Potest*		
	Investigador:	Guilherme Henrique dos Santos
	Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
	Objetivo:	Violar o sigilo do voto, a partir da sequência de votantes e do conteúdo obtido do *display* terminal de eleitor com acoplamento de um *splitter* na saída de vídeo e outro *display*.
	Etapas Propostas:	**1.** Abrir a urna; **2.** Conectar o cabo de transmissão de vídeo eDP da placa-mãe ao *splitter* de sinal eDP; **3.** Conectar o *splitter* de eDP à tela da urna e outro terminal a um transmissor remoto de vídeo.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Nenhuma.
	Considerações técnicas:	O investigador desmontou o painel frontal da urna e desencaixou o cabo de eDP e do teclado, desacoplando a tela da urna. Porém, ao tentar conectar o cabo de eDP da urna, ele constatou incompatibilidade no conector físico entre seu dispositivo e o utilizado pela urna.

PLANO DE TESTE 8: *Suffragium Simulata Substantiam Veritas Mutare Possunt*		
	Investigador:	Guilherme Henrique dos Santos
	Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
	Objetivo:	Alterar a destinação dos votos, substituindo os oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.
	Etapas Propostas:	**1.** Iniciar a votação na urna oficial (UE-A); **2.** Iniciar votação na urna de contingência 1 (UE-B); **3.** Habilitar eleitores(as) e inserir votos espúrios na UE-B, à medida que forem sendo habilitados e registrados pela UE-A; **4.** Provocar falhas na UE-A e na UE-B; **5.** Iniciar processo de contingência da UE-B numa terceira urna contingência (UE-C); **6.** Inserir votos espúrios na UE-C; **7.** Continuar a votação e encaminhar os votos espúrios da UE-C para totalização.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecido usuário/senha do SIS e acesso a mídias sem lacre.

	Considerações técnicas:	O sistema de totalização não aceitou o resultado emitido pela UE-C, dado que carrega consigo o número de correspondência de si mesmo e da UE-B. No GEDAI foi registrado como número de correspondência da UE-A. Se ocorrer um processo de contingência, a cadeia de correspondências esperada seria da UE-A e da urna que recebesse a contingência de UE-A.

PLANO DE TESTE 9: Extração, verificação e validação do conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis embarcados na urna eletrônica		
	Investigador:	João Benedito dos Santos Junior
	Apoio técnico:	Guilherme Fumagali Marques (USP)
	Objetivo:	Verificar a integridade e autenticidade de sistemas eleitorais, em tempo real, extraindo, verificando e validando o conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis que estiverem embarcados na urna eletrônica.
	Etapas Propostas:	1. Preparar ambiente; 2. Extrair arquivos da urna; 3. Verificar assinatura dos arquivos.
	Resultado:	Executado sem achados
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS.
	Considerações técnicas:	O objetivo inicial do investigador era executar o *script* “Verohash”, de autoria própria, desenvolvido em Java. Esse código receberia, como entrada, um arquivo texto que descreveria uma estrutura chave-valor, sendo a chave o identificador do arquivo (seu caminho no SO) e o valor um *hash* SHA512 codificado em Radix 64, com as informações a serem confirmadas (as fornecidas pelo TSE). O algoritmo procuraria pelos arquivos com mesmo identificador-chave, calcularia o *hash* e compararia com o de mesmo identificador na outra entrada. Com isso, o investigador pretendia ler o sistema de arquivo contido no SO da urna eletrônica, verificando cada dado. No entanto, após uma sequência de esclarecimentos no primeiro dia, houve o entendimento de que, para acessar os arquivos da forma pretendida, seria necessário extrair o *hardware* de armazenamento primário (mídia interna SSD) da urna eletrônica. Assim, em vez de consultar todos os arquivos, foi verificada, com sucesso, a integridade apenas dos arquivos da mídia de aplicação.

PLANO DE TESTE 10: Execução do JE-Connect utilizando computador com sistema operacional inválido	
Investigador:	Nicholas Barros dos Santos
Apoio técnico:	Matheus Santhiago Araujo Januario (USP) e Marcio Rosostolato Machado (TRE/SP)
Objetivo:	Analisar a eficácia da transmissão de dados de votação via JE-Connect em um computador que apresenta alguma falha na validação do seu sistema operacional, podendo ocasionar possíveis riscos de quebra de sigilo e do transporte dos dados obtidos durante o pleito.
Etapas Propostas:	1. Simular eleição com 10 votos; 2. Apurar os votos; 3. Executar JE-Connect com o sistema operacional inválido.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Remoção da chave de ativação do MS-Windows, fornecimento de usuário/senha do SIS e de *Kit*/senha do JE-Connect.
Considerações técnicas:	O plano de teste não obteve sucesso, pois a execução do JE-Connect não sofreu interferência do sistema operacional MS-Windows, mesmo estando sem a chave de ativação.

PLANO DE TESTE 11: Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados	
Investigador:	Nicholas Barros dos Santos
Apoio técnico:	Matheus Santhiago Araujo Januario (USP) e Marcio Rosostolato Machado (TRE/SP)
Objetivo:	Executar um *bot* de monitoramento num computador no qual será executado o JE-Connect, analisando seu comportamento para avaliar a integridade e segurança da transmissão dos votos para o TSE.
Etapas Propostas:	1. Executar *bot* de monitoramento; 2. Simular eleição; 3. Apurar votos; 4. Executar JE-Connect num computador operando com o *bot* de monitoramento.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect.
Considerações técnicas:	O plano de teste não obteve sucesso, pois partiu da premissa de que o JE-Connect era uma aplicação executada dentro do sistema operacional MS-Windows.

PLANO DE TESTE 12: USBExploit – acesso a dados da urna através da porta USB		
	Investigadores:	Marcos Roberto dos Santos, Leandro Caletti (não compareceu), Rafael Noll da Silva, Eduardo Bido e Rhayra Rodrigues Fiorentin
	Apoio técnico:	Firmiano Ramos Perlingeiro e Guilherme Fumagali Marques (USP)
	Objetivo:	Capturar informações da urna por meio da conexão de um cabo console ou adaptador USB (com conexão Ethernet ou Serial), que possibilite acesso aos dados, bem como dos votos inseridos.
	Etapas Propostas:	1. Conectar um cabo console em uma das portas da urna; 2. Executar *software* para obter acesso ao sistema operacional; 3. Executar *software* para validar os dados em memória e/ou capturar os votos impressos no *spool* de impressão e capturar chaves de assinatura; 4. Apropriar-se dos dados da urna bem como das chaves de assinatura.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect; Concessão de senha do BIOS da máquina com MS-Windows para alterar sequência de *boot*.
	Considerações técnicas:	Somente duas portas resultaram em retorno de energia: MR – Mídia de Resultado e a Interna (USB3 – livre na placa-mãe). Em ambos os casos, as luzes de conexão e transmissão demonstraram-se ativas. Em todos os cenários, não foi possível entregar IP de forma automática para a urna. Após os testes de conexão Ethernet, foi tentada a conexão por meio de um adaptador USB - USB-C para a urna, que não resultou em comunicação de dados e energia.

