Tribunal Superior Eleitoral

C O M P Ê N D I O

Teste Público de Segurança 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Brasília
TSE
2026

© 2026 Tribunal Superior Eleitoral

É proibida a reprodução total ou parcial desta obra sem a autorização expressa das autoras e dos autores.

Secretaria de Gestão da Informação e do Conhecimento
SAFS, Quadra 7, Lotes 1/2, 1º andar
Brasília/DF – 70095-901
Telefone: (61) 3030-9225

Secretária-Geral da Presidência
Andréa Maciel Pachá

Diretor-Geral da Secretaria do Tribunal
Miguel Ricardo de Oliveira Piazzi

Secretário de Gestão da Informação e do Conhecimento
Cleber Schumann

Coordenador de Editoração e Publicações
Washington Luiz de Oliveira

Unidade responsável pelo conteúdo
Secretaria de Tecnologia da Informação/TSE

Capa e projeto gráfico
Bruna Pagy
Seção de Editoração e Programação Visual (Seprov/Cedip/SGIC)

Diagramação
Leandro Morais
Seção de Editoração e Programação Visual (Seprov/Cedip/SGIC)

Revisão
Dara Abreu e Elisa Maria Silveira
Seção de Preparação e Revisão de Conteúdos (Seprev/Cedip/SGIC)

TRIBUNAL SUPERIOR ELEITORAL

Presidente
Ministra Cármen Lúcia

Vice-Presidente
Ministro Nunes Marques

Ministros
Ministro André Mendonça
Ministro Antonio Carlos Ferreira
Ministro Ricardo Villas Bôas Cueva
Ministro Floriano de Azevedo Marques
Ministra Estela Aranha

Sumário

1. APRESENTAÇÃO 6

2. TESTE PÚBLICO DE SEGURANÇA 6

2.1 Etapas do Teste Público de Segurança 6

2.1.1 Fase de preparação 7

2.1.2 Fase de realização 7

2.1.3 Fase de avaliação 7

2.2 Normas reguladoras do TPS 7

3. TESTE PÚBLICO DE SEGURANÇA 2023 8

3.1 Comissões do TPS 2023 10

3.1.1 Comissão Organizadora – Portaria-TSE n. 672/2023: 10

3.1.2 Comissão Reguladora – Portaria-TSE n. 672/2023: 11

3.1.3 Comissão de Comunicação Institucional – Portaria-TSE n. 672/2023: .. 11

3.1.4 Comissão Avaliadora – Portaria-TSE n. 701/2023, alterada pelas Portarias-TSE n. 950/2023 e 397/2024: I – representantes da Presidência do TSE: 11

3.2 Audiência pública 12

4. PLANOS DE TESTE APRESENTADOS 13

5. TESTE DE CONFIRMAÇÃO – TPS 2023 16

5.1 Resumo dos números do Teste Público de Segurança 2023 18

6. RESUMO DAS EDIÇÕES TPS: 2009, 2012, 2016, 2017, 2019, 2021 e 2023 19

6.1 1ª Edição – 2009 19

6.2 2ª Edição – 2012 20

6.3 3ª Edição – 2016 20

6.4 4ª Edição – 2017 21

6.5 5ª Edição – 2019 21

6.6 6ª Edição – 2021 22

6.7 7ª Edição – 2023 22

7. ANEXOS 24

7.1 Anexo A – Res.-TSE n. 23.444/2015 24

7.2 Anexo B – Lei n. 9.504/1997 28

7.3 Anexo C – Res.-TSE n. 23.542/2017 63

7.4 Anexo D – Portarias das comissões 64

7.5 Anexo E – Aviso de audiência pública 70

7.6 Anexo F – Editais 71

7.7 Anexo G – Lista de pré-inscrições 85

7.8 Anexo H – Análise dos planos de testes 87

7.9 Anexo I – Resultado dos recursos 89

7.10 Anexo J – Planos de testes aprovados 90

7.11 Anexo K – Lista definitiva de inscrições 251

7.12 Anexo L – Lista de presença – TPS 252

7.13 Anexo M – Planos de testes apresentados na semana de execução 260

7.14 Anexo N – Relatório técnico parcial do TSE 272

7.15 Anexo O – Relatório parcial da USP 306

7.16 Anexo P – Relatório parcial da Comissão Avaliadora 366

7.17 Anexo Q – Lista de presença – Teste de Confirmação 386

7.18 Anexo R – Termos de confirmação 388

7.19 Anexo S – Relatório final da Comissão Avaliadora 393

7.20 Anexo T – Relatório técnico final do TSE 403

7.21 Anexo U – Relatório final da USP 439

7.22 Anexo V – Res.-TSE n. 23.673/2021 499

7.23 Anexo W – Res.-TSE n. 23.728/2024 528

7.24 Anexo X – Relatório de esclarecimento 534

1. APRESENTAÇÃO

O processo eleitoral é o pilar fundamental da democracia. Por meio dele, as cidadãs e os cidadãos exercem seu direito de escolha, selecionando as(os) representantes que governarão e legislarão em seu nome.

A importância desse processo reside no fato de ser este um mecanismo que permite a expressão da vontade popular de forma pacífica e organizada.

Nesse contexto, a lisura e a segurança no processo eleitoral são essenciais para garantir a legitimidade e a confiança no sistema democrático, assegurando que as eleições sejam justas, transparentes e livres de fraudes.

2. TESTE PÚBLICO DE SEGURANÇA

O Teste Público de Segurança (TPS), regulamentado pela Res.-TSE n. 23.444, de 30 de abril de 2015 (Anexo A), é parte do processo eleitoral e visa fortalecer a confiabilidade, a transparência e a segurança da captação, apuração e transmissão dos votos, além de melhorar os sistemas eleitorais.

Por meio do TPS, é oferecida aos(às) participantes a oportunidade de identificar eventuais vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato do voto, para que essas possam ser corrigidas pelas equipes técnicas do TSE antes das eleições.

Nos termos do art. 2º da Res.-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 para o recebimento de arquivos, lacrados em cerimônia pública, conforme definido no § 2º do art. 66 da Lei n. 9.504/1997 (Anexo B), incluindo o *hardware* da urna e seus *softwares* embarcados.

Realizado desde 2009, o TPS faz parte do Ciclo de Transparência Democrática e é aberto às cidadãs e aos cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, conforme definido em edital, e é realizado, preferencialmente, no segundo semestre dos anos anteriores aos pleitos eleitorais.

Desde a sua regulamentação, já foram realizadas 7 edições do Teste Público de Segurança, nos anos de 2009, 2012, 2016, 2017, 2019, 2021 e 2023.

Pautado na transparência institucional, um dos pilares de atuação do TSE e de toda a Justiça Eleitoral brasileira, o principal objetivo do Teste Público de Segurança é contribuir com o desenvolvimento dos sistemas eleitorais, propiciando melhorias contínuas no processo eleitoral como um todo.

2.1 Etapas do Teste Público de Segurança

Conforme disposto no art. 17 da Res.-TSE n. 23.444/2015, o TPS é dividido em três fases: preparação, realização e avaliação.

2.1.1 Fase de preparação

Na fase de preparação, são realizadas as seguintes ações ou eventos:

I – audiência pública, com o objetivo de esclarecer as regras do TPS definidas na resolução;

II – publicação do edital, que deverá contemplar as regras específicas e as datas para a realização de todas as demais fases e ações do evento;

III – palestra informativa sobre o sistema eletrônico de votação, com o objetivo de subsidiar os(as) eventuais participantes sobre o funcionamento do sistema eleitoral;

IV – apresentação, em ambiente controlado, dos códigos-fonte dos sistemas eleitorais que farão parte do TPS;

V – geração de versão a ser utilizada no TPS, observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas;

VI – preparação e configuração dos sistemas adicionais que serão utilizados no teste e na elaboração dos respectivos planos de teste; e

VII – recebimento das inscrições e dos planos de teste das técnicas e dos técnicos que desejam participar do evento.

2.1.2 Fase de realização

Na fase de realização, as técnicas e os técnicos com inscrições homologadas comparecem ao TSE para o Teste Público de Segurança e executam os planos de teste previamente definidos, seguindo as regras previstas no edital.

Ao final da execução dos planos, cada investigadora e investigador apresenta relatório das ações executadas e dos resultados alcançados.

As investigadoras e os investigadores ou os grupos que identificarem alguma falha, vulnerabilidade explorada ou fraude no sistema eletrônico de votação deverão, ao final, fazer sugestões de melhoria relacionadas aos erros encontrados.

2.1.3 Fase de avaliação

Na fase de avaliação, a Comissão Avaliadora elabora relatório contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas durante o TPS.

2.2 Normas reguladoras do TPS

A Res.-TSE n. 23.444, de 30 de abril de 2015, alterada pela Res.-TSE n. 23.542 (Anexo C), de 18 de dezembro de 2017, foi publicada com o objetivo de instituir a realização periódica do Teste Público de Segurança nos sistemas eleitorais como parte do ciclo de desenvolvimento dos sistemas de votação e apuração, o qual deve acontecer,

preferencialmente, no segundo semestre dos anos que antecedem os pleitos eleitorais. A resolução também indica a elaboração de edital específico para cada uma das edições do teste.

Em 2017, a Res.-TSE n. 23.542/2017 alterou a norma matriz com o objetivo de incluir a convocação de diversas instituições – a saber: os partidos políticos, as coligações, a Ordem dos Advogados do Brasil, o Ministério Público, o Congresso Nacional, o Supremo Tribunal Federal, o Ministério da Transparência e a Controladoria-Geral da União, o Departamento de Polícia Federal, a Sociedade Brasileira de Computação e o Conselho Federal de Engenharia e Agronomia – para, havendo interesse, participar do TPS ou acompanhar os trabalhos, na forma regulamentada.

3. TESTE PÚBLICO DE SEGURANÇA 2023

A edição de 2023 foi organizada e executada conforme os principais marcos contidos no cronograma do Teste Público de Segurança 2023-2024 (figura abaixo).

A fase de realização do TPS aconteceu no período de 27 de novembro a 1º de dezembro de 2023, na sede do Tribunal Superior Eleitoral, e foi estendida por mais um dia, a pedido de dois grupos de investigadores(as).

Essa edição registrou recorde de participantes: 85 pré-inscrições, incluindo 29 individuais e 56 em grupos – o maior número já alcançado.

Dos 85 pré-inscritos, restaram 40 inscritos após a análise dos planos de ataque pela Comissão Reguladora. Inicialmente, foram apresentados 48 planos de teste e, após a decisão da referida comissão e o fim das fases recursais, restaram 34 planos aprovados para execução.

Durante a semana de execução dos planos de teste, considerando as desistências de participantes e a apresentação de novos planos, registraram-se 33 investigadoras(es) e 35 planos de teste executados, tendo sido apresentados 7 supostos achados (detalhados no item 5 – Teste de Confirmação).

Depois da análise da Comissão Avaliadora, cinco dos supostos achados foram recomendados para análise das equipes técnicas do TSE como possíveis pontos de melhoria:

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).

Cabe registrar que, em 2023, as inscritas e os inscritos puderam testar o modelo da urna eletrônica 2020, cuja estreia foi no último pleito geral; e o modelo 2022, utilizado pela primeira vez nas Eleições Municipais 2024.

O período de execução dos planos foi encerrado pelo então diretor-geral do TSE à época, Rogério Augusto Viana Galloro, que apresentou levantamento da semana e entregou o certificado de participação, assinado pelo ministro presidente, a todas as investigadoras e a todos os investigadores presentes. Na sequência, finalizou destacando a importância da realização do TPS para a sociedade e para a democracia: "É uma iniciativa fundamental do TSE para o aprimoramento da nossa capacidade de transparência e de realização de uma eleição capaz de transportar a vontade do eleitor com confiança e credibilidade".

Ao todo, o evento contou com a participação de mais de 200 pessoas, entre investigadoras, investigadores e integrantes das comissões Organizadora, Reguladora, Avaliadora e de Comunicação Institucional; equipes técnicas da Secretaria de Tecnologia da Informação do TSE; técnicas e técnicos dos TREs e da Universidade de São Paulo (USP); representantes da Agência Brasileira de Inteligência (Abin); e mais 23 áreas diretamente envolvidas na organização e execução do evento.

3.1 Comissões do TPS 2023

A Res.-TSE n. 23.444/2015 define a atuação e as atribuições das quatro comissões previstas no normativo: Comissão Organizadora, Comissão Reguladora, Comissão Avaliadora e Comissão de Comunicação Institucional.

Nesta edição do TPS, essas comissões foram instituídas pelas Portarias-TSE n. 672 e 701, esta última alterada pelas Portarias-TSE n. 950/2023 e 397/2024 (Anexo D), com as(os) seguintes integrantes:

3.1.1 Comissão Organizadora – Portaria-TSE n. 672/2023:

a) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral – coordenador dos trabalhos;

b) Simone Ferreira de Almeida Siqueira (Cosen/SAD), representante da Secretaria de Administração;

c) Geni Maria Péres Lobato (Gab/SAD), representante da Secretaria de Administração;

d) João Rodrigues de Magalhães (SPJ), representante da Secretaria de Polícia Judicial;

e) Giselly Siqueira (Secom), representante titular da Secretaria de Comunicação e Multimídia;

f) Cecília Malheiros de Melo (Secom), representante suplente da Secretaria de Comunicação e Multimídia;

g) Luciano Teixeira Andrade (Coinf/STI), representante da Secretaria de Tecnologia da Informação;

h) Andréa Gonçalves Barbosa (Neci/STI), representante da Secretaria de Tecnologia da Informação;

i) Renato Barros de Carvalho (ACP), representante da Assessoria de Cerimonial da Presidência;

j) Washington Luiz de Oliveira (Cedip/SGIC), representante da Secretaria de Gestão da Informação e do Conhecimento;

k) Isabella Dantas Sinotti (Cedip/SGIC), representante da Secretaria de Gestão da Informação e do Conhecimento; e

l) Maurício Miranda Sá (Seeve/Coede), representante da Secretaria de Gestão de Pessoas.

3.1.2 Comissão Reguladora – Portaria-TSE n. 672/2023:

a) Júlio Valente da Costa Júnior (STI), representante da Secretaria de Tecnologia da Informação – coordenador dos trabalhos;

b) Cristiano Moreira Andrade (Coinf/STI);

c) Elmano Amâncio de Sá Alves (AGC/STI);

d) Rafael Fernandes de Barros Costa Azevedo (Cotel/STI);

e) José de Melo Cruz (CSEle/STI);

f) Rodrigo Carneiro Munhoz Coimbra (Sevin/Cotel/STI);

g) Marcelo Carneiro Rodrigues (SDCiber/Coinf/STI);

h) Ivanildo Ferreira Gomes (Sesap/Coinf/STI);

i) Alberto Araújo Cavalcante Neto (Setot/CSEle/STI);

j) Vinícius Salustiano Alves dos Santos (Seint/CSEle/STI);

k) Carlos Eduardo Miranda Zottmann (Nesc/STI); e

l) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral.

3.1.3 Comissão de Comunicação Institucional – Portaria-TSE n. 672/2023:

a) Giselly Siqueira (Secom), representante da Secretaria de Comunicação e Multimídia – coordenadora dos trabalhos;

b) Cecília Malheiros de Melo (Cimp/Secom), representante da Secretaria de Comunicação e Multimídia;

c) Júlio Valente da Costa Júnior (STI), representante da Secretaria de Tecnologia da Informação;

d) Andréa Gonçalves Barbosa (Neci/STI), representante da Secretaria de Tecnologia da Informação; e

e) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral.