PLANO DE TESTE 13: Captura do vídeo transmitido no *display*, com a alteração dos cabos transmissores		
	Investigadores:	Rafael Basso Reis, Gabriel Viecili, André Izolani Rien (não compareceu), Brayan Vanz de Oliveira e Stefano Augusto Mossi
	Apoio técnico:	Victor Takashi Hayashi (USP)
	Objetivo:	Abrir a urna eletrônica e substituir o cabo HDMI por outro que possua um dispositivo, enviando a imagem para outro dispositivo conectado via *bluetooth*.
	Etapas Propostas:	1. Abrir a urna; 2. Substituir o cabo HDMI original da urna por um cabo HDMI modificado; 3. Verificar em quais candidatos(as) as pessoas estão votando.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de cabo *flat* de comunicação do *display* da urna para teste não intrusivo.
	Considerações técnicas:	O plano de teste partiu da premissa de que o cabo de transmissão de dados entre o *display* e a placa-mãe era HDMI, porém, ao abrir a urna, constatou-se que a transmissão era feita por um cabo com 30 pinos paralelos trançados, cuja especificação era desconhecida.

PLANO DE TESTE 14: Acesso a rede do TSE por intermédio do *software* JE-Connect realizando a execução de *shell* a partir de um dispositivo USB	
Investigadores:	Rafael Basso Reis, Gabriel Viecili, André Izolani Rien (não compareceu), Brayan Vanz de Oliveira e Stefano Augusto Mossi
Apoio técnico:	Victor Takashi Hayashi (USP)
Objetivo:	Abrir um *shell* no sistema operacional responsável pela comunicação do JE-Connect, obtendo acesso à rede do TSE.
Etapas Propostas:	1. Conectar o *pen drive* (*Kit* JE-Connect) no computador responsável pelo envio dos dados; 2. Executar abertura do *shell*; 3. Executar a enumeração da rede; 4. Aplicar *exploits* para permitir o acesso.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect; Fornecimento de senha do BIOS da máquina SIS para permitir *boot* pelo *pen drive*.
Considerações técnicas:	Foi executado o *script* "window.print" para abrir o assistente de impressão com impressora PDF, que permitiu observar os arquivos presentes no JE-Connect. Ainda que tenha sido possível visualizar arquivos, não foi possível alterá-los.

PLANO DE TESTE 15: Adulteração no JE-Connect	
Investigadores:	Vitor Aloisio do Nascimento Guia e Hitatiana Maria Santiago Ferreira da Silva Guia
Apoio técnico:	Matheus Tavares de Andrade (USP)
Objetivo:	Simular um agente mal-intencionado que adquiriu conhecimento de uma vulnerabilidade previamente desconhecida em um *software* presente na Mídia com Sistema Embarcado (MSE) até o momento da sua *release*. O objetivo é avaliar o comportamento do *Kit* do JE-Connect quando um agente obtém privilégios de usuário *root* não autorizados e tenta adulterar o *software* JE-Connect, bem como transmitir dados adulterados da Mídia de Resultados (MR).
Etapas Propostas:	1. Obter privilégio de usuário *root* não autorizado; 2. Adulterar JE-Connect; 3. Adulterar dados da Memória de Resultados (MR); 4. Transmitir dados adulterados.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect.
Considerações técnicas:	Foi utilizado o *script* "python/bu_dump.py" como exemplo, especialmente a biblioteca "asn1tools", para construir um novo boletim de urna adulterado, mas não foi possível realizar a transmissão de

		boletim adulterado pelo JE-Connect, pois o conteúdo não correspondia mais com a assinatura digital. As tentativas de elevação de privilégio de usuário *root* (primeira etapa proposta) também não foram bem-sucedidas.

PLANO DE TESTE 16: Violar a confidencialidade, integridade e disponibilidade das informações no Python do *software* JE-Connect		
	Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
	Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
	Objetivo:	Atacar o JE-Connect explorando a vulnerabilidade da linguagem de programação Python na função Str.str.format(). A vulnerabilidade surge quando o aplicativo Python usa a função str.format e string-f na formatação de *string*, permitindo que os(as) invasores(as) tenham acesso a informações confidenciais e/ou possam inserir um código executável.
	Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.
	Resultado:	Executado COM achado.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS. Autorização de uso de máquina virtual com Kali Linux e máquina virtual com JE-Connect.
	Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas. Contudo, durante os testes, os investigadores encontraram um achado ao executar a seguinte sequência de passos: 1. Inserir *Kit* JE-Connect; 2. Acessar tela inicial de *login*; 3. Realizar tentativas usando três credenciais ou mais, até que o sistema informe que o limite foi excedido e será reiniciado; 4. Teclar Ctrl+C, cancelando o reinício e resetando o número de tentativas de *login*. O sistema JE-Connect foi planejado para, a cada três erros de credenciais, realizar o *reboot* do *Kit*, para evitar tentativas de ataque de força bruta. A reinicialização ocorre mediante envio de comando de *reboot* ao sistema operacional Debian da máquina virtual do sistema JE-Connect. Com a atualização do sistema operacional Debian para a versão 12, este passou a exigir o parâmetro "-f" (*forcefully*), para que o processo de reinicialização não seja interrompido. Esse parâmetro não foi implementado no JE-Connect disponibilizado no TPS, apesar de já conhecido. A falta de atualização do parâmetro faz com que o processo

		de reinicialização pudesse ser interrompido pela digitação de teclas (ou seja, o comportamento relatado não é provocado exclusivamente com o uso das teclas "Ctrl+C"). Em que pese a ausência do parâmetro "-f", o Debian reinicializa após a 3ª solicitação de *reboot*, fazendo com que o JE-Connect disponibilizado no TPS aceite nove tentativas de credenciais erradas antes de reiniciar. Mesmo um(a) profissional a serviço da Justiça Eleitoral, detentor de senha de credencial de uso do sistema JE-Connect, não possui condições para alterar um boletim de urna assinado digitalmente ou evidenciar em quem determinado(a) eleitor(a) votou.
	Parecer Comissão Avaliadora:	"A falha no sistema de controle de acesso explorada neste teste deve ser revista e corrigida, pois representa uma vulnerabilidade nos conceitos aplicados ao projeto do *software*. Apesar do impacto no ponto explorado ser reduzido e não comprometer a condução e os resultados das eleições, pode ser uma falha de concepção, recomenda-se uma análise mais abrangente." A Comissão Avaliadora recomenda retorno no Teste de Confirmação para nova verificação, em versão ajustada do sistema eleitoral, da efetividade das correções a serem implementadas.