3.1.4 Comissão Avaliadora – Portaria-TSE n. 701/2023, alterada pelas Portarias-TSE n. 950/2023 e 397/2024: I – representantes da Presidência do TSE:

a) Rogério Marrone de Castro Sampaio – Juiz Auxiliar da Presidência, que a presidirá; e

b) Paulo Rogério Bonini – Juiz Auxiliar da Presidência.

II – membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:

a) Jamil Salem Barbar – Professor Doutor;

b) Mamede Lima-Marques – Professor Doutor;

c) Osvaldo Catsumi Imamura – Professor Doutor; e

d) Antônio Esio Marcondes Salgado – Professor Mestre.

III – representantes do Ministério Público Federal:

a) Renato Costa Salomão – Analista do MPU/Desenvolvimento de Sistemas; e

b) Thiago Henrique Fernandes – Analista do MPU/Desenvolvimento de Sistemas.

IV – representantes da Ordem dos Advogados do Brasil (OAB): Watson Odilon Pereira de Faria – Supervisor do Processo Eletrônico;

V – representante do Congresso Nacional: Veneziano Vital do Rêgo – Senador da República.

VI – representante do Departamento de Polícia Federal:

a) Paulo César Herrmann Wanner – Perito Criminal Federal e Coordenador da CCAT/CGCIBER/DCIBER; e

b) Flávio Silveira da Silva – Perito Criminal.

VII – representante do Tribunal de Contas da União: André Luiz Furtado Pacheco – Auditor Federal de Controle Externo.

VIII – representante do Conselho Federal de Engenharia e Agronomia:

a) Rodrigo de Souza Borges – Engenheiro de Computação e Gerente de Tecnologia da Informação; e

b) Fernando Batista da Silva – Assessor de TI do Confea.

IX – representante da Sociedade Brasileira de Computação: Roberto Samarone dos Santos Araújo – Professor Doutor.

3.2 Audiência pública

A audiência pública do TPS está definida no inciso I do art. 18 da Res.-TSE n. 23.444/2015, com o objetivo de esclarecer as regras do evento.

No TPS 2023, a audiência pública realizou-se no dia 15 de setembro de 2023, das 10h às 11h, conduzida pelo Exmo. Desembargador Cesar Mecchi Morales, Juiz Auxiliar da Presidência do TSE à época, e pelo Secretário de Tecnologia da Informação, Júlio Valente, e com a participação de técnicas e técnicos da STI/TSE.

O aviso da audiência pública foi disponibilizado no sítio do TPS: https://www.justicaeleitoral.jus.br/tps/arquivos/2023/edital/aviso-de-audiencia-publica.pdf (Anexo E).

A audiência ocorreu de forma virtual, por meio do canal do TSE no YouTube, cujo conteúdo está disponível em https://youtu.be/o5tWzhr99VA.

As dúvidas puderam ser enviadas até o início do evento para o *e-mail* tps2023@tse.jus.br.

4. PLANOS DE TESTE APRESENTADOS

Ao todo, foram apresentados 54 planos de teste, sendo:

- Na fase de pré-inscrição, 48, dos quais 34 foram aprovados para execução (desses 34, houve 3 desistências, restando, portanto, 31 planos aprovados para execução);

- Na semana de execução do TPS, 6, dos quais 4 foram aprovados para execução;

- Total de planos executados na semana do TPS: 35 planos.

A Comissão Reguladora fez a análise dos planos apresentados, com base nos requisitos elencados nos incisos do art. 20 do Edital n. 1/2023 (Anexo F), abaixo transcritos:

> I. não atenderem aos objetivos específicos de alterar a destinação dos votos ou fragilizar o sigilo do voto;
>
> II. não atenderem ao objeto estabelecido no art. 2º do edital;
>
> III. não demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou
>
> IV. forem entregues após o prazo estipulado no Marco 7 do calendário do evento.

A seguir, consta a relação dos planos de testes executados no TPS:

ID	Nome	Investigadoras(es)	
1	Quebra do sigilo do voto	I-1	Aline Barbosa da Silva
2	Fragilizar sigilo do voto		
3	Invadir a mídia de carga da urna eletrônica		
4	Mídia de resultado: a confiança do cidadão na urna eletrônica e o coração da democracia	I-2	Érika Maria Rodrigues de Castro

ID	Nome	Investigadoras(es)	
5	*Fraus Omnia Corrumpit*	I-3	Guilherme Henrique dos Santos
6	*Nihil Autem Absconditum Est, Quod Non Reveletur*		
7	*Qui Duplicat, Videre Suffragio Potest*		
8	*Suffragium Simulata Substantiam Veritas Mutare Possunt*		
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
10	Execução do JE-Connect utilizando computador com sistema operacional inválido	I-5	Nicholas Barros dos Santos
11	Comportamento do JE-Connect na execução de um bot de monitoramento no computador transmissor de dados		
12	*USBExploit* – acesso a dados da urna por meio da porta USB	G-1	Marcos Roberto dos Santos Leandro Caletti (não compareceu) Rafael Noll da Silva Eduardo Bido Rhayra Rodrigues Fiorentin
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
14	Acesso à rede do TSE por intermédio do *software* JE-Connect realizando a execução de shell a partir de dispositivo USB		
15	Adulteração no JE-Connect	G-3	Vitor Aloisio do Nascimento Guia Hitatiana Maria Santiago Ferreira da Silva Guia

ID	Nome	Investigadoras(es)	
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
17	Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no *software* JE-Connect		
18	Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no *software* JE-Connect		
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		
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		
21	Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo kit JE, possibilitando comandos a partir de *scripts* em área restrita		
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
23	Extrair a chave que cifra/decifra o *kernel* da urna eletrônica modelo 2020		
24	Utilizar a chave que cifra/decifra o *kernel* da urna para alterar o Registro Digital de Voto		
25	Recuperar a chave de criptografia do *BitLocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI		
26	Alterar dados/programas nos sistemas SIS/GEDAI		
27	Ataque de *cold boot* à urna eletrônica		
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
29	Tentativa de reconhecimento das teclas digitadas usando IA		
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
31	Inconsistência de *software*	G-8	Avelino Francisco Zorzo (não compareceu) Ariel Rossetto Ril Daniel Dalalana Bertoglio

ID	Nome	Investigadoras(es)	
32	*Ab imitio Invalidi, Post Validi**	I-3	Guilherme Henrique dos Santos
33	*Omnia Invalidi est**		
34	*Suffragium non est relatus**		
35	Escalação de privilégio no Windows (SIS)*	G-4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho

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

Sobre esse item, estão anexados neste compêndio: a relação de pré-inscrições (Anexo G), a análise dos planos de testes apresentados (Anexo H), o resultado dos recursos (Anexo I), os planos de teste aprovados (Anexo J), a lista definitiva de inscrições no TPS 2023 (Anexo K) e as listas de presença das(os) participantes dessa edição (Anexo L).

Também compõe este compêndio a íntegra de todos os planos de testes aprovados e submetidos à Comissão Reguladora (Anexo J), além daqueles apresentados e aprovados durante a semana de execução dos testes (Anexo M).

Os relatórios parciais publicados no *site* do TPS 2023 também se encontram anexados neste compêndio: o relatório técnico parcial da equipe do TSE (Anexo N), o relatório parcial da equipe da USP (Anexo O) e o relatório parcial da Comissão Avaliadora (Anexo P).

5. TESTE DE CONFIRMAÇÃO – TPS 2023

O Teste de Confirmação aconteceu no período de 15 a 17 de maio de 2024, com a presença dos integrantes indicados, que retornaram à sede do TSE, repetiram os planos de testes anteriormente executados e, tendo sido constatadas as melhorias implementadas pelo TSE, assinaram o termo de confirmação (Anexo R) previsto no § 6º do art. 37 do Edital n. 1/2023 do TPS 2023.

No período entre a semana de execução dos planos e o Teste de Confirmação, as equipes técnicas do TSE desenvolveram ações para os cinco planos recomendados pela Comissão Avaliadora para verificação, com a finalidade de mitigar eventuais riscos nos sistemas eleitorais.

Segue abaixo o 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, o grupo da Polícia Federal identificou uma vulnerabilidade no sistema de inicialização da urna eletrônica. Por meio de dispositivo conectado à urna, entendeu-se como o equipamento faz a leitura da mídia de aplicação, o que viabilizou a modificação no *bootloader* entre as etapas de validação de assinatura digital e de execução. Isso quer dizer que, em um ambiente de laboratório restrito nas dependências do TSE, foi possível alterar a porção de *software* responsável por iniciar o sistema operacional da urna eletrônica. A capacidade de modificação do *bootloader* permitiu à investigadora e aos investigadores revelar a chave usada para decifrar o *kernel* do sistema operacional.

A solução técnica implementada pelo TSE consistiu na modificação do *BIOS/UEFI* das urnas eletrônicas para que as etapas de validação de assinatura e execução do *bootloader* fossem feitas com 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 eletrônica, 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: foi desenvolvida 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 consistiu na identificação da alteração de uma configuração de proteção na *BIOS* do equipamento. Quando detectado o desligamento dessa proteção, o sistema reage de forma a remover as chaves de criptografia armazenadas no *chip* TPM do computador, inviabilizando, com isso, a extração da chave *BitLocker*. Ademais, implementou-se uma proteção adicional de segundo fator na inicialização.

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 da universidade 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 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: identificou-se, no Verificador de Autenticação de Programas, que, no momento de impressão de relatórios, era possível, por meio da janela de arquivos, navegar em pastas que deveriam estar sem acesso para determinada(o) usuária(o). Para a correção, foi implementada a limitação de privilégios, de modo a impedir o acesso indevido.

Sobre esse item, estão anexados neste compêndio: a lista de presença das(os) participantes do Teste de Confirmação (Anexo Q) e os termos de confirmação (Anexo R), bem como o relatório final apresentado pela USP (Anexo U).

Sendo assim, após a implementação das soluções acima descritas, os integrantes dos grupos da Polícia Federal (denominado G-5) e da Universidade Federal de Mato Grosso do Sul (denominado G-4) foram convidados a repetirem os seus respectivos planos de teste, em versão ajustada dos sistemas eleitorais, nos termos do art. 37 do Edital n. 1/2023.

O evento foi aberto, no dia 15 de maio de 2024, pelo então diretor-geral do TSE, Rogério Augusto Viana Galloro, e encerrado, em 17 de maio de 2024, pelo secretário de Tecnologia da Informação do TSE, Júlio Valente da Costa Júnior.

Nos termos do art. 38 do Edital n. 1/2023 do TPS 2023, foram publicados o relatório de avaliação geral elaborado pelo TSE (Anexo T), o relatório final dos resultados e das conclusões do Teste Público de Segurança, elaborado pela Comissão Avaliadora (Anexo S) e o relatório de esclarecimento às recomendações proferidas pela Comissão Avaliadora do TPS 2023 (Anexo X).

5.1 Resumo dos números do Teste Público de Segurança 2023

Fase de execução dos planos de testes 27 de novembro a 2 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 inscritas(os) aprovadas(os) após fase recursal	40
Total de planos aprovados após fase recursal	34
Total de inscrições aprovadas na semana do TPS	13
Total de inscritas(os) aprovadas(os) 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

Fase de execução dos planos de testes 27 de novembro a 2 de dezembro de 2023	
Total de sugestões de melhoria	6
Solicitação de extensão de prazo para a execução de planos	2
Pedidos 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	4	5	9
Planos executados novamente	2	3	5
Termos de confirmação assinados	2	3	5
Formulários recebidos durante os testes	6	9	15
Pedidos deferidos	4	8	12
Pedidos indeferidos	1	0	1
Sugestões de melhoria	1	1	2

6. RESUMO DAS EDIÇÕES TPS: 2009, 2012, 2016, 2017, 2019, 2021 e 2023

6.1 1ª Edição – 2009

A primeira edição do Teste Público de Segurança ocorreu no período de 10 a 13 de novembro de 2009, com os seguintes números:

6.2 2ª Edição – 2012

A segunda edição do Teste Público de Segurança ocorreu no período de 20 a 22 de março de 2012, com os seguintes números:

6.3 3ª Edição – 2016

A terceira edição do Teste Público de Segurança ocorreu no período de 8 a 10 de março de 2016, com os seguintes números:

6.4 4ª Edição – 2017

A quarta edição do Teste Público de Segurança ocorreu no período de 27 a 30 de novembro de 2017, com os seguintes números:

6.5 5ª Edição – 2019

A quinta edição do Teste Público de Segurança ocorreu no período de 25 a 29 de novembro de 2019, com os seguintes números:

6.6 6ª Edição – 2021

A sexta edição do Teste Público de Segurança ocorreu no período de 22 a 27 de novembro de 2021, com os seguintes números:

6.7 7ª Edição – 2023

A sétima edição do Teste Público de Segurança ocorreu no período de 27 de novembro a 2 de dezembro, com os seguintes números:

No total, considerando todas as 7 edições, o TPS já contou com a participação de 157 investigadoras e investigadores, com 148 planos de testes apresentados e com 112 executados, resultando em 247 horas de testes públicos de segurança.

É importante destacar que o TPS é executado com as últimas versões dos sistemas e equipamentos disponíveis por ocasião do evento (versões lacradas previamente) e com os últimos modelos disponíveis de urna eletrônica.

Como procedimento integrante do processo de desenvolvimento de *softwares* adotado pelo TSE, as novas versões dos sistemas eleitorais serão geradas com as correções e evoluções decorrentes do TPS – e dos testes realizados pelas próprias equipes técnicas do TSE –, as quais são compiladas e lacradas em até 20 dias antes das eleições, nos termos da Res.-TSE n. 23.673/2021 (Anexo V), atualizada pela Res.-TSE n. 23.728/2024 (Anexo W), que dispõe sobre os procedimentos de fiscalização e auditoria do processo eletrônico de votação.

7. ANEXOS

7.1 Anexo A – Res.-TSE n. 23.444/2015

Resolução nº 23.444, de 30 de abril de 2015 – Brasília/DF

Dispõe sobre a realização periódica do Teste Público de Segurança (TPS) nos sistemas eleitorais que especifica.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das atribuições que lhe conferem o art. 23, IX, do Código Eleitoral e o art. 105 da Lei nº 9.504, de 30 de setembro de 1997, resolve expedir a seguinte instrução:

Capítulo I

DO OBJETO

Art. 1º Fica instituído o Teste Público de Segurança (TPS) no ciclo de desenvolvimento dos sistemas de votação e apuração.

§ 1º O TPS de que trata esta resolução constitui parte integrante do processo eleitoral brasileiro e será realizado antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

§ 2º A presidência dos trabalhos relativos ao TPS será exercida pelo presidente do Tribunal Superior Eleitoral.

Art. 2º Os sistemas eleitorais que poderão 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 nº 9.504/1997, incluindo o *hardware* da urna e seus *softwares* embarcados.

Capítulo II

DO OBJETIVO

Art. 3º O Teste Público de Segurança tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral.

Parágrafo único. O Teste Público de Segurança contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Capítulo III

DAS DEFINIÇÕES

Art. 4º Para os fins desta resolução, considera-se:

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

II – Vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas não seja condição suficiente para alcançar um dos objetivos definidos no parágrafo único do art. 3º.

III – Fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis.

IV – Plano de testes: documento que será fornecido para identificação e descrição das ações a serem desempenhadas pelo(s) técnico(s) e/ou grupo(s) de técnicos quando da realização do teste.

V – Ambiente de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para que o(s) técnico(s) e/ou o(s) grupo(s) de técnicos possam preparar e realizar os testes.

Capítulo IV

DAS ATRIBUIÇÕES

Art. 5º As unidades do Tribunal Superior Eleitoral deverão atuar, observadas as respectivas atribuições, para a plena realização do teste instituído por esta resolução.