PLANO DE TESTE 17: Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no *software* JE-Connect		
	Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
	Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
	Objetivo:	Atacar o JE-Connect explorando a vulnerabilidade da linguagem de programação Python. Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, nos quais um(a) invasor(a) pode abusar dos recursos XML para acessar os arquivos locais, gerar conexões de rede para outras máquinas ou contornar *firewalls*.
	Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.
	Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas.

PLANO DE TESTE 18: Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no *software* JE-Connect	
Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
Objetivo:	Atacar o JE-Connect explorando a vulnerabilidade da linguagem de programação Python. A função urllib.parse na linguagem de programação Python possui uma falha de segurança de alta gravidade na função de análise de URL do Python, que pode ser explorada para ignorar os métodos de filtragem de domínio ou protocolo implementados com uma lista de bloqueio, resultando em leituras arbitrárias de arquivos e execução de comandos.
Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.
Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas.

PLANO DE TESTE 19: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita do Python no *software* JE-Connect	
Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
Objetivo:	Atacar o JE-Connect executando um *exploit* funcional que permite chamar qualquer comando do sistema sem acesso direto a métodos como os.system. Este *exploit* é implementado em Python puro e funciona sem importar bibliotecas externas e sem instalar o *driver* “code.__new__”.
Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.

Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.
Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas.

PLANO DE TESTE 20: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de *scripts* em área restrita e nas bibliotecas Python no *software* JE-Connect	
Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
Objetivo:	Atacar o JE-Connect executando vários *exploits* funcionais para permitir chamadas de comandos e funções às bibliotecas nativas e externas do Python e obter acesso às informações.
Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.
Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas.

PLANO DE TESTE 21: Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo *KIT* JE, possibilitando comandos a partir de *scripts* em área restrita	
Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
Objetivo:	Atacar o JE-Connect executando vários *exploits* funcionais para permitir chamadas de comandos e obter acesso às informações, com escalada de privilégio.
Etapas Propostas:	1. Virtualizar a execução do JE-Connect; 2. Violar a confidencialidade dos dados com acesso a informações

		confidenciais; 3. Violar a integridade dos dados com alteração de informações confidenciais; 4. Violar a disponibilidade dos dados com a interferência das informações confidenciais.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS e *Kit*/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.
	Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano, pois as barreiras de segurança impedem a virtualização do JE-Connect. Com isso, todas as demais etapas do plano ficaram comprometidas.

PLANO DE TESTE 22: Executar código espúrio na urna eletrônica modelo 2020		
	Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
	Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
	Objetivo:	Executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), utilizando um equipamento (USBArmory) para simular uma mídia de carga e alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
	Etapas Propostas:	1. Clonar mídia de carga; 2. Carregar sua imagem no USBArmory; 3. Realizar uma carga na urna, utilizando o USBArmory como mídia de carga, mapeando, assim, todos os acessos realizados na mídia de carga; 4. Analisar os acessos gerados pelo passo anterior, identificando possíveis pontos onde o ataque TOCTOU pode ser executado; 5. Realizar uma nova carga executando o ataque TOCTOU, substituindo a mídia de carga após a sua validação.
	Resultado:	Executado COM achado.
	Flexibilizações de segurança:	Fornecimento de usuário e senha do SIS/Gedai-UE para a geração de mídias de carga. Livre acesso à urna eletrônica.
	Considerações técnicas:	A equipe de investigadores revelou um problema na cadeia de confiança da urna. Mais especificamente, ficou evidenciada a existência de um *bug* no BIOS/UEFI da urna, que permitiu um ataque do tipo TOCTOU (*time of check, time of use*) sobre o *bootloader*. Com a capacidade de manipulação do *bootloader*, a equipe de investigadores foi capaz de alterá-lo para que fosse exposta a chave de decifração do *kernel* (chave de SO). Também foi feita modificação para a exibição de mensagem na tela da urna (ASCII art). Não foram feitas modificações no *kernel* do sistema operacional,

		bibliotecas ou aplicativos da urna, ainda que a equipe tenha tentado atacá-los pelo método TOCTOU. Como o ataque se deu pela interceptação do tráfego USB da mídia de aplicação (mídia externa), as manipulações se deram somente sobre a mídia de carga. As modificações feitas sobre o *bootloader* não poderiam ser replicadas para a mídia interna da urna. Isso porque não ficou evidenciada a capacidade de interceptação do tráfego da interface SATA M.2 da mídia interna da urna, com vista à replicação do ataque TOCTOU sobre o BIOS/UEFI. Portanto, qualquer tentativa de gravação de *bootloader* modificado na mídia interna da urna seria prontamente identificada pela cadeia de confiança. O achado não seria capaz de violar a integridade do voto, uma vez que não ficou evidenciada a capacidade, mesmo no limite hipotético, de manipulação da cadeia de confiança executada a partir da mídia interna da urna, tampouco a capacidade de manipulação do *Software* de Votação ou de qualquer outro aplicativo instalado na urna e usado nos processos de captação e apuração de votos. Pelas mesmas razões, também não seria possível violar o anonimato do voto.
	Parecer Comissão Avaliadora:	"A janela de ataque explorada foi entre a execução da inicialização da urna, um *bootloader* controlado pelo MSE, Módulo de Segurança Embarcado, mas com um coadjuvante que é o programa de carga do BIOS/UEFI, um módulo que controla o funcionamento básico da urna. É um ataque complexo, de um grau de realização baixo por conta dos mecanismos de segurança implementados, mas que deve ser tratado adequadamente para mitigar os riscos apresentados." A Comissão Avaliadora recomenda retorno no Teste de Confirmação para nova verificação, em versão ajustada do sistema eleitoral, da efetividade das correções a serem implementadas.

PLANO DE TESTE 23: Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020		
	Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
	Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
	Objetivo:	Partindo do sucesso na execução do plano de teste "Executar código espúrio na urna eletrônica modelo 2020", extrair a chave que cifra/decifra o *kernel* da urna modelo 2020 a partir da execução de código arbitrário.
	Etapas Propostas:	1. Rodar um código arbitrário a partir da mídia de carga simulada (USBArmory); 2. Executar um processo capaz de acessar a chave do *kernel*.
	Resultado:	Executado COM achado.
	Flexibilizações de segurança:	Fornecimento de usuário e senha do SIS/Gedai-UE para a geração de mídias de carga. Livre acesso à urna eletrônica.

	Considerações técnicas:	A equipe de investigadores revelou um problema na cadeia de confiança da urna. Mais especificamente, ficou evidenciada a existência de um *bug* no BIOS/UEFI da urna, que permitiu um ataque do tipo TOCTOU sobre o *bootloader*. Com a capacidade de manipulação do *bootloader*, a equipe de investigadores foi capaz de alterá-lo para que fosse exposta a chave de decifração do *kernel* (chave do sistema operacional – SO). A chave do SO é de uso exclusivo para a abertura do núcleo do sistema operacional. Outras chaves utilizadas pelo *software* da urna são derivadas a partir de semente decifrada pelo *hardware* de segurança das urnas (MSE). A mesma semente é usada para a derivação da chave do SO. Os investigadores conseguiram expor essa semente sem, no entanto, expor o elemento derivado que é repassado para o *kernel*, a partir do qual é derivada a chave de decifração do RDV. Portanto, a partir da chave do SO não é possível obter a chave de decifração do RDV, ainda que seja possível obtê-la a partir da semente exposta. A afirmação de que o RDV é somente protegido por criptografia não é correta. Durante toda a votação, o arquivo de RDV é mantido cifrado e assinado digitalmente. Portanto, a capacidade de decifrar e cifrar um RDV não é condição suficiente para gerar um arquivo válido para a urna. Finalmente, um ataque de violação de sigilo da votação por meio da decifração de RDVs consecutivos, embora possível, precisa ser considerado no contexto de uma seção eleitoral, na qual o acesso à mídia de votação (mídia externa na qual é mantida cópia do RDV) se daria em ambiente com diversas pessoas – mesários(as), eleitores(as) e até mesmo fiscais –, com o sucessivo rompimento e reposição de lacres físicos, o que tornaria o ataque pouco prático. Considerando o objetivo de manipulação do RDV, como o arquivo é mantido assinado digitalmente, não há risco de violação à integridade ou ao sigilo do voto.
	Parecer Comissão Avaliadora:	"Uma intervenção do tipo TOCTOU sobre o *bootloader* permitindo o acesso ao processo de entrega da semente para a geração de chave criptográfica deve ser analisada e corrigida. De acordo com a documentação do *software*, esta janela não deveria existir, mas não está declarada de forma explícita nos requisitos de implementação e no modelo desenvolvimento de *software* seguro. Assim, recomendamos uma análise dos documentos que originam os requisitos de desenvolvimento e que norteiam a codificação e os testes de conformidade." A Comissão Avaliadora recomenda retorno no Teste de Confirmação para nova verificação, em versão ajustada do sistema eleitoral, da efetividade das correções a serem implementadas.

PLANO DE TESTE 24: Utilizar a chave que cifra/decifra o *kernel* da urna para alterar o Registro Digital de Voto	
Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
Objetivo:	Partindo do sucesso na execução do plano de teste "Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020", derivar uma chave para cifrar um RDV falso. Posteriormente, esse RDV falso poderia ser carregado em uma urna de contingência.
Etapas Propostas:	1. Executar um programa que utilize a chave do *kernel* como parâmetro e seja capaz de gerar um RDV válido; 2. Salvar esse RDV numa *flash* externa e utilizá-la na urna de contingência.
Resultado:	Não executado.
Flexibilizações de segurança:	Nenhuma.
Considerações técnicas:	Plano de teste não executado por opção do grupo.

PLANO DE TESTE 25: Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI	
Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
Objetivo:	Utilizar técnicas avançadas para recuperar a chave guardada no TPM, utilizada pelo Bitlocker, para cifrar o disco da máquina onde são executados os *softwares* SIS/GEDAI.
Etapas Propostas:	1. Tentar utilizar algum *software* disponível publicamente para capturar a chave TPM; 2. Em caso de falha, tentar utilizar a placa PCILeech para pegar a chave do Bitlocker que está na memória RAM; 3. Em caso de falha, tentar habilitar opções pertinentes no BIOS para possibilitar o ataque; 4. Em caso de falha, utilizar o leitor/gravador externo de BIOS para habilitar as opções pertinentes para possibilitar o ataque; 5. Em caso de falha, utilizar técnica de restauração do Windows; 6. Em caso de falha, utilizar o ataque Intel DCI para habilitar a depuração de *hardware* e, assim, capturar a chave TPM.
Resultado:	Executado COM achado.
Flexibilizações de segurança:	Fornecimento da senha da BIOS. Abertura do gabinete do computador com SIS/Gedai-UE.
Considerações	O plano de teste foi bem-sucedido ao explorar vulnerabilidade documentada do sistema operacional Windows e o seu mecanismo de

	técnicas:	cifração de unidades de armazenamento, chamado BitLocker. Não se tratou, portanto, da exploração de vulnerabilidade em sistema desenvolvido pela Justiça Eleitoral. A abertura das partições BitLocker, nas quais residem o SIS e os sistemas eleitorais, não é condição suficiente para o comprometimento do Gedai-UE. O Gedai-UE é protegido por assinatura digital independente de qualquer mecanismo de segurança do SIS ou nativo do Windows. Essa assinatura é validada de forma ativa por um serviço especialmente desenvolvido para a proteção de chaves e validação de aplicativos, com o apoio de chave embarcada no processador TPM e em *driver* monitor de ambiente. Nenhuma dessas barreiras de segurança foi exercitada pelo grupo de investigadores. No limite hipotético de comprometimento do Gedai-UE (o que não foi realizado pelo grupo), não seria possível alterar o *software* da urna ou dados de votação. Isso porque o *software* e os dados estão protegidos por assinaturas digitais geradas fora do Gedai-UE e validadas pela urna.
	Parecer Comissão Avaliadora:	"O sistema de geração de mídias de carga da urna eletrônica é executado em um ambiente protegido pelo SIS e pelo Windows. O resultado obtido neste teste mostra a vulnerabilidade da primeira camada (Windows) que, apesar de não comprometer a segunda camada (SIS), demonstra os riscos associados ao modelo de segurança adotado. Recomenda-se uma nova análise de riscos para o aprimoramento dos conceitos adotados neste domínio." A Comissão Avaliadora recomenda retorno no Teste de Confirmação para nova verificação, em versão ajustada do sistema eleitoral, da efetividade das correções a serem implementadas.