Art. 6º Atuarão no Teste Público de Segurança:

I – Comissão Organizadora;

II – Comissão Reguladora;

III – Comissão Avaliadora;

IV – Comissão de Comunicação Institucional.

Art. 7º A gerência geral da realização do TPS será feita por integrantes da Diretoria-Geral, designados por portaria do presidente do Tribunal.

Art. 8º A Comissão Organizadora terá as seguintes atribuições:

I – planejar e elaborar o projeto geral para a realização do evento;

II – organizar e prover a infraestrutura necessária para a realização de todas as fases do TPS;

III – convocar as demais áreas do Tribunal, observadas as respectivas atribuições administrativas, a fim de providenciar ações ou infraestrutura para a realização do evento;

IV – manter informadas a Presidência e a Diretoria-Geral sobre o andamento dos trabalhos.

Parágrafo único. A Comissão Organizadora será composta pelas áreas da Diretoria-Geral, administração, segurança, imprensa e comunicação social, infraestrutura de TI e do cerimonial.

Art. 9º A Comissão Reguladora terá as seguintes atribuições:

I – definir os procedimentos e a metodologia utilizados;

II – aprovar a(s) inscrição(ões) do(s) técnico(s) e/ou do(s) grupo(s) de técnicos que tenha(m) atendido às exigências constantes do edital;

III – supervisionar e documentar todas as fases do evento;

IV – aprovar os planos de testes elaborados pelo(s) técnico(s) e/ou grupo(s) de técnicos;

V – realizar outras atividades relacionadas à disciplina do TPS, visando ao fiel cumprimento do objetivo desta resolução, ressalvadas as atribuições das demais comissões e da Presidência do Tribunal Superior Eleitoral;

VI – elaborar, em conjunto com a Comissão Organizadora, a minuta do edital que disciplinará a convocação e as etapas do TPS.

Parágrafo único. Os componentes da Comissão de que trata o *caput* deste artigo serão indicados por portaria, entre os quais no mínimo um com conhecimentos jurídicos indicado pela Presidência do Tribunal, integrantes da Secretaria de Tecnologia da Informação e um integrante da Comissão de Comunicação Institucional, definida no art. 11 desta resolução.

Art. 10. A Comissão Avaliadora terá as seguintes atribuições:

I – validar a metodologia e os critérios de julgamento definidos pela Comissão Disciplinadora do Teste Público de Segurança;

II – avaliar e homologar os resultados obtidos e produzir relatório final conclusivo.

§ 1º A Comissão de que trata o *caput* deste artigo será nomeada pelo presidente do Tribunal, com a seguinte composição:

I – um representante indicado pelo ministro presidente;

II – membros da comunidade acadêmica ou científica de notório saber na área de segurança da informação;

III – um representante do Ministério Público Federal;

IV – um representante da Ordem dos Advogados do Brasil;

V – um representante do Congresso Nacional;

VI – um perito criminal federal da área de informática, do Departamento de Polícia Federal;

VII – um engenheiro elétrico/eletrônico ou de computação, com o devido registro profissional no Conselho Regional de Engenharia e Agronomia (Crea), indicado pelo Conselho Federal de Engenharia e Agronomia (Confea);

VIII – um representante da Sociedade Brasileira de Computação (SBC).

§ 2º A Comissão poderá se valer de integrantes do Tribunal para assessorá-los.

§ 3º O Tribunal disponibilizará serviços de secretariado, espaço e infraestrutura à Comissão.

§ 4º Para a indicação dos integrantes definidos nos incisos III a VIII do § 1º deste artigo as respectivas instituições serão oficiadas para indicarem os componentes mencionados.

Art. 11. A Comissão de Comunicação Institucional terá as seguintes atribuições:

I – elaborar o plano de comunicação sobre o evento;

II – receber as solicitações de informação do público externo e centralizar a publicação de informações e notícias sobre o TPS, observadas as orientações da Presidência e da Diretoria-Geral;

III – responsabilizar-se pela cobertura jornalística do evento e credenciamento dos veículos de comunicação.

Parágrafo único. A Comissão de Comunicação Institucional será composta pelas áreas da Diretoria-Geral, imprensa e comunicação social e tecnologia da informação.

Capítulo V

DA PARTICIPAÇÃO

Art. 12. Poderão participar, na condição de técnico(s) e/ou de grupo(s) de técnicos, cidadãos brasileiros maiores de 18 anos, individualmente ou em grupo, que preencham os requisitos definidos em edital.

§ 1º O edital de que trata o *caput* disciplinará a quantidade máxima de participantes e equipes, bem como os critérios para inscrição, seleção e avaliação.

§ 2º Em caso de inscrições em quantidade superior à definida no edital de que trata o § 1º deste artigo, haverá sorteio público, entre as inscrições aprovadas.

Art. 13. É vedada a participação, na condição de técnico(s) e/ou grupo(s) de técnicos, de componentes das comissões referidas no art. 6º desta resolução.

Art. 14. Para promover a participação no TPS, o(s) técnico(s) e/ou grupo(s) de técnicos que reside(m) fora do município de realização do evento poderá(ão) requerer passagens e diárias ao Tribunal Superior Eleitoral.

Parágrafo único. As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral, além daquelas estipuladas no respectivo edital.

Art. 15. Ao final da fase de realização do Teste Público de Segurança, cada técnico ou grupo de técnicos deverá apresentar relatório técnico das ações executadas e resultados alcançados, de acordo com as regras definidas em edital.

Art. 16. O(s) técnico(s) e/ou grupo(s) de técnicos, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, deverá(ão) apresentar a(s) respectiva(s) sugestão(ões) de melhoria.

§ 1º Em um prazo de até 6 (seis) meses após a realização do TPS, o(s) técnico(s) e/ou grupo(s) de técnicos poderá(ão) ser convocado(s) a executar novamente, em uma nova versão do sistema eleitoral com as devidas correções, os mesmos testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 2º A nova execução dos testes de que trata o parágrafo anterior não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas no sistema.

§ 3º Para o disposto no § 1º, as modificações realizadas serão apresentadas, observado o disposto no § 2º do artigo 18.

Capítulo VI

DAS FASES DO TESTE PÚBLICO DE SEGURANÇA

Art. 17. O Teste Público de Segurança será dividido nas fases de preparação, realização e avaliação.

Art. 18. Na fase de preparação, deverão ser realizadas as seguintes ações ou eventos:

I – audiência pública com o objetivo de esclarecer as regras do TPS definidas nesta resolução;

II – publicação do edital que deverá contemplar as regras específicas e datas para a realização de todas as demais fases e ações do evento;

III – palestra informativa sobre o sistema eletrônico de votação com o objetivo de subsidiar os eventuais participantes sobre o funcionamento do sistema eleitoral;

IV – apresentação, em ambiente controlado, dos códigos-fonte dos sistemas eleitorais que farão parte do TPS;

V – geração de versão a ser utilizada no TPS, observados os procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas;

VI – preparação e configuração dos sistemas adicionais que serão utilizados no teste e elaboração dos respectivos planos de teste;

VII – recebimento das inscrições e planos de teste dos técnicos que desejam participar do evento.

https://www.tse.jus.br/legislacao/codigo-eleitoral/normas-editadas-pelo-tse/resolucao-no-23-444-de-30-de-abril-de-2015-2013-brasilia-2013-df 3/5

§ 1º Poderão ser definidas outras ações ou eventos intermediários para atender objetivos complementares desta fase, desde que estejam definidos no edital da respectiva edição do TPS.

§ 2º A apresentação dos códigos-fonte, de que trata o inciso IV deste artigo, será feita em ambiente controlado, com acesso mediante termo de confidencialidade e regras específicas definidas em edital.

Art. 19. Na fase de realização, os técnicos com inscrições homologadas comparecerão no local determinado para a realização do Teste Público de Segurança para executar no ambiente de teste os planos de teste previamente definidos, conforme regras definidas no edital.

Art. 20. Na fase de avaliação, a Comissão Avaliadora definida no art. 10, de posse dos planos de testes e documentação de execução dos testes, deverá elaborar relatório de avaliação contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes identificadas durante o TPS.

§ 1º O Tribunal promoverá evento de encerramento para demonstrar os resultados alcançados, que deverá contar com a presença do(s) técnico(s) e/ou grupo(s) de técnicos e Comissão Avaliadora.

§ 2º A Secretaria de Gestão da Informação será responsável por editar publicação específica, em formato físico e eletrônico, contendo um compêndio da documentação produzida e conclusões da Comissão Avaliadora.

§ 3º A publicação, em formato eletrônico, de que trata o parágrafo anterior deverá ser disponibilizada no sítio do Tribunal Superior Eleitoral.

Capítulo VII

DAS DISPOSIÇÕES GERAIS

Art. 21. O edital que disciplinará cada edição do Teste Público de Segurança será publicado no *DJE*/TSE e divulgado no sítio eletrônico do Tribunal Superior Eleitoral.

Parágrafo único. Os partidos políticos, as coligações, a Ordem dos Advogados do Brasil, o Ministério Público, o Congresso Nacional, o Supremo Tribunal Federal, o Ministério da Transparência e Controladoria-Geral da União, o Departamento de Polícia Federal, a Sociedade Brasileira de Computação, o Conselho Federal de Engenharia e Agronomia serão formalmente convocados para, querendo, participar e acompanhar o TPS na forma regulamentada nesta resolução.

- Parágrafo único acrescido pelo art. 1º da Res.-TSE nº 23542/2017.

Art. 22. Será dada publicidade à composição das comissões descritas no art. 6º desta resolução no *DJE*/TSE e no sítio eletrônico do Tribunal Superior Eleitoral.

Art. 23. Os participantes do TPS que tiverem a inscrição aprovada deverão manter conduta ética nas declarações e ilações sobre as hipóteses e resultados encontrados.

Art. 24. Fica autorizada a contratação e/ou celebração de convênio com instituições renomadas para realizar a pré-avaliação da segurança dos sistemas eleitorais e assessorar a realização do TPS.

Art. 25. O Tribunal Superior Eleitoral promoverá a criação de uma unidade ou núcleo permanente para tratar sistematicamente as questões relativas à segurança do processo eleitoral informatizado e à realização do teste de que cuida esta norma.

Art. 26. Os casos omissos serão dirimidos pela Presidência do Tribunal Superior Eleitoral.

Art. 27. Esta resolução entra em vigor na data de sua publicação.

Brasília, 30 de abril de 2015.

Ministro DIAS TOFFOLI, presidente e relator – Ministro GILMAR MENDES – Ministro LUIZ FUX – Ministro JOÃO OTÁVIO DE NORONHA – Ministra MARIA THEREZA DE ASSIS MOURA – Ministro HENRIQUE NEVES DA SILVA – Ministro ADMAR GONZAGA

Publicada no *DJE* de 21.5.2015.

7.2 Anexo B – Lei n. 9.504/1997

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 9.504, DE 30 DE SETEMBRO DE 1997.

Mensagem de veto
(Vide Decreto nº 7.791, de 2012)
Vide Emenda Constitucional nº 97,de 2017

Estabelece normas para as eleições.

O VICE PRESIDENTE DA REPÚBLICA no exercício do cargo de **PRESIDENTE DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Disposições Gerais

Art. 1º As eleições para Presidente e Vice-Presidente da República, Governador e Vice-Governador de Estado e do Distrito Federal, Prefeito e Vice-Prefeito, Senador, Deputado Federal, Deputado Estadual, Deputado Distrital e Vereador dar-se-ão, em todo o País, no primeiro domingo de outubro do ano respectivo.

Parágrafo único. Serão realizadas simultaneamente as eleições:

I - para Presidente e Vice-Presidente da República, Governador e Vice-Governador de Estado e do Distrito Federal, Senador, Deputado Federal, Deputado Estadual e Deputado Distrital;

II - para Prefeito, Vice-Prefeito e Vereador.

Art. 2º Será considerado eleito o candidato a Presidente ou a Governador que obtiver a maioria absoluta de votos, não computados os em branco e os nulos.

§ 1º Se nenhum candidato alcançar maioria absoluta na primeira votação, far-se-á nova eleição no último domingo de outubro, concorrendo os dois candidatos mais votados, e considerando-se eleito o que obtiver a maioria dos votos válidos.

§ 2º Se, antes de realizado o segundo turno, ocorrer morte, desistência ou impedimento legal de candidato, convocar-se-á, dentre os remanescentes, o de maior votação.

§ 3º Se, na hipótese dos parágrafos anteriores, remanescer em segundo lugar mais de um candidato com a mesma votação, qualificar-se-á o mais idoso.

§ 4º A eleição do Presidente importará a do candidato a Vice-Presidente com ele registrado, o mesmo se aplicando à eleição de Governador.

Art. 3º Será considerado eleito Prefeito o candidato que obtiver a maioria dos votos, não computados os em branco e os nulos.

§ 1º A eleição do Prefeito importará a do candidato a Vice-Prefeito com ele registrado.

§ 2º Nos Municípios com mais de duzentos mil eleitores, aplicar-se-ão as regras estabelecidas nos §§ 1º a 3º do artigo anterior.

Art. 4º Poderá participar das eleições o partido que, até seis meses antes do pleito, tenha registrado seu estatuto no Tribunal Superior Eleitoral, conforme o disposto em lei, e tenha, até a data da convenção, órgão de direção constituído na circunscrição, de acordo com o respectivo estatuto (Redação dada pela Lei nº 13.488, de 2017)

Art. 5º Nas eleições proporcionais, contam-se como válidos apenas os votos dados a candidatos regularmente inscritos e às legendas partidárias.

Das Coligações

Art. 6º É facultado aos partidos políticos, dentro da mesma circunscrição, celebrar coligações para eleição majoritária. (Redação dada pela Lei nº 14.211, de 2021)

§ 1º A coligação terá denominação própria, que poderá ser a junção de todas as siglas dos partidos que a integram, sendo a ela atribuídas as prerrogativas e obrigações de partido político no que se refere ao processo eleitoral, e devendo funcionar como um só partido no relacionamento com a Justiça Eleitoral e no trato dos interesses interpartidários.

§ 1º-A. A denominação da coligação não poderá coincidir, incluir ou fazer referência a nome ou número de candidato, nem conter pedido de voto para partido político. (Incluído pela Lei nº 12.034, de 2009)

§ 2º Na propaganda para eleição majoritária, a coligação usará, obrigatoriamente, sob sua denominação, as legendas de todos os partidos que a integram; na propaganda para eleição proporcional, cada partido usará apenas sua legenda sob o nome da coligação.

§ 3º Na formação de coligações, devem ser observadas, ainda, as seguintes normas:

I - na chapa da coligação, podem inscrever-se candidatos filiados a qualquer partido político dela integrante;

II - o pedido de registro dos candidatos deve ser subscrito pelos presidentes dos partidos coligados, por seus delegados, pela maioria dos membros dos respectivos órgãos executivos de direção ou por representante da coligação, na forma do inciso III;

III - os partidos integrantes da coligação devem designar um representante, que terá atribuições equivalentes às de presidente de partido político, no trato dos interesses e na representação da coligação, no que se refere ao processo eleitoral;

IV - a coligação será representada perante a Justiça Eleitoral pela pessoa designada na forma do inciso III ou por delegados indicados pelos partidos que a compõem, podendo nomear até:

a) três delegados perante o Juízo Eleitoral;

b) quatro delegados perante o Tribunal Regional Eleitoral;

c) cinco delegados perante o Tribunal Superior Eleitoral.