PLANO DE TESTE 26: Alterar dados/programas nos sistemas SIS/GEDAI		
	Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
	Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
	Objetivo:	Utilizando técnicas de análise de código/engenharia reversa e, se necessário, algum *hardware* de apoio, comprometer o funcionamento adequado dos sistemas SIS/GEDAI de modo a propagar informações falsas entre os sistemas e a urna eletrônica, ou mesmo não propagar informação alguma.
	Etapas Propostas:	1. Instalar a placa PCILeech no *desktop* no qual o GEDAI está instalado; 2. Utilizando o *software* da placa, tentar alterar estrutura de dados/programas sensíveis do GEDAI; 3. Caso não funcione o primeiro passo e a chave de recuperação do Bitlocker tenha sido obtida por outros métodos, utilizar uma máquina virtual para: 3.1. Desativar as proteções do Subsistema de Instalação e Segurança (SIS); 3.2. Instalar um *debugger* na máquina; 3.3. Modificar programas/estrutura de dados que propagam informações entre a urna e seu ecossistema. Ex.: modificar a

		tabela de correspondência ou não transmiti-la, porém registrar em *logs* que ela foi transmitida.
	Resultado:	Não executado.
	Flexibilizações de segurança:	Nenhuma.
	Considerações técnicas:	Plano de teste não executado por opção do grupo.

PLANO DE TESTE 27: Ataque de *cold boot* à urna eletrônica		
	Investigadores:	Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
	Apoio técnico:	Fernando Frota Redígolo (USP) e Cleyton Luiz de Melo Eufrásio (TRE/GO)
	Objetivo:	Congelamento da memória RAM da urna visando à extração dos dados em leitor externo para posterior decodificação.
	Etapas Propostas:	1. Com a urna em funcionamento, aplicar *spray* de congelamento no pente de memória; 2. Mantendo a memória congelada, mover e inseri-la rapidamente na máquina de destino; 3. Executar *boot* na máquina de destino capturando o conteúdo da memória.
	Resultado:	Não executado.
	Flexibilizações de segurança:	Nenhuma.
	Considerações técnicas:	Plano de teste não executado por opção do grupo.

PLANO DE TESTE 28: Tentativa de *Man-in-the-Middle* na comunicação do teclado com Arduíno		
	Investigadores:	Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa e Camila Ferreira Alves
	Apoio técnico:	Yeda Regina Venturini (USP)
	Objetivo:	Conduzir uma avaliação abrangente da segurança da comunicação entre o teclado e a placa-mãe nas urnas eletrônicas. O teste visa garantir a integridade do processo eleitoral, respeitando as regulamentações e autorizações legais necessárias. Para isso, será realizada a análise da transmissão de dados, o protocolo criptográfico, possíveis padrões nos sinais e a avaliação da integridade física do *hardware* envolvido.
	Etapas Propostas:	1. Interconectar um arduíno entre o teclado e a placa-mãe; 2. Capturar os dados transitados entre teclado e a placa-mãe; 3. Analisar os dados coletados com o objetivo de violar o sigilo.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS para geração de mídia de carga e votação. Autorização para remoção do lacre físico e abertura do gabinete da urna eletrônica.

	Considerações técnicas:	Apesar de várias tentativas, não foi possível executar a primeira etapa do plano devido à dificuldade de identificação dos pinos e retransmissão de sinal pelo Arduíno no mesmo padrão recebido pelo teclado. A comunicação entre o teclado do eleitor e a placa-mãe é autenticada e cifrada. Portanto, ainda que fosse feita a retransmissão de sinal pelo Arduíno, não seria possível expor a digitação feita pelo(a) eleitor(a), tampouco alterá-la.

PLANO DE TESTE 29: Tentativa de reconhecimento das teclas digitadas usando IA		
	Investigadores:	Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa e Camila Ferreira Alves
	Apoio técnico:	Yeda Regina Venturini (USP)
	Objetivo:	Avaliar a segurança do sistema, concentrando-se na detecção de teclas pressionadas por meio de ataques de canal lateral baseados em áudio. O escopo abrange a identificação específica das urnas a serem testadas, com o objetivo claro de analisar a resiliência do sistema contra potenciais vulnerabilidades relacionadas à captura de áudio durante o processo de votação. A metodologia envolve o uso de equipamento de gravação de áudio para registrar as frequências acústicas geradas pelas teclas durante a interação com o teclado das urnas eletrônicas. A coleta de dados ocorre em ambientes simulados, replicando condições realistas de uso, garantindo que o equipamento de gravação seja operado de maneira não intrusiva e sem acesso à internet. A análise de dados inclui o processamento de áudio para isolar as teclas pressionadas e a aplicação de técnicas de aprendizado profundo para treinar um modelo capaz de identificar essas teclas a partir das amostras coletadas. A avaliação de resultados envolve a análise das detecções em relação ao comportamento normal das urnas, com a atribuição de níveis de gravidade e risco às vulnerabilidades identificadas.
	Etapas Propostas:	1. Capturar os sinais sonoros emitidos pelo teclado da urna, usando teclas conhecidas; 2. Submeter os sinais obtidos para aprendizado da IA (inteligência artificial); 3. Capturar outros sinais sonoros do teclado, não conhecidos, para reconhecimento pela IA, violando, assim, o sigilo.
	Resultado:	Executado COM achado.
	Flexibilizações de segurança:	Nenhuma.
	Considerações técnicas:	O plano de testes evidenciou a possibilidade de identificação de teclas do terminal do eleitor, utilizando o som emitido pelo pressionamento da tecla (clique mecânico). Foi observada uma média de acurácia de aproximadamente 50%, testando com modelos de urnas diferentes e posições variadas de microfone, mas restrito às teclas numéricas 1, 2, 3 e 4. Entende-se que, embora o modelo possa ser promissor em caso de um

		aprendizado maior de máquina, com maior amostra e mais tempo, a aplicabilidade no caso real ainda seria o maior obstáculo. Não houve tentativa ou ação que pudesse adulterar a destinação dos votos, pois o plano só previa a identificação da tecla pressionada apenas pelo seu som. É importante destacar que, para uma violação bem-sucedida do anonimato do voto do(a) eleitor(a), é preciso que todas as teclas por ele(a) digitadas sejam identificadas, uma vez que cada voto é composto de múltiplos dígitos. Em outras palavras, um modelo de IA precisa ser capaz de identificar as teclas com acurácia bastante elevada. Há ainda o grande obstáculo da captura do som em uma seção eleitoral, com microfones direcionais (que possibilitariam um menor ruído) ou de qualquer outro tipo. Isso porque seria complexo manter um microfone sem ser detectado na cabina (o que seria identificado pelo procedimento de inspeção da cabina, realizado pelo menos cinco vezes ao longo do dia da votação) ou em outro local, como um microfone direcional posicionado atrás do(a) eleitor(a), orientada para o painel frontal da urna.
	Parecer Comissão Avaliadora:	Considerando que não houve impacto ou aplicabilidade de eventual achado, não houve recomendação para verificação de solução no Teste de Confirmação.

Obs.: O resultado de 70% de acurácia citado no relatório da Comissão Avaliadora refere-se a testes efetivados apenas pelo grupo fora do ambiente de testes, sem acompanhamento da equipe técnica e em um único modelo de urna.

PLANO DE TESTE 30: Teste de capacidade do teclado da urna eletrônica em receber múltiplas entradas simultâneas		
	Investigadores:	André Mário dos Reis dos Santos, Alexandre Zago Boava e Diego Vergaças de Sousa Carvalho
	Apoio técnico:	Nelson Yamamoto (USP)
	Objetivo:	Testar o funcionamento do teclado da urna eletrônica com o intuito de garantir que o registro corresponda corretamente às teclas acionadas no teclado, mesmo sob condições não usuais de acionamento dessas.
	Etapas Propostas:	1. Acionar grupos de teclas simultaneamente, inicialmente com duas teclas e mantendo uma pressionada. Em seguida, pressionar outras novas teclas, uma de cada vez. A cada nova tecla pressionada, verificar: se o novo dígito mostrado na tela corresponde à tecla pressionada; se as teclas BRANCO, CORRIGE e CONFIRMA funcionam corretamente; e, ao manter todas as teclas pressionadas, verificar qual é o comportamento do equipamento; 2. Reproduzir o teste do item (1) com mais uma tecla mantida pressionada; 3. Reproduzir o item (2), com mais uma tecla pressionada, e assim por diante, de modo a caracterizar uma breve análise combinatória das teclas pressionadas, testando assim a capacidade do teclado de lidar com várias entradas ao mesmo tempo; 4. Observar o comportamento do *software* ao manter uma tecla ou um grupo de teclas pressionado(a) por um período longo.

	Resultado:	Executado COM achado.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS para geração de mídia de carga e votação. Autorização para remoção do lacre físico e abertura do gabinete da urna eletrônica.
	Considerações técnicas:	O plano de testes evidenciou o correto funcionamento do teclado da urna, expresso como requisito do edital de licitação para fabricação do equipamento, que consiste na impossibilidade de acionamento de simultâneo de duas teclas. Em nenhuma hipótese, há a efetivação da digitação por teclas por engano quando outras estão acionadas. Não há, portanto, qualquer ameaça à integridade do voto. Da mesma forma, não há qualquer risco ao anonimato do voto.
	Parecer Comissão Avaliadora:	Considerando que não houve impacto ou aplicabilidade de eventual achado, não houve recomendação para verificação de solução no Teste de Confirmação.

PLANO DE TESTE 31: Inconsistência de *Software*		
	Investigadores:	Avelino Francisco Zorzo (não compareceu), Ariel Rossetto Ril e Daniel Dalalana Bertoglio
	Apoio técnico:	Ryan Weege Achjian (USP)
	Objetivo:	Avaliação se o *software* carregado na urna eletrônica é o mesmo que foi lacrado na cerimônia pública.
	Etapas Propostas:	1. Listar todos arquivos em um diretório usando um script Python3; 2. Ler o conteúdo dos arquivos listados; 3. Computar o SHA512 de cada conteúdo lido; 4. Computar o valor Base64 de cada SHA512; 5. Comparar os resultados com os *hashes* públicos assinados.
	Resultado:	Executado sem achados.
	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS para geração de mídia de carga e votação. Fornecimento dos *hashes* publicados no *site* do TSE.
	Considerações técnicas:	O *script* desenvolvido pelos investigadores é utilizado na mídia interna da urna e resulta em 100% de sucesso, ou seja, o *hash* calculado de todos os arquivos internos é exatamente igual àqueles publicados no *site* do TSE.

PLANO DE TESTE 32: *Ab imitio Invalidi, Post Validi* *	
Investigador:	Guilherme Henrique dos Santos
Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
Objetivo:	Modificar a tabela de correspondências visualizada no GEDAI.
Etapas Propostas:	1. Analisar o código-fonte do GEDAI para inferir meios de se alterar a tabela de correspondências; 2. Modificar a tabela de correspondências.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Nenhuma.
Considerações técnicas:	Este plano de teste foi proposto durante o TPS. Após analisar o código-fonte do GEDAI e sua documentação, com foco nos códigos com descrições DDL das tabelas de correspondência no GEDAI, o investigador constatou que não era possível alterar o valor de correspondências.

(*) Plano de teste apresentado e aprovado durante a realização do TPS 2023

PLANO DE TESTE 33: *Omnia Invalidi est* *	
Investigador:	Guilherme Henrique dos Santos
Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
Objetivo:	Verificação dos números de correspondência contidos no arquivo digital do BUSA.
Etapas Propostas:	1. Gerar uma mídia de resultado, configurando a urna para acionar o App SA; 2. Iniciar o SA (em urna disponível) e iniciar processo de digitação de BU (boletim de urna); 3. Apurar o resultado e gerar o arquivo de BUSA; 4. Conferir a existência de números de correspondência embarcados no arquivo de BUSA gerado.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Concedido livre acesso ao *app* SA.
Considerações técnicas:	Este plano de teste foi proposto durante o TPS. No BUSA, apenas o número de correspondência da urna que executou o SA é registrado. Como restrição procedimental complementar, o envio sempre possui uma justificativa do juiz. Foi apresentada sugestão de melhoria pelo investigador para que *"seja colocada no BUSA campo para correspondência de carga para ser possível identificar por quais urnas passaram determinada votação"*, a qual foi submetida à analise da equipe técnica do TSE.