§ 4º O partido político coligado somente possui legitimidade para atuar de forma isolada no processo eleitoral quando questionar a validade da própria coligação, durante o período compreendido entre a data da convenção e o termo final do prazo para a impugnação do registro de candidatos. (Incluído pela Lei nº 12.034, de 2009)

§ 5º A responsabilidade pelo pagamento de multas decorrentes de propaganda eleitoral é solidária entre os candidatos e os respectivos partidos, não alcançando outros partidos mesmo quando integrantes de uma mesma coligação. (Incluído pela Lei nº 12.891, de 2013)

Das Federações
(Incluído pela Lei nº 14.208, de 2021)

Art. 6º-A Aplicam-se à federação de partidos de que trata o art. 11-A da Lei nº 9.096, de 19 de setembro de 1995 (Lei dos Partidos Políticos), todas as normas que regem as atividades dos partidos políticos no que diz respeito às eleições, inclusive no que se refere à escolha e registro de candidatos para as eleições majoritárias e proporcionais, à arrecadação e aplicação de recursos em campanhas eleitorais, à propaganda eleitoral, à contagem de votos, à obtenção de cadeiras, à prestação de contas e à convocação de suplentes. (Incluído pela Lei nº 14.208, de 2021)

Parágrafo único. É vedada a formação de federação de partidos após o prazo de realização das convenções partidárias. (Incluído pela Lei nº 14.208, de 2021) (Vide ADI Nº 7021)

Das Convenções para a Escolha de Candidatos

Art. 7º As normas para a escolha e substituição dos candidatos e para a formação de coligações serão estabelecidas no estatuto do partido, observadas as disposições desta Lei.

§ 1º Em caso de omissão do estatuto, caberá ao órgão de direção nacional do partido estabelecer as normas a que se refere este artigo, publicando-as no Diário Oficial da União até cento e oitenta dias antes das eleições.

§ 2º Se a convenção partidária de nível inferior se opuser, na deliberação sobre coligações, às diretrizes legitimamente estabelecidas pelo órgão de direção nacional, nos termos do respectivo estatuto, poderá esse órgão anular a deliberação e os atos dela decorrentes. (Redação dada pela Lei nº 12.034, de 2009)

§ 3º As anulações de deliberações dos atos decorrentes de convenção partidária, na condição acima estabelecida, deverão ser comunicadas à Justiça Eleitoral no prazo de 30 (trinta) dias após a data limite para o registro de candidatos. (Redação dada pela Lei nº 12.034, de 2009)

§ 4º Se, da anulação, decorrer a necessidade de escolha de novos candidatos, o pedido de registro deverá ser apresentado à Justiça Eleitoral nos 10 (dez) dias seguintes à deliberação, observado o disposto no art. 13. (Incluído pela Lei nº 12.034, de 2009)

Art. 8º A escolha dos candidatos pelos partidos e a deliberação sobre coligações deverão ser feitas no período de 20 de julho a 5 de agosto do ano em que se realizarem as eleições, lavrando-se a respectiva ata em livro aberto, rubricado pela Justiça Eleitoral, publicada em vinte e quatro horas em qualquer meio de comunicação. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º Aos detentores de mandato de Deputado Federal, Estadual ou Distrital, ou de Vereador, e aos que tenham exercido esses cargos em qualquer período da legislatura que estiver em curso, é assegurado o registro de candidatura para o mesmo cargo pelo partido a que estejam filiados. (Vide ADIN - 2.530-9)

§ 2º Para a realização das convenções de escolha de candidatos, os partidos políticos poderão usar gratuitamente prédios públicos, responsabilizando-se por danos causados com a realização do evento.

Art. 9º Para concorrer às eleições, o candidato deverá possuir domicílio eleitoral na respectiva circunscrição pelo prazo de seis meses e estar com a filiação deferida pelo partido no mesmo prazo. (Redação dada pela Lei nº 13.488, de 2017)

Parágrafo único. Havendo fusão ou incorporação de partidos após o prazo estipulado no *caput*, será considerada, para efeito de filiação partidária, a data de filiação do candidato ao partido de origem.

Do Registro de Candidatos

Art. 10. Cada partido poderá registrar candidatos para a Câmara dos Deputados, a Câmara Legislativa, as Assembleias Legislativas e as Câmaras Municipais no total de até 100% (cem por cento) do número de lugares a preencher mais 1 (um). (Redação dada pela Lei nº 14.211, de 2021)

I - (Revogado); (Redação dada pela Lei nº 14.211, de 2021)

II - (Revogado). (Redação dada pela Lei nº 14.211, de 2021)

§ 1º (Revogado). (Redação dada pela Lei nº 13.165, de 2015)

§ 2º (Revogado). (Redação dada pela Lei nº 13.165, de 2015)

§ 3º Do número de vagas resultante das regras previstas neste artigo, cada partido ou coligação preencherá o mínimo de 30% (trinta por cento) e o máximo de 70% (setenta por cento) para candidaturas de cada sexo. (Redação dada pela Lei nº 12.034, de 2009)

§ 4º Em todos os cálculos, será sempre desprezada a fração, se inferior a meio, e igualada a um, se igual ou superior.

§ 5º No caso de as convenções para a escolha de candidatos não indicarem o número máximo de candidatos previsto no **caput**, os órgãos de direção dos partidos respectivos poderão preencher as vagas remanescentes até trinta dias antes do pleito. (Redação dada pela Lei nº 13.165, de 2015)

§ 6º (VETADO). (Incluído pela Lei nº 14.211, de 2021)

§ 7º (VETADO) (Incluído pela Lei nº 14.211, de 2021)

Art. 11. Os partidos e coligações solicitarão à Justiça Eleitoral o registro de seus candidatos até as dezenove horas do dia 15 de agosto do ano em que se realizarem as eleições. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º O pedido de registro deve ser instruído com os seguintes documentos:

I - cópia da ata a que se refere o art. 8º;

II - autorização do candidato, por escrito;

III - prova de filiação partidária;

IV - declaração de bens, assinada pelo candidato;

V - cópia do título eleitoral ou certidão, fornecida pelo cartório eleitoral, de que o candidato é eleitor na circunscrição ou requereu sua inscrição ou transferência de domicílio no prazo previsto no art. 9º;

VI - certidão de quitação eleitoral;

VII - certidões criminais fornecidas pelos órgãos de distribuição da Justiça Eleitoral, Federal e Estadual;

VIII - fotografia do candidato, nas dimensões estabelecidas em instrução da Justiça Eleitoral, para efeito do disposto no § 1º do art. 59.

IX - propostas defendidas pelo candidato a Prefeito, a Governador de Estado e a Presidente da República. (Incluído pela Lei nº 12.034, de 2009)

§ 2º A idade mínima constitucionalmente estabelecida como condição de elegibilidade é verificada tendo por referência a data da posse, salvo quando fixada em dezoito anos, hipótese em que será aferida na data-limite para o pedido de registro. (Redação dada pela Lei nº 13.165, de 2015)

§ 3º Caso entenda necessário, o Juiz abrirá prazo de setenta e duas horas para diligências.

§ 4º Na hipótese de o partido ou coligação não requerer o registro de seus candidatos, estes poderão fazê-lo perante a Justiça Eleitoral, observado o prazo máximo de quarenta e oito horas seguintes à publicação da lista dos candidatos pela Justiça Eleitoral. (Redação dada pela Lei nº 12.034, de 2009)

§ 5º Até a data a que se refere este artigo, os Tribunais e Conselhos de Contas deverão tornar disponíveis à Justiça Eleitoral relação dos que tiveram suas contas relativas ao exercício de cargos ou funções públicas rejeitadas por irregularidade insanável e por decisão irrecorrível do órgão competente, ressalvados os casos em que a questão estiver sendo submetida à apreciação do Poder Judiciário, ou que haja sentença judicial favorável ao interessado.

§ 6º A Justiça Eleitoral possibilitará aos interessados acesso aos documentos apresentados para os fins do disposto no § 1º. (Incluído pela Lei nº 12.034, de 2009)

§ 7º A certidão de quitação eleitoral abrangerá exclusivamente a plenitude do gozo dos direitos políticos, o regular exercício do voto, o atendimento a convocações da Justiça Eleitoral para auxiliar os trabalhos relativos ao pleito, a inexistência de multas aplicadas, em caráter definitivo, pela Justiça Eleitoral e não remitidas, e a apresentação de contas de campanha eleitoral. (Incluído pela Lei nº 12.034, de 2009)

§ 8º Para fins de expedição da certidão de que trata o § 7º, considerar-se-ão quites aqueles que: (Incluído pela Lei nº 12.034, de 2009)

I - condenados ao pagamento de multa, tenham, até a data da formalização do seu pedido de registro de candidatura, comprovado o pagamento ou o parcelamento da dívida regularmente cumprido; (Incluído pela Lei nº 12.034, de 2009)

II - pagarem a multa que lhes couber individualmente, excluindo-se qualquer modalidade de responsabilidade solidária, mesmo quando imposta concomitantemente com outros candidatos e em razão do mesmo fato. (Incluído pela Lei nº 12.034, de 2009)

III - o parcelamento das multas eleitorais é direito dos cidadãos e das pessoas jurídicas e pode ser feito em até sessenta meses, salvo quando o valor da parcela ultrapassar 5% (cinco por cento) da renda mensal, no caso de cidadão, ou 2% (dois por cento) do faturamento, no caso de pessoa jurídica, hipótese em que poderá estender-se por prazo superior, de modo que as parcelas não ultrapassem os referidos limites; (Redação dada pela Lei nº 13.488, de 2017)

IV - o parcelamento de multas eleitorais e de outras multas e débitos de natureza não eleitoral imputados pelo poder público é garantido também aos partidos políticos em até sessenta meses, salvo se o valor da parcela ultrapassar o limite de 2% (dois por cento) do repasse mensal do Fundo Partidário, hipótese em que poderá estender-se por prazo superior, de modo que as parcelas não ultrapassem o referido limite. (Incluído pela Lei nº 13.488, de 2017)

§ 9º A Justiça Eleitoral enviará aos partidos políticos, na respectiva circunscrição, até o dia 5 de junho do ano da eleição, a relação de todos os devedores de multa eleitoral, a qual embasará a expedição das certidões de quitação eleitoral. (Incluído pela Lei nº 12.034, de 2009)

§ 10. As condições de elegibilidade e as causas de inelegibilidade devem ser aferidas no momento da formalização do pedido de registro da candidatura, ressalvadas as alterações, fáticas ou jurídicas, supervenientes ao registro que afastem a inelegibilidade. (Incluído pela Lei nº 12.034, de 2009)

§ 11. A Justiça Eleitoral observará, no parcelamento a que se refere o § 8º deste artigo, as regras de parcelamento previstas na legislação tributária federal. (Incluído pela Lei nº 12.034, de 2009)

§ 12. (VETADO) (Incluído pela Lei nº 12.034, de 2009)

§ 13. Fica dispensada a apresentação pelo partido, coligação ou candidato de documentos produzidos a partir de informações detidas pela Justiça Eleitoral, entre eles os indicados nos incisos III, V e VI do § 1º deste artigo. (Incluído pela Lei nº 12.891, de 2013)

§ 14. É vedado o registro de candidatura avulsa, ainda que o requerente tenha filiação partidária. (Incluído pela Lei nº 13.488, de 2017)

§ 15. (VETADO). (Incluído pela Lei nº 13.877, de 2019)

Art. 12. O candidato às eleições proporcionais indicará, no pedido de registro, além de seu nome completo, as variações nominais com que deseja ser registrado, até o máximo de três opções, que poderão ser o prenome, sobrenome, cognome, nome abreviado, apelido ou nome pelo qual é mais conhecido, desde que não se estabeleça dúvida quanto à sua identidade, não atente contra o pudor e não seja ridículo ou irreverente, mencionando em que ordem de preferência deseja registrar-se.

§ 1º Verificada a ocorrência de homonímia, a Justiça Eleitoral procederá atendendo ao seguinte:

I - havendo dúvida, poderá exigir do candidato prova de que é conhecido por dada opção de nome, indicada no pedido de registro;

II - ao candidato que, na data máxima prevista para o registro, esteja exercendo mandato eletivo ou o tenha exercido nos últimos quatro anos, ou que nesse mesmo prazo se tenha candidatado com um dos nomes que indicou, será deferido o seu uso no registro, ficando outros candidatos impedidos de fazer propaganda com esse mesmo nome;

III - ao candidato que, pela sua vida política, social ou profissional, seja identificado por um dado nome que tenha indicado, será deferido o registro com esse nome, observado o disposto na parte final do inciso anterior;

IV - tratando-se de candidatos cuja homonímia não se resolva pelas regras dos dois incisos anteriores, a Justiça Eleitoral deverá notificá-los para que, em dois dias, cheguem a acordo sobre os respectivos nomes a serem usados;

V - não havendo acordo no caso do inciso anterior, a Justiça Eleitoral registrará cada candidato com o nome e sobrenome constantes do pedido de registro, observada a ordem de preferência ali definida.

§ 2º A Justiça Eleitoral poderá exigir do candidato prova de que é conhecido por determinada opção de nome por ele indicado, quando seu uso puder confundir o eleitor.

§ 3º A Justiça Eleitoral indeferirá todo pedido de variação de nome coincidente com nome de candidato a eleição majoritária, salvo para candidato que esteja exercendo mandato eletivo ou o tenha exercido nos últimos quatro anos, ou que, nesse mesmo prazo, tenha concorrido em eleição com o nome coincidente.

§ 4º Ao decidir sobre os pedidos de registro, a Justiça Eleitoral publicará as variações de nome deferidas aos candidatos.

§ 5º A Justiça Eleitoral organizará e publicará, até trinta dias antes da eleição, as seguintes relações, para uso na votação e apuração:

I - a primeira, ordenada por partidos, com a lista dos respectivos candidatos em ordem numérica, com as três variações de nome correspondentes a cada um, na ordem escolhida pelo candidato;

II - a segunda, com o índice onomástico e organizada em ordem alfabética, nela constando o nome completo de cada candidato e cada variação de nome, também em ordem alfabética, seguidos da respectiva legenda e número.

Art. 13. É facultado ao partido ou coligação substituir candidato que for considerado inelegível, renunciar ou falecer após o termo final do prazo do registro ou, ainda, tiver seu registro indeferido ou cancelado.

§ 1º A escolha do substituto far-se-á na forma estabelecida no estatuto do partido a que pertencer o substituído, e o registro deverá ser requerido até 10 (dez) dias contados do fato ou da notificação do partido da decisão judicial que deu origem à substituição. (Redação dada pela Lei nº 12.034, de 2009)

§ 2º Nas eleições majoritárias, se o candidato for de coligação, a substituição deverá fazer-se por decisão da maioria absoluta dos órgãos executivos de direção dos partidos coligados, podendo o substituto ser filiado a qualquer partido dela integrante, desde que o partido ao qual pertencia o substituído renuncie ao direito de preferência.

§ 3º Tanto nas eleições majoritárias como nas proporcionais, a substituição só se efetivará se o novo pedido for apresentado até 20 (vinte) dias antes do pleito, exceto em caso de falecimento de candidato, quando a substituição poderá ser efetivada após esse prazo. (Redação dada pela Lei nº 12.891, de 2013)

Art. 14. Estão sujeitos ao cancelamento do registro os candidatos que, até a data da eleição, forem expulsos do partido, em processo no qual seja assegurada ampla defesa e sejam observadas as normas estatutárias.

Parágrafo único. O cancelamento do registro do candidato será decretado pela Justiça Eleitoral, após solicitação do partido.