(*) Plano de teste apresentado e aprovado durante a realização do TPS 2023

PLANO DE TESTE 34: *Suffragium non est relates* *	
Investigador:	Guilherme Henrique dos Santos
Apoio técnico:	Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)
Objetivo:	Verificar se um(a) eleitor(a) já votou, após introduzir uma mídia de votação que não tenha sido clonada antes do voto na urna eletrônica.
Etapas Propostas:	1. Gerar mídia de votação; 2. Preparar urna para votação; 3. Iniciar a votação, inserindo um voto; 4. Clonar mídia de votação; 5. Reinserir a mídia de votação e adicionar um voto; 6. Remover a mídia e inserir a mídia clone; 7. Tentar habilitar o(a) mesmo(a) eleitor(a) que inseriu o primeiro voto.
Resultado:	Executado sem achados.
Flexibilizações de segurança:	Nenhuma.
Considerações técnicas:	Este plano de teste foi proposto durante o TPS. O investigador verificou se havia um procedimento de sincronização, entre a mídia interna e a externa, do estado da votação. Apesar de conectar externamente uma mídia de votação, sem o voto mais recente, a urna ainda tinha o seu conteúdo sincronizado pelo conteúdo da mídia interna.

(*) Plano de teste apresentado e aprovado durante a realização do TPS 2023

PLANO DE TESTE 35: Escalação de privilégio no Windows (SIS) *	
Investigadores:	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
Apoio técnico:	Gabriel Soares dos Santos Nunes (USP) e Mlexener Bezerra Romeiro (TRE/PE)
Objetivo:	Atacar o SIS promovendo escalação de privilégios por meio da impressão da lista de certificados no VAP do SIS-desktop.
Etapas Propostas:	1. Acessar máquina SIS logada com usuário padrão; 2. Acessar a ferramenta verificador de autenticação de programas, no gerenciador de aplicações seguras do SIS-desktop; 3. Clicar no menu superior "Exibir"; 4. Clicar em "Lista de certificados válidos"; 5. Clicar no botão "imprimir"; 6. Clicar no ícone de "impressão", canto superior esquerdo; 7. Copiar pastas com arquivos e subpastas, no Explorer aberto, com acesso administrativo no sistema; 8. Mover arquivos protegidos para pasta controlada pelo atacante.
Resultado:	Executado COM achado.

	Flexibilizações de segurança:	Fornecimento de usuário/senha do SIS.
	Considerações técnicas:	Este plano de teste foi proposto durante o TPS. O VAP possui direito de solicitar ao SIS a abertura e fechamento de proteção (*open protection e close protection*) de acesso a todas as pastas de arquivos. Isto é necessário para que possa realizar a leitura e verificação dos arquivos assinados. Ao final da leitura dos arquivos, o VAP disponibilizado no TPS deveria invocar o método "close protection" antes de apresentar o relatório de conferência de assinaturas. Identificamos, no código-fonte, que o fechamento de proteção é solicitado, no entanto, com a recente mudança do componente utilizado para leituras de arquivos PDF, o fechamento de proteções não ocorre no momento esperado. Os investigadores exploraram essa característica para ter acesso ao conteúdo dos arquivos. 0 privilégio permitiu aos investigadores ler, alterar ou apagar arquivos. Registre-se que a eventual alteração do conteúdo de arquivos assinados provocaria inconsistência e bloqueio do equipamento pelo SIS. Alterações também seriam detectadas com ouso do VAD ou VAP. A visualização dos arquivos mantidos no SIS não produz efeito sobre a integridade ou o anonimato do voto. Eventual alteração de arquivos ensejaria incoerência de assinatura digital, uma vez que os arquivos são verificados pelo Gedai-UE e pela urna no momento de sua execução.
	Parecer Comissão Avaliadora:	“Um aplicativo que é executado com determinados privilégios, acima de uma conta comum, deve estar protegido de forma a manter todas as regras de segurança previstas consistentes. Recomenda-se uma análise da questão apresentada para que o processo seja revisto e mantido consistente com os privilégios propostos, evitando eventos não previstos que possam obstruir os procedimentos planejados e projetados. O conceito aplicado para empregar os processos ‘open protection’ e ‘close protection’ em ambientes hostis necessita ser revisto.” A Comissão Avaliadora recomenda retorno no Teste de Confirmação para nova verificação, em versão ajustada do sistema eleitoral, da efetividade das correções a serem implementadas.

(*) Plano de teste apresentado e aprovado durante a realização do TPS 2023

DA REALIZAÇÃO DO TESTE PÚBLICO DE SEGURANÇA DA URNA – EDIÇÃO 2023

▪ Da semana de execução dos testes – de 27 de novembro a 02 de dezembro de 2023

O Teste Público de Segurança da Urna de 2023 – semana de execução dos planos de testes – aconteceu no período de 27 de novembro a 1º de dezembro de 2023, na sede do Tribunal Superior Eleitoral, tendo sido prorrogado por mais um dia, a pedido de dois grupos de investigadores.

O TPS 2023 foi a 7ª edição realizada e alcançou um recorde de pré-inscrições, totalizando 85, divididos em 29 pré-inscrições individuais e 56 participantes reunidos em 15 grupos, sendo 18 mulheres e 67 homens.

Ao todo, foram apresentados 48 planos de testes, dos quais, após análise da Comissão Reguladora e finalizados os prazos recursais, 34 foram aprovados para serem executados durante a semana do TPS, restando 40 participantes inscritos.

Considerando a desistência de 4 inscritos e 3 faltantes, bem como a aprovação de 4 novos planos e a não execução de 3 planos na semana do Teste Público de Segurança da Urna, tem-se, durante a semana do TPS, 33 participantes e 35 planos executados.

Dos planos executados, foram apresentados 7 supostos achados, dos quais 5 (3 do grupo da Polícia Federal e 2 do grupo da UFMS) foram recomendados pela Comissão Avaliadora para análise das equipes técnicas do TSE como possíveis pontos de melhoria e, consequentemente, para serem executados novamente no Teste de Confirmação, com o objetivo de verificar, em versão ajustada do sistema eleitoral, a efetividade das correções que foram implementadas pelas equipes do TSE. São eles:

1) Grupo Polícia Federal:

Planos/achados:

- Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020 (Achado n. 177);
- Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI (Achado n. 178);
- Executar código espúrio na urna eletrônica modelo 2020 (Achado n. 179).

2) Grupo UFMS:

Planos/achados:

- Violar a confidencialidade, integridade e disponibilidade das informações no Python do *Software* JE-Connect (Achado n. 79);
- Escalação de privilégio no Windows – SIS (Achado n. 168).

▪ Do Teste de Confirmação – de 15 a 17 de maio de 2024

Os achados aceitos pela Comissão Avaliadora foram avaliados pelas equipes técnicas da Secretaria de Tecnologia da Informação do TSE e do TRE/TO (no caso da JE-Connect), que buscaram soluções efetivas e as implementaram de acordo com os processos utilizados no desenvolvimento dos sistemas eleitorais.