Art. 15. A identificação numérica dos candidatos se dará mediante a observação dos seguintes critérios:

I - os candidatos aos cargos majoritários concorrerão com o número identificador do partido ao qual estiverem filiados;

II - os candidatos à Câmara dos Deputados concorrerão com o número do partido ao qual estiverem filiados, acrescido de dois algarismos à direita;

III - os candidatos às Assembléias Legislativas e à Câmara Distrital concorrerão com o número do partido ao qual estiverem filiados acrescido de três algarismos à direita;

IV - o Tribunal Superior Eleitoral baixará resolução sobre a numeração dos candidatos concorrentes às eleições municipais.

§ lº Aos partidos fica assegurado o direito de manter os números atribuídos à sua legenda na eleição anterior, e aos candidatos, nesta hipótese, o direito de manter os números que lhes foram atribuídos na eleição anterior para o mesmo cargo.

§ 2º Aos candidatos a que se refere o § 1º do art. 8º, é permitido requerer novo número ao órgão de direção de seu partido, independentemente do sorteio a que se refere o § 2º do art. 100 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

§ 3º Os candidatos de coligações majoritárias serão registrados com o número de legenda do respectivo partido. (Redação dada pela Lei nº 14.211, de 2021)

Art. 16. Até vinte dias antes da data das eleições, os Tribunais Regionais Eleitorais enviarão ao Tribunal Superior Eleitoral, para fins de centralização e divulgação de dados, a relação dos candidatos às eleições majoritárias e proporcionais, da qual constará obrigatoriamente a referência ao sexo e ao cargo a que concorrem. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º Até a data prevista no **caput**, todos os pedidos de registro de candidatos, inclusive os impugnados e os respectivos recursos, devem estar julgados pelas instâncias ordinárias, e publicadas as decisões a eles relativas. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º Os processos de registro de candidaturas terão prioridade sobre quaisquer outros, devendo a Justiça Eleitoral adotar as providências necessárias para o cumprimento do prazo previsto no § 1º, inclusive com a realização de sessões extraordinárias e a convocação dos juízes suplentes pelos Tribunais, sem prejuízo da eventual aplicação do disposto no art. 97 e de representação ao Conselho Nacional de Justiça. (Incluído pela Lei nº 12.034, de 2009)

Art. 16-A. O candidato cujo registro esteja sub judice poderá efetuar todos os atos relativos à campanha eleitoral, inclusive utilizar o horário eleitoral gratuito no rádio e na televisão e ter seu nome mantido na urna eletrônica enquanto estiver sob essa condição, ficando a validade dos votos a ele atribuídos condicionada ao deferimento de seu registro por instância superior. (Incluído pela Lei nº 12.034, de 2009)

Parágrafo único. O cômputo, para o respectivo partido ou coligação, dos votos atribuídos ao candidato cujo registro esteja sub judice no dia da eleição fica condicionado ao deferimento do registro do candidato. (Incluído pela Lei nº 12.034, de 2009) (Vide ADI nº 4542) (Vide ADI nº 4513)

Art. 16-B. O disposto no art. 16-A quanto ao direito de participar da campanha eleitoral, inclusive utilizar o horário eleitoral gratuito, aplica-se igualmente ao candidato cujo pedido de registro tenha sido protocolado no prazo legal e ainda não tenha sido apreciado pela Justiça Eleitoral. (Incluído pela Lei nº 12.891, de 2013)

Do Fundo Especial de Financiamento de Campanha (FEFC)
(Incluído pela Lei nº 13.487, de 2017)

Art. 16-C. O Fundo Especial de Financiamento de Campanha (FEFC) é constituído por dotações orçamentárias da União em ano eleitoral, em valor ao menos equivalente: (Incluído pela Lei nº 13.487, de 2017)

I - ao definido pelo Tribunal Superior Eleitoral, a cada eleição, com base nos parâmetros definidos em lei; (Incluído pela Lei nº 13.487, de 2017)

II - ao percentual do montante total dos recursos da reserva específica a programações decorrentes de emendas de bancada estadual impositiva, que será encaminhado no projeto de lei orçamentária anual. (Redação dada pela Lei nº 13.877, de 2019)

§ 1º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 2º O Tesouro Nacional depositará os recursos no Banco do Brasil, em conta especial à disposição do Tribunal Superior Eleitoral, até o primeiro dia útil do mês de junho do ano do pleito. (Incluído pela Lei nº 13.487, de 2017)

§ 3º Nos quinze dias subsequentes ao depósito, o Tribunal Superior Eleitoral: (Incluído pela Lei nº 13.487, de 2017)

I - divulgará o montante de recursos disponíveis no Fundo Eleitoral; e (Incluído pela Lei nº 13.487, de 2017)

II - (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 4º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 5º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 6º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 7º Os recursos de que trata este artigo ficarão à disposição do partido político somente após a definição de critérios para a sua distribuição, os quais, aprovados pela maioria absoluta dos membros do órgão de direção executiva nacional do partido, serão divulgados publicamente. (Incluído pela Lei nº 13.487, de 2017)

§ 8º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 9º (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 10. (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 11. Os recursos provenientes do Fundo Especial de Financiamento de Campanha que não forem utilizados nas campanhas eleitorais deverão ser devolvidos ao Tesouro Nacional, integralmente, no momento da apresentação da respectiva prestação de contas. (Incluído pela Lei nº 13.487, de 2017)

§ 12. (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 13. (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 14. (VETADO). (Incluído pela Lei nº 13.487, de 2017)

§ 15. O percentual dos recursos a que se refere o inciso II do **caput** deste artigo poderá ser reduzido mediante compensação decorrente do remanejamento, se existirem, de dotações em excesso destinadas ao Poder Legislativo. (Incluído pela Lei nº 13.487, de 2017)

§ 16. Os partidos podem comunicar ao Tribunal Superior Eleitoral até o 1º (primeiro) dia útil do mês de junho a renúncia ao FEFC, vedada a redistribuição desses recursos aos demais partidos. (Incluído pela Lei nº 13.877, de 2019)

Art. 16-D. Os recursos do Fundo Especial de Financiamento de Campanha (FEFC), para o primeiro turno das eleições, serão distribuídos entre os partidos políticos, obedecidos os seguintes critérios: (Incluído pela Lei nº 13.488, de 2017)

I - 2% (dois por cento), divididos igualitariamente entre todos os partidos com estatutos registrados no Tribunal Superior Eleitoral; (Incluído pela Lei nº 13.488, de 2017)

II - 35% (trinta e cinco por cento), divididos entre os partidos que tenham pelo menos um representante na Câmara dos Deputados, na proporção do percentual de votos por eles obtidos na última eleição geral para a Câmara dos Deputados; (Incluído pela Lei nº 13.488, de 2017)

III - 48% (quarenta e oito por cento), divididos entre os partidos, na proporção do número de representantes na Câmara dos Deputados, consideradas as legendas dos titulares; (Incluído pela Lei nº 13.488, de 2017)

IV - 15% (quinze por cento), divididos entre os partidos, na proporção do número de representantes no Senado Federal, consideradas as legendas dos titulares. (Incluído pela Lei nº 13.488, de 2017)

§ 1º (VETADO). (Incluído pela Lei nº 13.488, de 2017)

§ 2º Para que o candidato tenha acesso aos recursos do Fundo a que se refere este artigo, deverá fazer requerimento por escrito ao órgão partidário respectivo. (Incluído pela Lei nº 13.488, de 2017)

§ 3º Para fins do disposto no inciso III do **caput** deste artigo, a distribuição dos recursos entre os partidos terá por base o número de representantes eleitos para a Câmara dos Deputados na última eleição geral, ressalvados os casos dos detentores de mandato que migraram em razão de o partido pelo qual foram eleitos não ter cumprido os requisitos previstos no § 3º do art. 17 da Constituição Federal. (Incluído pela Lei nº 13.877, de 2019)

§ 4º Para fins do disposto no inciso IV do **caput** deste artigo, a distribuição dos recursos entre os partidos terá por base o número de representantes eleitos para o Senado Federal na última eleição geral, bem como os Senadores filiados ao partido que, na data da última eleição geral, encontravam-se no 1º (primeiro) quadriênio de seus mandatos. (Incluído pela Lei nº 13.877, de 2019)

Da Arrecadação e da Aplicação de Recursos nas Campanhas Eleitorais

Art. 17. As despesas da campanha eleitoral serão realizadas sob a responsabilidade dos partidos, ou de seus candidatos, e financiadas na forma desta Lei.

Art. 17-A. (Revogado pela Lei nº 13.165, de 2015)

Art. 18. Os limites de gastos de campanha serão definidos em lei e divulgados pelo Tribunal Superior Eleitoral. (Redação dada pela Lei nº 13.488, de 2017)

§ 1º (Revogado). (Redação dada pela Lei nº 13.165, de 2015)

§ 2º (Revogado). (Redação dada pela Lei nº 13.165, de 2015)

Art. 18-A. Serão contabilizadas nos limites de gastos de cada campanha as despesas efetuadas pelos candidatos e as efetuadas pelos partidos que puderem ser individualizadas. (Incluído pela Lei nº 13.165, de 2015)

Parágrafo único. Para fins do disposto no **caput** deste artigo, os gastos advocatícios e de contabilidade referentes a consultoria, assessoria e honorários, relacionados à prestação de serviços em campanhas eleitorais e em favor destas, bem como em processo judicial decorrente de defesa de interesses de candidato ou partido político, não estão sujeitos a limites de gastos ou a limites que possam impor dificuldade ao exercício da ampla defesa. (Incluído pela Lei nº 13.877, de 2019)

Art. 18-B. O descumprimento dos limites de gastos fixados para cada campanha acarretará o pagamento de multa em valor equivalente a 100% (cem por cento) da quantia que ultrapassar o limite estabelecido, sem prejuízo da apuração da ocorrência de abuso do poder econômico. (Incluído pela Lei nº 13.165, de 2015)

Art. 18-C. O limite de gastos nas campanhas dos candidatos às eleições para prefeito e vereador, na respectiva circunscrição, será equivalente ao limite para os respectivos cargos nas eleições de 2016, atualizado pelo Índice Nacional de Preços ao Consumidor Amplo (IPCA), aferido pela Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), ou por índice que o substituir. (Incluído pela Lei nº 13.878, de 2019)

Parágrafo único. Nas campanhas para segundo turno das eleições para prefeito, onde houver, o limite de gastos de cada candidato será de 40% (quarenta por cento) do limite previsto no **caput** deste artigo. (Incluído pela Lei nº 13.878, de 2019)

Art. 19. (Revogado pela Lei nº 13.165, de 2015)

Art. 20. O candidato a cargo eletivo fará, diretamente ou por intermédio de pessoa por ele designada, a administração financeira de sua campanha usando recursos repassados pelo partido, inclusive os relativos à cota do Fundo Partidário, recursos próprios ou doações de pessoas físicas, na forma estabelecida nesta Lei. (Redação dada pela Lei nº 13.165, de 2015)

Art. 21. O candidato é solidariamente responsável com a pessoa indicada na forma do art. 20 desta Lei pela veracidade das informações financeiras e contábeis de sua campanha, devendo ambos assinar a respectiva prestação de contas. (Redação dada pela Lei nº 11.300, de 2006)

Art. 22. É obrigatório para o partido e para os candidatos abrir conta bancária específica para registrar todo o movimento financeiro da campanha.

§ 1º Os bancos são obrigados a: (Redação dada pela Lei nº 12.891, de 2013)

I - acatar, em até três dias, o pedido de abertura de conta de qualquer candidato escolhido em convenção, sendo-lhes vedado condicioná-la a depósito mínimo e à cobrança de taxas ou de outras despesas de manutenção; (Redação dada pela Lei nº 13.165, de 2015)

II - identificar, nos extratos bancários das contas correntes a que se refere o **caput**, o CPF ou o CNPJ do doador. (Incluído pela Lei nº 12.891, de 2013)

III - encerrar a conta bancária no final do ano da eleição, transferindo a totalidade do saldo existente para a conta bancária do órgão de direção indicado pelo partido, na forma prevista no art. 31, e informar o fato à Justiça Eleitoral. (Incluído pela Lei nº 13.165, de 2015)

§ 2º O disposto neste artigo não se aplica aos casos de candidatura para Prefeito e Vereador em Municípios onde não haja agência bancária ou posto de atendimento bancário. (Redação dada pela Lei nº 13.165, de 2015)

§ 3º O uso de recursos financeiros para pagamentos de gastos eleitorais que não provenham da conta específica de que trata o **caput** deste artigo implicará a desaprovação da prestação de contas do partido ou candidato; comprovado abuso de poder econômico, será cancelado o registro da candidatura ou cassado o diploma, se já houver sido outorgado. (Incluído pela Lei nº 11.300, de 2006)

§ 4º Rejeitadas as contas, a Justiça Eleitoral remeterá cópia de todo o processo ao Ministério Público Eleitoral para os fins previstos no art. 22 da Lei Complementar nº 64, de 18 de maio de 1990. (Incluído pela Lei nº 11.300, de 2006)

Art. 22-A. Os candidatos estão obrigados à inscrição no Cadastro Nacional da Pessoa Jurídica - CNPJ. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º Após o recebimento do pedido de registro da candidatura, a Justiça Eleitoral deverá fornecer em até 3 (três) dias úteis, o número de registro de CNPJ. (Incluído pela Lei nº 12.034, de 2009)

§ 2º Cumprido o disposto no § 1º deste artigo e no § 1º do art. 22, ficam os candidatos autorizados a promover a arrecadação de recursos financeiros e a realizar as despesas necessárias à campanha eleitoral. (Redação dada pela Lei nº 13.165, de 2015)

§ 3º Desde o dia 15 de maio do ano eleitoral, é facultada aos pré-candidatos a arrecadação prévia de recursos na modalidade prevista no inciso IV do § 4º do art. 23 desta Lei, mas a liberação de recursos por parte das entidades arrecadadoras fica condicionada ao registro da candidatura, e a realização de despesas de campanha deverá observar o calendário eleitoral. (Incluído pela Lei nº 13.488, de 2017)

§ 4º Na hipótese prevista no § 3º deste artigo, se não for efetivado o registro da candidatura, as entidades arrecadadoras deverão devolver os valores arrecadados aos doadores. (Incluído pela Lei nº 13.488, de 2017)

Art. 23. Pessoas físicas poderão fazer doações em dinheiro ou estimáveis em dinheiro para campanhas eleitorais, obedecido o disposto nesta Lei. (Redação dada pela Lei nº 12.034, de 2009) (Vide ADIN 5970)

§ 1º As doações e contribuições de que trata este artigo ficam limitadas a 10% (dez por cento) dos rendimentos brutos auferidos pelo doador no ano anterior à eleição. (Redação dada pela Lei nº 13.165, de 2015)

I - (revogado); (Redação dada pela Lei nº 13.165, de 2015)

II - (revogado). (Redação dada pela Lei nº 13.165, de 2015)

§ 1º-A (Revogado pela lei nº 13.488, de 2017)

§ 1º-B - (VETADO) (Incluído pela Lei nº 13.165, de 2015)

§ 2º As doações estimáveis em dinheiro a candidato específico, comitê ou partido deverão ser feitas mediante recibo, assinado pelo doador, exceto na hipótese prevista no § 6º do art. 28. (Redação dada pela Lei nº 12.891, de 2013)

§ 2º-A. O candidato poderá usar recursos próprios em sua campanha até o total de 10% (dez por cento) dos limites previstos para gastos de campanha no cargo em que concorrer. (Incluído pela Lei nº 13.878, de 2019)

§ 3º A doação de quantia acima dos limites fixados neste artigo sujeita o infrator ao pagamento de multa no valor de até 100% (cem por cento) da quantia em excesso. (Redação dada pela Lei nº 13.488, de 2017)

§ 4º As doações de recursos financeiros somente poderão ser efetuadas na conta mencionada no art. 22 desta Lei por meio de: (Redação dada pela Lei nº 11.300, de 2006) (Vide ADIN 5970)