Feito isso, para que as soluções fossem validadas, foi realizado, no período de 15 a 17 de maio de 2024, o Teste de Confirmação. Conforme prevê o Edital n° 1/2023 do TPS, as investigadoras e os investigadores dos grupos da Universidade Federal do Mato Grosso do Sul (G-4) e da Polícia Federal (G-5) foram convocados para retornarem ao TSE e repetirem, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade ou a fraude.

Nesse período, os investigadores e a investigadora verificaram os ajustes feitos pelas equipes da STI do TSE e constataram que as melhorias implementadas contribuíram para o aperfeiçoamento da urna eletrônica e dos sistemas eleitorais.

Sendo assim, uma vez realizados os novos testes e tendo sido constatadas as melhorias implementadas, a investigadora e os investigadores assinaram o Termo de Confirmação previsto no § 6º do art. 37 do Edital n° 1/2023, do TPS2023, que é a fase final do TPS.

▪ Resumo das ações implementadas pelas equipes técnicas da STI/TSE:

1) Grupo Polícia Federal:

- **Plano de Teste: Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020 (Achado n. 177)**
- **Plano de Teste: Executar código espúrio na urna eletrônica modelo 2020 (Achado n. 179)**

Ações da equipe técnica do TSE para os dois achados: Durante a realização do TPS 2023, a equipe da Polícia Federal foi capaz de identificar uma vulnerabilidade no sistema de inicialização da urna. Por meio de um dispositivo conectado à urna, foi possível entender como o equipamento faz a leitura da mídia de aplicação. Com isso, foi possível fazer uma modificação no *bootloader* entre as etapas de validação de assinatura digital e de execução. Em outras palavras, em um ambiente de laboratório, foi possível alterar a porção de *software* responsável por iniciar o sistema operacional da urna. A capacidade de modificação do *bootloader* permitiu à investigadora e aos investigadores revelar uma chave usada para a decifração do *kernel* do sistema operacional.

A solução implementada pelo TSE foi a modificação do BIOS/UEFI das urnas para que as etapas de validação de assinatura e execução do *bootloader* fossem feitas com um único acesso à mídia de aplicação. Além disso, o *bootloader* também foi modificado para não carregar qualquer módulo, apenas para executar o *kernel* do sistema operacional. Dessa forma, não é mais possível alterar o *bootloader*, preservando-se a total integridade do sistema de inicialização da urna, assim como o sigilo de chaves do sistema.

- **Plano de Teste: Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI (Achado n. 178)**

Ações da equipe técnica do TSE: O TSE desenvolveu uma solução que identifica o ataque em curso e apaga o *chip* de computador onde se encontram as chaves necessárias para acesso aos dados da Justiça Eleitoral. Mitiga-se, dessa forma, o acesso aos dados do sistema GEDAI por pessoas não autorizadas.

A solução implementada foi a identificação na alteração de uma configuração de proteção na BIOS do equipamento, quando detectado o desligamento desta proteção, o sistema reage de forma a remover as chaves de criptografia armazenadas no chip TPM da estação inviabilizando, com isso, a extração da chave BitLocker. Ademais, foi implementada uma proteção adicional de segundo fator na inicialização do computador.

2) Grupo UFMS

- **Plano de Teste: Violar a confidencialidade, integridade e disponibilidade das informações no Python do *software* JE-Connect (Achado n. 79)**

Ações da equipe técnica da JE-Connect: A atualização do sistema operacional Linux Debian, versão 12, alterou o comportamento padrão do *reboot* e isso permitiu que os investigadores fizessem até nove tentativas, o que levou à interrupção com o comando CTRL+C.

A JE-Connect adota, em sua implementação, um controle que, após 3 (três) tentativas de inserção do PIN fracassadas, o sistema reinicializa automaticamente, e isso é o comportamento padrão do sistema.

Como solução, foi realizada a correção efetiva no comando de *reboot*, adequando a operação ao seu comportamento padrão.

- **Plano de Teste: Escalação de privilégio no Windows (SIS) (Achado n. 168)**

Ações da equipe técnica do TSE: Foi identificado, no Verificador de Autenticação de Programas - VAP, que, no momento de impressão de relatórios, era possível, por meio da janela de arquivos, navegar em pastas que deveriam estar sem acesso para determinado(a) usuário(a). Para correção, foi implementada limitação de privilégios, de modo a impedir o acesso indevido.

Todas as implementações acima descritas foram ratificadas pela investigadora e pelos investigadores durante o Teste de Confirmação, tendo sido, portanto, assinado por todos o Termo de Confirmação de que trata o 6º do art. 37 do Edital n° 1/2023 do TPS2023.

RESUMO DOS NÚMEROS DO TESTE PÚBLICO DE SEGURANÇA DA URNA – EDIÇÃO 2023

Execução dos Planos de Testes – 27 de novembro a 02 de dezembro de 2023	
Total de pré-inscritos	**85**
Total de planos apresentados durante a fase de pré-inscrição	**48**
Total de inscrições aprovadas após fase recursal	**16**
Total de inscritos aprovados após fase recursal	**40**
Total de planos aprovados após fase recursal	**34**
Total de inscrições aprovadas que participaram da semana do TPS	**13**
Total de inscritos aprovados que participaram da semana do TPS	**33**
Total de planos executados na semana do TPS	**35**
Novos planos apresentados durante a semana	**6**
Total de supostos achados apresentados	**7**
Total de sugestões de melhoria	**6**
Solicitação de extensão de prazo para a execução de planos	**2**
Formulários recebidos durante os testes	**178**
Pedidos deferidos ou deferidos com ressalva	**172**

Teste de Confirmação – 15 a 17 de maio de 2024	UFMS	PF	Total
Investigadoras e investigadores	**04**	**05**	**09**
Planos executados novamente	**02**	**03**	**05**
Termos de Confirmação assinados	**02**	**03**	**05**
Formulários recebidos durante os testes	**06**	**09**	**15**
Pedidos deferidos	**04**	**08**	**12**
Pedidos indeferidos	**01**	**00**	**01**
Sugestões de melhoria	**01**	**01**	**02**

Além das investigadoras e dos investigadores, o TPS 2023 contou com a participação direta de membros das Comissões Reguladora, Avaliadora, Organizadora e de Comunicação Institucional, das equipes técnicas da Secretaria de Tecnologia da Informação do TSE, de técnicos dos TREs, técnicos da USP, representantes da Abin e de mais 23 áreas diretamente envolvidas na organização e execução do evento.

Documento consolidado e revisado pelo
Núcleo Estratégico de Comunicação de Informática – Neci
Secretaria de Tecnologia da Informação – STI

Tribunal Superior Eleitoral