I - cheques cruzados e nominais ou transferência eletrônica de depósitos; (Incluído pela Lei nº 11.300, de 2006)

II - depósitos em espécie devidamente identificados até o limite fixado no inciso I do § 1º deste artigo. (Incluído pela Lei nº 11.300, de 2006)

III - mecanismo disponível em sítio do candidato, partido ou coligação na internet, permitindo inclusive o uso de cartão de crédito, e que deverá atender aos seguintes requisitos: (Incluído pela Lei nº 12.034, de 2009)

a) identificação do doador; (Incluído pela Lei nº 12.034, de 2009)

b) emissão obrigatória de recibo eleitoral para cada doação realizada. (Incluído pela Lei nº 12.034, de 2009)

IV - instituições que promovam técnicas e serviços de financiamento coletivo por meio de sítios na internet, aplicativos eletrônicos e outros recursos similares, que deverão atender aos seguintes requisitos: (Incluído pela Lei nº 13.488, de 2017)

a) cadastro prévio na Justiça Eleitoral, que estabelecerá regulamentação para prestação de contas, fiscalização instantânea das doações, contas intermediárias, se houver, e repasses aos candidatos; (Incluído pela Lei nº 13.488, de 2017)

b) identificação obrigatória, com o nome completo e o número de inscrição no Cadastro de Pessoas Físicas (CPF) de cada um dos doadores e das quantias doadas; (Incluído pela Lei nº 13.488, de 2017)

c) disponibilização em sítio eletrônico de lista com identificação dos doadores e das respectivas quantias doadas, a ser atualizada instantaneamente a cada nova doação; (Incluído pela Lei nº 13.488, de 2017)

d) emissão obrigatória de recibo para o doador, relativo a cada doação realizada, sob a responsabilidade da entidade arrecadadora, com envio imediato para a Justiça Eleitoral e para o candidato de todas as informações relativas à doação; (Incluído pela Lei nº 13.488, de 2017)

e) ampla ciência a candidatos e eleitores acerca das taxas administrativas a serem cobradas pela realização do serviço; (Incluído pela Lei nº 13.488, de 2017)

f) não incidência em quaisquer das hipóteses listadas no art. 24 desta Lei; (Incluído pela Lei nº 13.488, de 2017)

g) observância do calendário eleitoral, especialmente no que diz respeito ao início do período de arrecadação financeira, nos termos dispostos no § 2º do art. 22-A desta Lei; (Incluído pela Lei nº 13.488, de 2017)

h) observância dos dispositivos desta Lei relacionados à propaganda na internet; (Incluído pela Lei nº 13.488, de 2017)

V - comercialização de bens e/ou serviços, ou promoção de eventos de arrecadação realizados diretamente pelo candidato ou pelo partido político. (Incluído pela Lei nº 13.488, de 2017) (Vide ADIN 5970)

§ 4º-A Na prestação de contas das doações mencionadas no § 4º deste artigo, é dispensada a apresentação de recibo eleitoral, e sua comprovação deverá ser realizada por meio de documento bancário que identifique o CPF dos doadores. (Incluído pela Lei nº 13.488, de 2017)

§ 4º-B As doações realizadas por meio das modalidades previstas nos incisos III e IV do § 4º deste artigo devem ser informadas à Justiça Eleitoral pelos candidatos e partidos no prazo previsto no inciso I do § 4º do art. 28 desta Lei, contado a partir do momento em que os recursos arrecadados forem depositados nas contas bancárias dos candidatos, partidos ou coligações. (Incluído pela Lei nº 13.488, de 2017)

§ 5º Ficam vedadas quaisquer doações em dinheiro, bem como de troféus, prêmios, ajudas de qualquer espécie feitas por candidato, entre o registro e a eleição, a pessoas físicas ou jurídicas. (Incluído pela Lei nº 11.300, de 2006)

§ 6º Na hipótese de doações realizadas por meio das modalidades previstas nos incisos III e IV do § 4º deste artigo, fraudes ou erros cometidos pelo doador sem conhecimento dos candidatos, partidos ou coligações não ensejarão a responsabilidade destes nem a rejeição de suas contas eleitorais. (Redação dada pela Lei nº 13.488, de 2017)

§ 7º O limite previsto no § 1º deste artigo não se aplica a doações estimáveis em dinheiro relativas à utilização de bens móveis ou imóveis de propriedade do doador ou à prestação de serviços próprios, desde que o valor estimado não ultrapasse R$ 40.000,00 (quarenta mil reais) por doador. (Redação dada pela Lei nº 13.488, de 2017)

§ 8º Ficam autorizadas a participar das transações relativas às modalidades de doações previstas nos incisos III e IV do § 4º deste artigo todas as instituições que atendam, nos termos da lei e da regulamentação expedida pelo Banco Central, aos critérios para operar arranjos de pagamento. (Incluído pela Lei nº 13.488, de 2017)

§ 9º As instituições financeiras e de pagamento não poderão recusar a utilização de cartões de débito e de crédito como meio de doações eleitorais de pessoas físicas. (Incluído pela Lei nº 13.488, de 2017)

§ 10. O pagamento efetuado por pessoas físicas, candidatos ou partidos em decorrência de honorários de serviços advocatícios e de contabilidade, relacionados à prestação de serviços em campanhas eleitorais e em favor destas, bem como em processo judicial decorrente de defesa de interesses de candidato ou partido político, não será considerado para a aferição do limite previsto no § 1º deste artigo e não constitui doação de bens e serviços estimáveis em dinheiro. (Incluído pela Lei nº 13.877, de 2019)

Art. 24. É vedado, a partido e candidato, receber direta ou indiretamente doação em dinheiro ou estimável em dinheiro, inclusive por meio de publicidade de qualquer espécie, procedente de: (Vide ADPF Nº 548)

I - entidade ou governo estrangeiro;

II - órgão da administração pública direta e indireta ou fundação mantida com recursos provenientes do Poder Público;

III - concessionário ou permissionário de serviço público;

IV - entidade de direito privado que receba, na condição de beneficiária, contribuição compulsória em virtude de disposição legal;

V - entidade de utilidade pública;

VI - entidade de classe ou sindical;

VII - pessoa jurídica sem fins lucrativos que receba recursos do exterior.

VIII - entidades beneficentes e religiosas; (Incluído pela Lei nº 11.300, de 2006)

IX - entidades esportivas; (Redação dada pela Lei nº 12.034, de 2009)

X - organizações não-governamentais que recebam recursos públicos; (Incluído pela Lei nº 11.300, de 2006)

XI - organizações da sociedade civil de interesse público. (Incluído pela Lei nº 11.300, de 2006)

XII - (VETADO). (Incluído pela Lei nº 13.165, de 2015)

§ 1º Não se incluem nas vedações de que trata este artigo as cooperativas cujos cooperados não sejam concessionários ou permissionários de serviços públicos, desde que não estejam sendo beneficiadas com recursos públicos, observado o disposto no art. 81. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º (VETADO). (Incluído pela Lei nº 13.165, de 2015)

§ 3º (VETADO). (Incluído pela Lei nº 13.165, de 2015)

§ 4º O partido ou candidato que receber recursos provenientes de fontes vedadas ou de origem não identificada deverá proceder à devolução dos valores recebidos ou, não sendo possível a identificação da fonte, transferi-los para a conta única do Tesouro Nacional. (Incluído pela Lei nº 13.165, de 2015)

Art. 24-A. (VETADO). (Incluído pela Lei nº 13.165, de 2015)

Art. 24-B. (VETADO). (Incluído pela Lei nº 13.165, de 2015)

Art. 24-C. O limite de doação previsto no § 1º do art. 23 será apurado anualmente pelo Tribunal Superior Eleitoral e pela Secretaria da Receita Federal do Brasil. (Incluído pela Lei nº 13.165, de 2015)

§ 1º O Tribunal Superior Eleitoral deverá consolidar as informações sobre as doações registradas até 31 de dezembro do exercício financeiro a ser apurado, considerando: (Incluído pela Lei nº 13.165, de 2015)

I - as prestações de contas anuais dos partidos políticos, entregues à Justiça Eleitoral até 30 de abril do ano subsequente ao da apuração, nos termos do art. 32 da Lei nº 9.096, de 19 de setembro de 1995; (Incluído pela Lei nº 13.165, de 2015)

II - as prestações de contas dos candidatos às eleições ordinárias ou suplementares que tenham ocorrido no exercício financeiro a ser apurado. (Incluído pela Lei nº 13.165, de 2015)

§ 2º O Tribunal Superior Eleitoral, após a consolidação das informações sobre os valores doados e apurados, encaminhá-las-á à Secretaria da Receita Federal do Brasil até 30 de maio do ano seguinte ao da apuração. (Incluído pela Lei nº 13.165, de 2015)

§ 3º A Secretaria da Receita Federal do Brasil fará o cruzamento dos valores doados com os rendimentos da pessoa física e, apurando indício de excesso, comunicará o fato, até 30 de julho do ano seguinte ao da apuração, ao Ministério Público Eleitoral, que poderá, até o final do exercício financeiro, apresentar representação com vistas à aplicação da penalidade prevista no art. 23 e de outras sanções que julgar cabíveis. (Incluído pela Lei nº 13.165, de 2015)

Art 25. O partido que descumprir as normas referentes à arrecadação e aplicação de recursos fixadas nesta Lei perderá o direito ao recebimento da quota do Fundo Partidário do ano seguinte, sem prejuízo de responderem os candidatos beneficiados por abuso do poder econômico.

Parágrafo único. A sanção de suspensão do repasse de novas quotas do Fundo Partidário, por desaprovação total ou parcial da prestação de contas do candidato, deverá ser aplicada de forma proporcional e razoável, pelo período de 1 (um) mês a 12 (doze) meses, ou por meio do desconto, do valor a ser repassado, na

importância apontada como irregular, não podendo ser aplicada a sanção de suspensão, caso a prestação de contas não seja julgada, pelo juízo ou tribunal competente, após 5 (cinco) anos de sua apresentação. (Incluído pela Lei nº 12.034, de 2009)

Art. 26. São considerados gastos eleitorais, sujeitos a registro e aos limites fixados nesta Lei: (Redação dada pela Lei nº 11.300, de 2006)

I - confecção de material impresso de qualquer natureza e tamanho, observado o disposto no § 3º do art. 38 desta Lei; (Redação dada pela Lei nº 12.891, de 2013)

II - propaganda e publicidade direta ou indireta, por qualquer meio de divulgação, destinada a conquistar votos;

III - aluguel de locais para a promoção de atos de campanha eleitoral;

IV - despesas com transporte ou deslocamento de candidato e de pessoal a serviço das candidaturas, observadas as exceções previstas no § 3º deste artigo. (Redação dada pela Lei nº 13.488, de 2017)

V - correspondência e despesas postais;

VI - despesas de instalação, organização e funcionamento de Comitês e serviços necessários às eleições;

VII - remuneração ou gratificação de qualquer espécie a pessoal que preste serviços às candidaturas ou aos comitês eleitorais;

VIII - montagem e operação de carros de som, de propaganda e assemelhados;

IX - a realização de comícios ou eventos destinados à promoção de candidatura; (Redação dada pela Lei nº 11.300, de 2006)

X - produção de programas de rádio, televisão ou vídeo, inclusive os destinados à propaganda gratuita;

XI - (Revogado); (Redação dada pela Lei nº 11.300, de 2006)

XII - realização de pesquisas ou testes pré-eleitorais;

XIII - (Revogado); (Redação dada pela Lei nº 11.300, de 2006)

XIV - (revogado); (Redação dada pela Lei nº 12.891, de 2013)

XV - custos com a criação e inclusão de sítios na internet e com o impulsionamento de conteúdos contratados diretamente com provedor da aplicação de internet com sede e foro no País; (Redação dada pela Lei nº 13.488, de 2017)

§ 1º São estabelecidos os seguintes limites com relação ao total do gasto da campanha: (Redação dada pela Lei nº 13.488, de 2017)

I - alimentação do pessoal que presta serviços às candidaturas ou aos comitês eleitorais: 10% (dez por cento); (Incluído pela Lei nº 12.891, de 2013)

II - aluguel de veículos automotores: 20% (vinte por cento). (Incluído pela Lei nº 12.891, de 2013)

§ 2º Para os fins desta Lei, inclui-se entre as formas de impulsionamento de conteúdo a priorização paga de conteúdos resultantes de aplicações de busca na internet. (Incluído dada pela Lei nº 13.488, de 2017)

§ 3º Não são consideradas gastos eleitorais nem se sujeitam a prestação de contas as seguintes despesas de natureza pessoal do candidato: (Incluído dada pela Lei nº 13.488, de 2017)

a) combustível e manutenção de veículo automotor usado pelo candidato na campanha; (Incluído dada pela Lei nº 13.488, de 2017)

b) remuneração, alimentação e hospedagem do condutor do veículo a que se refere a alínea *a* deste parágrafo; (Incluído dada pela Lei nº 13.488, de 2017)

c) alimentação e hospedagem própria; (Incluído dada pela Lei nº 13.488, de 2017)

d) uso de linhas telefônicas registradas em seu nome como pessoa física, até o limite de três linhas (Incluído dada pela Lei nº 13.488, de 2017)

§ 4º As despesas com consultoria, assessoria e pagamento de honorários realizadas em decorrência da prestação de serviços advocatícios e de contabilidade no curso das campanhas eleitorais serão consideradas gastos eleitorais, mas serão excluídas do limite de gastos de campanha. (Incluído pela Lei nº 13.877, de 2019)

§ 5º Para fins de pagamento das despesas de que trata este artigo, inclusive as do § 4º deste artigo, poderão ser utilizados recursos da campanha, do candidato, do fundo partidário ou do FEFC. (Incluído pela Lei nº 13.877, de 2019)

§ 6º Os recursos originados do fundo de que trata o art. 16-C desta Lei utilizados para pagamento das despesas previstas no § 4º deste artigo serão informados em anexo à prestação de contas dos candidatos. (Incluído pela Lei nº 13.877, de 2019)

Art. 27. Qualquer eleitor poderá realizar gastos, em apoio a candidato de sua preferência, até a quantia equivalente a um mil UFIR, não sujeitos a contabilização, desde que não reembolsados.

§ 1º Fica excluído do limite previsto no **caput** deste artigo o pagamento de honorários decorrentes da prestação de serviços advocatícios e de contabilidade, relacionados às campanhas eleitorais e em favor destas. (Incluído pela Lei nº 13.877, de 2019)

§ 2º Para fins do previsto no § 1º deste artigo, o pagamento efetuado por terceiro não compreende doação eleitoral. (Incluído pela Lei nº 13.877, de 2019)

Da Prestação de Contas

Art. 28. A prestação de contas será feita:

I - no caso dos candidatos às eleições majoritárias, na forma disciplinada pela Justiça Eleitoral;

II - no caso dos candidatos às eleições proporcionais, de acordo com os modelos constantes do Anexo desta Lei.

§ 1º As prestações de contas dos candidatos às eleições majoritárias serão feitas pelo próprio candidato, devendo ser acompanhadas dos extratos das contas bancárias referentes à movimentação dos recursos financeiros usados na campanha e da relação dos cheques recebidos, com a indicação dos respectivos números, valores e emitentes. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º As prestações de contas dos candidatos às eleições proporcionais serão feitas pelo próprio candidato. (Redação dada pela Lei nº 13.165, de 2015)

§ 3º As contribuições, doações e as receitas de que trata esta Lei serão convertidas em UFIR, pelo valor desta no mês em que ocorrerem.

§ 4º Os partidos políticos, as coligações e os candidatos são obrigados, durante as campanhas eleitorais, a divulgar em sítio criado pela Justiça Eleitoral para esse fim na rede mundial de computadores (internet): (Redação dada pela Lei nº 13.165, de 2015)

I - os recursos em dinheiro recebidos para financiamento de sua campanha eleitoral, em até 72 (setenta e duas) horas de seu recebimento; (Incluído pela Lei nº 13.165, de 2015)

II - no dia 15 de setembro, relatório discriminando as transferências do Fundo Partidário, os recursos em dinheiro e os estimáveis em dinheiro recebidos, bem como os gastos realizados. (Incluído pela Lei nº 13.165, de 2015)

§ 5º (VETADO). (Incluído pela Lei nº 12.891, de 2013)

§ 6º Ficam também dispensadas de comprovação na prestação de contas: (Incluído pela Lei nº 12.891, de 2013)

I - a cessão de bens móveis, limitada ao valor de R$ 4.000,00 (quatro mil reais) por pessoa cedente; (Incluído pela Lei nº 12.891, de 2013)

II - doações estimáveis em dinheiro entre candidatos ou partidos, decorrentes do uso comum tanto de sedes quanto de materiais de propaganda eleitoral, cujo gasto deverá ser registrado na prestação de contas do responsável pelo pagamento da despesa. (Redação dada pela Lei nº 13.165, de 2015)

III - a cessão de automóvel de propriedade do candidato, do cônjuge e de seus parentes até o terceiro grau para seu uso pessoal durante a campanha. (Incluído dada pela Lei nº 13.488, de 2017)

§ 7º As informações sobre os recursos recebidos a que se refere o § 4º deverão ser divulgadas com a indicação dos nomes, do CPF ou CNPJ dos doadores e dos respectivos valores doados. (Incluído pela Lei nº 13.165, de 2015)

§ 8º Os gastos com passagens aéreas efetuados nas campanhas eleitorais serão comprovados mediante a apresentação de fatura ou duplicata emitida por agência de viagem, quando for o caso, desde que informados os beneficiários, as datas e os itinerários, vedada a exigência de apresentação de qualquer outro documento para esse fim. (Incluído pela Lei nº 13.165, de 2015)

§ 9º A Justiça Eleitoral adotará sistema simplificado de prestação de contas para candidatos que apresentarem movimentação financeira correspondente a, no máximo, R$ 20.000,00 (vinte mil reais), atualizados monetariamente, a cada eleição, pelo Índice Nacional de Preços ao Consumidor - INPC da Fundação Instituto Brasileiro de Geografia e Estatística - IBGE ou por índice que o substituir. (Incluído pela Lei nº 13.165, de 2015)

§ 10. O sistema simplificado referido no § 9º deverá conter, pelo menos: (Incluído pela Lei nº 13.165, de 2015)

I - identificação das doações recebidas, com os nomes, o CPF ou CNPJ dos doadores e os respectivos valores recebidos; (Incluído pela Lei nº 13.165, de 2015)

II - identificação das despesas realizadas, com os nomes e o CPF ou CNPJ dos fornecedores de material e dos prestadores dos serviços realizados; (Incluído pela Lei nº 13.165, de 2015)

III - registro das eventuais sobras ou dívidas de campanha. (Incluído pela Lei nº 13.165, de 2015)

§ 11. Nas eleições para Prefeito e Vereador de Municípios com menos de cinquenta mil eleitores, a prestação de contas será feita sempre pelo sistema simplificado a que se referem os §§ 9º e 10. (Incluído pela Lei nº 13.165, de 2015)

§ 12. Os valores transferidos pelos partidos políticos oriundos de doações serão registrados na prestação de contas dos candidatos como transferência dos partidos e, na prestação de contas anual dos partidos, como transferência aos candidatos. (Redação dada pela Lei nº 13.877, de 2019)

Art. 29. Ao receber as prestações de contas e demais informações dos candidatos às eleições majoritárias e dos candidatos às eleições proporcionais que optarem por prestar contas por seu intermédio, os comitês deverão:

I - (revogado); (Redação dada pela Lei nº 13.165, de 2015)

II - resumir as informações contidas na prestação de contas, de forma a apresentar demonstrativo consolidado das campanhas; (Redação dada pela Lei nº 13.165, de 2015)

III - encaminhar à Justiça Eleitoral, até o trigésimo dia posterior à realização das eleições, o conjunto das prestações de contas dos candidatos e do próprio comitê, na forma do artigo anterior, ressalvada a hipótese do inciso seguinte;

IV - havendo segundo turno, encaminhar a prestação de contas, referente aos 2 (dois) turnos, até o vigésimo dia posterior à sua realização. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º (Revogado). (Redação dada pela Lei nº 13.165, de 2015)

§ 2º A inobservância do prazo para encaminhamento das prestações de contas impede a diplomação dos eleitos, enquanto perdurar.

§ 3º Eventuais débitos de campanha não quitados até a data de apresentação da prestação de contas poderão ser assumidos pelo partido político, por decisão do seu órgão nacional de direção partidária. (Incluído pela Lei nº 12.034, de 2009)

§ 4º No caso do disposto no § 3º, o órgão partidário da respectiva circunscrição eleitoral passará a responder por todas as dívidas solidariamente com o candidato, hipótese em que a existência do débito não poderá ser considerada como causa para a rejeição das contas. (Incluído pela Lei nº 12.034, de 2009)

Art. 30. A Justiça Eleitoral verificará a regularidade das contas de campanha, decidindo: (Redação dada pela Lei nº 12.034, de 2009)

I - pela aprovação, quando estiverem regulares; (Incluído pela Lei nº 12.034, de 2009)

II - pela aprovação com ressalvas, quando verificadas falhas que não lhes comprometam a regularidade; (Incluído pela Lei nº 12.034, de 2009)

III - pela desaprovação, quando verificadas falhas que lhes comprometam a regularidade; (Incluído pela Lei nº 12.034, de 2009)

IV - pela não prestação, quando não apresentadas as contas após a notificação emitida pela Justiça Eleitoral, na qual constará a obrigação expressa de prestar as suas contas, no prazo de setenta e duas horas. (Incluído pela Lei nº 12.034, de 2009)

§ 1º A decisão que julgar as contas dos candidatos eleitos será publicada em sessão até três dias antes da diplomação. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º Erros formais e materiais corrigidos não autorizam a rejeição das contas e a cominação de sanção a candidato ou partido.

§ 2º-A. Erros formais ou materiais irrelevantes no conjunto da prestação de contas, que não comprometam o seu resultado, não acarretarão a rejeição das contas. (Incluído pela Lei nº 12.034, de 2009)

§ 3º Para efetuar os exames de que trata este artigo, a Justiça Eleitoral poderá requisitar técnicos do Tribunal de Contas da União, dos Estados, do Distrito Federal ou dos Municípios, pelo tempo que for necessário.

§ 4º Havendo indício de irregularidade na prestação de contas, a Justiça Eleitoral poderá requisitar do candidato as informações adicionais necessárias, bem como determinar diligências para a complementação dos dados ou o saneamento das falhas. (Redação dada pela Lei nº 13.165, de 2015)

§ 5º Da decisão que julgar as contas prestadas pelos candidatos caberá recurso ao órgão superior da Justiça Eleitoral, no prazo de 3 (três) dias, a contar da publicação no Diário Oficial. (Redação dada pela Lei nº 13.165, de 2015)

§ 6º No mesmo prazo previsto no § 5º, caberá recurso especial para o Tribunal Superior Eleitoral, nas hipóteses previstas nos incisos I e II do § 4º do art. 121 da Constituição Federal. (Incluído pela Lei nº 12.034, de 2009)

§ 7º O disposto neste artigo aplica-se aos processos judiciais pendentes. (Incluído pela Lei nº 12.034, de 2009)

Art. 30-A. Qualquer partido político ou coligação poderá representar à Justiça Eleitoral, no prazo de 15 (quinze) dias da diplomação, relatando fatos e indicando provas, e pedir a abertura de investigação judicial para apurar condutas em desacordo com as normas desta Lei, relativas à arrecadação e gastos de recursos. (Redação dada pela Lei nº 12.034, de 2009) (Vide Emenda Constitucional nº 107, de 2020)

§ 1º Na apuração de que trata este artigo, aplicar-se-á o procedimento previsto no art. 22 da Lei Complementar nº 64, de 18 de maio de 1990, no que couber. (Incluído pela Lei nº 11.300, de 2006)

§ 2º Comprovados captação ou gastos ilícitos de recursos, para fins eleitorais, será negado diploma ao candidato, ou cassado, se já houver sido outorgado. (Incluído pela Lei nº 11.300, de 2006)

§ 3º O prazo de recurso contra decisões proferidas em representações propostas com base neste artigo será de 3 (três) dias, a contar da data da publicação do julgamento no Diário Oficial. (Incluído pela Lei nº 12.034, de 2009)

Art. 31. Se, ao final da campanha, ocorrer sobra de recursos financeiros, esta deve ser declarada na prestação de contas e, após julgados todos os recursos, transferida ao partido, obedecendo aos seguintes critérios: (Redação dada pela Lei nº 12.891, de 2013)

I - no caso de candidato a Prefeito, Vice-Prefeito e Vereador, esses recursos deverão ser transferidos para o órgão diretivo municipal do partido na cidade onde ocorreu a eleição, o qual será responsável exclusivo pela identificação desses recursos, sua utilização, contabilização e respectiva prestação de contas perante o juízo eleitoral correspondente; (Incluído pela Lei nº 12.891, de 2013)

II - no caso de candidato a Governador, Vice-Governador, Senador, Deputado Federal e Deputado Estadual ou Distrital, esses recursos deverão ser transferidos para o órgão diretivo regional do partido no Estado onde ocorreu a eleição ou no Distrito Federal, se for o caso, o qual será responsável exclusivo pela identificação desses recursos, sua utilização, contabilização e respectiva prestação de contas perante o Tribunal Regional Eleitoral correspondente; (Incluído pela Lei nº 12.891, de 2013)

III - no caso de candidato a Presidente e Vice-Presidente da República, esses recursos deverão ser transferidos para o órgão diretivo nacional do partido, o qual será responsável exclusivo pela identificação desses recursos, sua utilização, contabilização e respectiva prestação de contas perante o Tribunal Superior Eleitoral; (Incluído pela Lei nº 12.891, de 2013)

IV - o órgão diretivo nacional do partido não poderá ser responsabilizado nem penalizado pelo descumprimento do disposto neste artigo por parte dos órgãos diretivos municipais e regionais. (Incluído pela Lei nº 12.891, de 2013)

Parágrafo único. As sobras de recursos financeiros de campanha serão utilizadas pelos partidos políticos, devendo tais valores ser declarados em suas prestações de contas perante a Justiça Eleitoral, com a identificação dos candidatos. (Redação dada pela Lei nº 12.034, de 2009)

Art. 32. Até cento e oitenta dias após a diplomação, os candidatos ou partidos conservarão a documentação concernente a suas contas.

Parágrafo único. Estando pendente de julgamento qualquer processo judicial relativo às contas, a documentação a elas concernente deverá ser conservada até a decisão final.

Das Pesquisas e Testes Pré-Eleitorais

Art. 33. As entidades e empresas que realizarem pesquisas de opinião pública relativas às eleições ou aos candidatos, para conhecimento público, são obrigadas, para cada pesquisa, a registrar, junto à Justiça Eleitoral, até cinco dias antes da divulgação, as seguintes informações:

I - quem contratou a pesquisa;

II - valor e origem dos recursos despendidos no trabalho;

III - metodologia e período de realização da pesquisa;

IV - plano amostral e ponderação quanto a sexo, idade, grau de instrução, nível econômico e área física de realização do trabalho a ser executado, intervalo de confiança e margem de erro; (Redação dada pela Lei nº 12.891, de 2013)

V - sistema interno de controle e verificação, conferência e fiscalização da coleta de dados e do trabalho de campo;

VI - questionário completo aplicado ou a ser aplicado;

VII - nome de quem pagou pela realização do trabalho e cópia da respectiva nota fiscal. (Redação dada pela Lei nº 12.891, de 2013)

§ 1º As informações relativas às pesquisas serão registradas nos órgãos da Justiça Eleitoral aos quais compete fazer o registro dos candidatos.

§ 2º A Justiça Eleitoral afixará no prazo de vinte e quatro horas, no local de costume, bem como divulgará em seu sítio na internet, aviso comunicando o registro das informações a que se refere este artigo, colocando-as à disposição dos partidos ou coligações com candidatos ao pleito, os quais a elas terão livre acesso pelo prazo de 30 (trinta) dias. (Redação dada pela Lei nº 12.034, de 2009)

§ 3º A divulgação de pesquisa sem o prévio registro das informações de que trata este artigo sujeita os responsáveis a multa no valor de cinqüenta mil a cem mil UFIR.

§ 4º A divulgação de pesquisa fraudulenta constitui crime, punível com detenção de seis meses a um ano e multa no valor de cinqüenta mil a cem mil UFIR.

§ 5º É vedada, no período de campanha eleitoral, a realização de enquetes relacionadas ao processo eleitoral. (Incluído pela Lei nº 12.891, de 2013)

Art. 34. (VETADO)

§ 1º Mediante requerimento à Justiça Eleitoral, os partidos poderão ter acesso ao sistema interno de controle, verificação e fiscalização da coleta de dados das entidades que divulgaram pesquisas de opinião relativas às eleições, incluídos os referentes à identificação dos entrevistadores e, por meio de escolha livre e aleatória de planilhas individuais, mapas ou equivalentes, confrontar e conferir os dados publicados, preservada a identidade dos respondentes.

§ 2º O não-cumprimento do disposto neste artigo ou qualquer ato que vise a retardar, impedir ou dificultar a ação fiscalizadora dos partidos constitui crime, punível com detenção, de seis meses a um ano, com a alternativa de prestação de serviços à comunidade pelo mesmo prazo, e multa no valor de dez mil a vinte mil UFIR.

§ 3º A comprovação de irregularidade nos dados publicados sujeita os responsáveis às penas mencionadas no parágrafo anterior, sem prejuízo da obrigatoriedade da veiculação dos dados corretos no mesmo espaço, local, horário, página, caracteres e outros elementos de destaque, de acordo com o veículo usado.

Art. 35. Pelos crimes definidos nos arts. 33, § 4º e 34, §§ 2º e 3º, podem ser responsabilizados penalmente os representantes legais da empresa ou entidade de pesquisa e do órgão veiculador.

Art. 35-A. (Vide ADIN 3.741-2)

Da Propaganda Eleitoral em Geral

Art. 36. A propaganda eleitoral somente é permitida após o dia 15 de agosto do ano da eleição. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º Ao postulante a candidatura a cargo eletivo é permitida a realização, na quinzena anterior à escolha pelo partido, de propaganda intrapartidária com vista à indicação de seu nome, vedado o uso de rádio, televisão e *outdoor*.

§ 2º Não será permitido qualquer tipo de propaganda política paga no rádio e na televisão. (Redação dada pela Lei nº 13.487, de 2017)

§ 3º A violação do disposto neste artigo sujeitará o responsável pela divulgação da propaganda e, quando comprovado o seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 25.000,00 (vinte e cinco mil reais), ou ao equivalente ao custo da propaganda, se este for maior. (Redação dada pela Lei nº 12.034, de 2009)

§ 4º Na propaganda dos candidatos a cargo majoritário deverão constar, também, os nomes dos candidatos a vice ou a suplentes de senador, de modo claro e legível, em tamanho não inferior a 30% (trinta por cento) do nome do titular. (Redação dada pela Lei nº 13.165, de 2015)

§ 5º A comprovação do cumprimento das determinações da Justiça Eleitoral relacionadas a propaganda realizada em desconformidade com o disposto nesta Lei poderá ser apresentada no Tribunal Superior Eleitoral, no caso de candidatos a Presidente e Vice-Presidente da República, nas sedes dos respectivos Tribunais Regionais Eleitorais, no caso de candidatos a Governador, Vice-Governador, Deputado Federal, Senador da República, Deputados Estadual e Distrital, e, no Juízo Eleitoral, na hipótese de candidato a Prefeito, Vice-Prefeito e Vereador. (Incluído pela Lei nº 12.034, de 2009)

Art. 36-A. Não configuram propaganda eleitoral antecipada, desde que não envolvam pedido explícito de voto, a menção à pretensa candidatura, a exaltação das qualidades pessoais dos pré-candidatos e os seguintes atos, que poderão ter cobertura dos meios de comunicação social, inclusive via internet: (Redação dada pela Lei nº 13.165, de 2015)

I - a participação de filiados a partidos políticos ou de pré-candidatos em entrevistas, programas, encontros ou debates no rádio, na televisão e na internet, inclusive com a exposição de plataformas e projetos políticos, observado pelas emissoras de rádio e de televisão o dever de conferir tratamento isonômico; (Redação dada pela Lei nº 12.891, de 2013)

II - a realização de encontros, seminários ou congressos, em ambiente fechado e a expensas dos partidos políticos, para tratar da organização dos processos eleitorais, discussão de políticas públicas, planos de governo ou alianças partidárias visando às eleições, podendo tais atividades ser divulgadas pelos instrumentos de comunicação intrapartidária; (Redação dada pela Lei nº 12.891, de 2013)

III - a realização de prévias partidárias e a respectiva distribuição de material informativo, a divulgação dos nomes dos filiados que participarão da disputa e a realização de debates entre os pré-candidatos; (Redação dada pela Lei nº 13.165, de 2015)

IV - a divulgação de atos de parlamentares e debates legislativos, desde que não se faça pedido de votos; (Redação dada pela Lei nº 12.891, de 2013)

V - a divulgação de posicionamento pessoal sobre questões políticas, inclusive nas redes sociais; (Redação dada pela Lei nº 13.165, de 2015)

VI - a realização, a expensas de partido político, de reuniões de iniciativa da sociedade civil, de veículo ou meio de comunicação ou do próprio partido, em qualquer localidade, para divulgar ideias, objetivos e propostas partidárias. (Incluído pela Lei nº 13.165, de 2015

VII - campanha de arrecadação prévia de recursos na modalidade prevista no inciso IV do § 4º do art. 23 desta Lei. (Incluído dada pela Lei nº 13.488, de 2017)

§ 1º É vedada a transmissão ao vivo por emissoras de rádio e de televisão das prévias partidárias, sem prejuízo da cobertura dos meios de comunicação social. (Incluído pela Lei nº 13.165, de 2015)

§ 2º Nas hipóteses dos incisos I a VI do **caput**, são permitidos o pedido de apoio político e a divulgação da pré-candidatura, das ações políticas desenvolvidas e das que se pretende desenvolver. (Incluído pela Lei nº 13.165, de 2015)

§ 3º O disposto no § 2º não se aplica aos profissionais de comunicação social no exercício da profissão. (Incluído pela Lei nº 13.165, de 2015)

Art. 36-B. Será considerada propaganda eleitoral antecipada a convocação, por parte do Presidente da República, dos Presidentes da Câmara dos Deputados, do Senado Federal e do Supremo Tribunal Federal, de redes de radiodifusão para divulgação de atos que denotem propaganda política ou ataques a partidos políticos e seus filiados ou instituições. (Incluído pela Lei nº 12.891, de 2013)

Parágrafo único. Nos casos permitidos de convocação das redes de radiodifusão, é vedada a utilização de símbolos ou imagens, exceto aqueles previstos no § 1º do art. 13 da Constituição Federal. (Incluído pela Lei nº 12.891, de 2013)

Art. 37. Nos bens cujo uso dependa de cessão ou permissão do poder público, ou que a ele pertençam, e nos bens de uso comum, inclusive postes de iluminação pública, sinalização de tráfego, viadutos, passarelas, pontes, paradas de ônibus e outros equipamentos urbanos, é vedada a veiculação de propaganda de qualquer natureza, inclusive pichação, inscrição a tinta e exposição de placas, estandartes, faixas, cavaletes, bonecos e assemelhados. (Redação dada pela Lei nº 13.165, de 2015) (Vide ADPF Nº 548)

§ 1º A veiculação de propaganda em desacordo com o disposto no **caput** deste artigo sujeita o responsável, após a notificação e comprovação, à restauração do bem e, caso não cumprida no prazo, a multa no valor de R$ 2.000,00 (dois mil reais) a R$ 8.000,00 (oito mil reais). (Redação dada pela Lei nº 11.300, de 2006)

§ 2º Não é permitida a veiculação de material de propaganda eleitoral em bens públicos ou particulares, exceto de: (Redação dada pela Lei nº 13.488, de 2017)

I - bandeiras ao longo de vias públicas, desde que móveis e que não dificultem o bom andamento do trânsito de pessoas e veículos; (Incluído dada pela Lei nº 13.488, de 2017)

II - adesivo plástico em automóveis, caminhões, bicicletas, motocicletas e janelas residenciais, desde que não exceda a 0,5 m² (meio metro quadrado). (Incluído dada pela Lei nº 13.488, de 2017)

§ 3º Nas dependências do Poder Legislativo, a veiculação de propaganda eleitoral fica a critério da Mesa Diretora.

§ 4º Bens de uso comum, para fins eleitorais, são os assim definidos pela Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil e também aqueles a que a população em geral tem acesso, tais como cinemas, clubes, lojas, centros comerciais, templos, ginásios, estádios, ainda que de propriedade privada. (Incluído pela Lei nº 12.034, de 2009)

§ 5º Nas árvores e nos jardins localizados em áreas públicas, bem como em muros, cercas e tapumes divisórios, não é permitida a colocação de propaganda eleitoral de qualquer natureza, mesmo que não lhes cause dano. (Incluído pela Lei nº 12.034, de 2009)

§ 6º É permitida a colocação de mesas para distribuição de material de campanha e a utilização de bandeiras ao longo das vias públicas, desde que móveis e que não dificultem o bom andamento do trânsito de pessoas e veículos. (Redação dada pela Lei nº 12.891, de 2013)

§ 7º A mobilidade referida no § 6º estará caracterizada com a colocação e a retirada dos meios de propaganda entre as seis horas e as vinte e duas horas. (Incluído pela Lei nº 12.034, de 2009)

§ 8º A veiculação de propaganda eleitoral em bens particulares deve ser espontânea e gratuita, sendo vedado qualquer tipo de pagamento em troca de espaço para esta finalidade. (Incluído pela Lei nº 12.034, de 2009)

Art. 38. Independe da obtenção de licença municipal e de autorização da Justiça Eleitoral a veiculação de propaganda eleitoral pela distribuição de folhetos, adesivos, volantes e outros impressos, os quais devem ser editados sob a responsabilidade do partido, coligação ou candidato. (Redação dada pela Lei nº 12.891, de 2013)

§ 1º Todo material impresso de campanha eleitoral deverá conter o número de inscrição no Cadastro Nacional da Pessoa Jurídica - CNPJ ou o número de inscrição no Cadastro de Pessoas Físicas - CPF do responsável pela confecção, bem como de quem a contratou, e a respectiva tiragem. (Incluído pela Lei nº 12.034, de 2009)

§ 2º Quando o material impresso veicular propaganda conjunta de diversos candidatos, os gastos relativos a cada um deles deverão constar na respectiva prestação de contas, ou apenas naquela relativa ao que houver arcado com os custos. (Incluído pela Lei nº 12.034, de 2009)

§ 3º Os adesivos de que trata o **caput** deste artigo poderão ter a dimensão máxima de 50 (cinquenta) centímetros por 40 (quarenta) centímetros. (Incluído pela Lei nº 12.891, de 2013)

§ 4º É proibido colar propaganda eleitoral em veículos, exceto adesivos microperfurados até a extensão total do para-brisa traseiro e, em outras posições, adesivos até a dimensão máxima fixada no § 3º. (Incluído pela Lei nº 12.891, de 2013)

Art. 39. A realização de qualquer ato de propaganda partidária ou eleitoral, em recinto aberto ou fechado, não depende de licença da polícia. (Vide ADIN 5970)

§ 1º O candidato, partido ou coligação promotora do ato fará a devida comunicação à autoridade policial em, no mínimo, vinte e quatro horas antes de sua realização, a fim de que esta lhe garanta, segundo a prioridade do aviso, o direito contra quem tencione usar o local no mesmo dia e horário.

§ 2º A autoridade policial tomará as providências necessárias à garantia da realização do ato e ao funcionamento do tráfego e dos serviços públicos que o evento possa afetar.

§ 3º O funcionamento de alto-falantes ou amplificadores de som, ressalvada a hipótese contemplada no parágrafo seguinte, somente é permitido entre as oito e as vinte e duas horas, sendo vedados a instalação e o uso daqueles equipamentos em distância inferior a duzentos metros:

I - das sedes dos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios, das sedes dos Tribunais Judiciais, e dos quartéis e outros estabelecimentos militares;

II - dos hospitais e casas de saúde;

III - das escolas, bibliotecas públicas, igrejas e teatros, quando em funcionamento.

§ 4º A realização de comícios e a utilização de aparelhagens de sonorização fixas são permitidas no horário compreendido entre as 8 (oito) e as 24 (vinte e quatro) horas, com exceção do comício de encerramento da campanha, que poderá ser prorrogado por mais 2 (duas) horas. (Redação dada pela Lei nº 12.891, de 2013)

§ 5º Constituem crimes, no dia da eleição, puníveis com detenção, de seis meses a um ano, com a alternativa de prestação de serviços à comunidade pelo mesmo período, e multa no valor de cinco mil a quinze mil UFIR:

I - o uso de alto-falantes e amplificadores de som ou a promoção de comício ou carreata;

II - a arregimentação de eleitor ou a propaganda de boca de urna; (Redação dada pela Lei nº 11.300, de 2006)

III - a divulgação de qualquer espécie de propaganda de partidos políticos ou de seus candidatos. (Redação dada pela Lei nº 12.034, de 2009)

IV - a publicação de novos conteúdos ou o impulsionamento de conteúdos nas aplicações de internet de que trata o art. 57-B desta Lei, podendo ser mantidos em funcionamento as aplicações e os conteúdos publicados anteriormente. (Incluído dada pela Lei nº 13.488, de 2017)

§ 6º É vedada na campanha eleitoral a confecção, utilização, distribuição por comitê, candidato, ou com a sua autorização, de camisetas, chaveiros, bonés, canetas, brindes, cestas básicas ou quaisquer outros bens ou materiais que possam proporcionar vantagem ao eleitor. (Incluído pela Lei nº 11.300, de 2006)

§ 7º É proibida a realização de *showmício* e de evento assemelhado para promoção de candidatos, bem como a apresentação, remunerada ou não, de artistas com a finalidade de animar comício e reunião eleitoral. (Incluído pela Lei nº 11.300, de 2006) (Vide ADIN 5970)

§ 8º É vedada a propaganda eleitoral mediante **outdoors**, inclusive eletrônicos, sujeitando-se a empresa responsável, os partidos, as coligações e os candidatos à imediata retirada da propaganda irregular e ao pagamento de multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 15.000,00 (quinze mil reais). (Redação dada pela Lei nº 12.891, de 2013)

§ 9º Até as vinte e duas horas do dia que antecede a eleição, serão permitidos distribuição de material gráfico, caminhada, carreata, passeata ou carro de som que transite pela cidade divulgando jingles ou mensagens de candidatos. (Incluído pela Lei nº 12.034, de 2009)

§ 9º-A. Considera-se carro de som, além do previsto no § 12, qualquer veículo, motorizado ou não, ou ainda tracionado por animais, que transite divulgando **jingles** ou mensagens de candidatos. (Incluído pela Lei nº 13.165, de 2015)

§ 10. Fica vedada a utilização de trios elétricos em campanhas eleitorais, exceto para a sonorização de comícios. (Incluído pela Lei nº 12.034, de 2009)

§ 11. É permitida a circulação de carros de som e minitrios como meio de propaganda eleitoral, desde que observado o limite de oitenta decibéis de nível de pressão sonora, medido a sete metros de distância do veículo, e respeitadas as vedações previstas no § 3º deste artigo, apenas em carreatas, caminhadas e passeatas ou durante reuniões e comícios. (Redação dada pela Lei nº 13.488, de 2017)

§ 12. Para efeitos desta Lei, considera-se: (Incluído pela Lei nº 12.891, de 2013)

I - carro de som: veículo automotor que usa equipamento de som com potência nominal de amplificação de, no máximo, 10.000 (dez mil) watts; (Incluído pela Lei nº 12.891, de 2013)

II - minitrio: veículo automotor que usa equipamento de som com potência nominal de amplificação maior que 10.000 (dez mil) watts e até 20.000 (vinte mil) watts; (Incluído pela Lei nº 12.891, de 2013)

III - trio elétrico: veículo automotor que usa equipamento de som com potência nominal de amplificação maior que 20.000 (vinte mil) watts. (Incluído pela Lei nº 12.891, de 2013)

Art. 39-A. É permitida, no dia das eleições, a manifestação individual e silenciosa da preferência do eleitor por partido político, coligação ou candidato, revelada exclusivamente pelo uso de bandeiras, broches, dísticos e adesivos. (Incluído pela Lei nº 12.034, de 2009)

§ 1º É vedada, no dia do pleito, até o término do horário de votação, a aglomeração de pessoas portando vestuário padronizado, bem como os instrumentos de propaganda referidos no caput, de modo a caracterizar manifestação coletiva, com ou sem utilização de veículos. (Incluído pela Lei nº 12.034, de 2009)

§ 2º No recinto das seções eleitorais e juntas apuradoras, é proibido aos servidores da Justiça Eleitoral, aos mesários e aos escrutinadores o uso de vestuário ou objeto que contenha qualquer propaganda de partido político, de coligação ou de candidato. (Incluído pela Lei nº 12.034, de 2009)

§ 3º Aos fiscais partidários, nos trabalhos de votação, só é permitido que, em seus crachás, constem o nome e a sigla do partido político ou coligação a que sirvam, vedada a padronização do vestuário. (Incluído pela Lei nº 12.034, de 2009)

§ 4º No dia do pleito, serão afixadas cópias deste artigo em lugares visíveis nas partes interna e externa das seções eleitorais. (Incluído pela Lei nº 12.034, de 2009)

Art. 40. O uso, na propaganda eleitoral, de símbolos, frases ou imagens, associadas ou semelhantes às empregadas por órgão de governo, empresa pública ou sociedade de economia mista constitui crime, punível com detenção, de seis meses a um ano, com a alternativa de prestação de serviços à comunidade pelo mesmo período, e multa no valor de dez mil a vinte mil UFIR.

Art. 40-A. (VETADO) (Incluído pela Lei nº 11.300, de 2006)

Art. 40-B. A representação relativa à propaganda irregular deve ser instruída com prova da autoria ou do prévio conhecimento do beneficiário, caso este não seja por ela responsável. (Incluído pela Lei nº 12.034, de 2009)

Parágrafo único. A responsabilidade do candidato estará demonstrada se este, intimado da existência da propaganda irregular, não providenciar, no prazo de quarenta e oito horas, sua retirada ou regularização e, ainda, se as circunstâncias e as peculiaridades do caso específico revelarem a impossibilidade de o beneficiário não ter tido conhecimento da propaganda. (Incluído pela Lei nº 12.034, de 2009)

Art. 41. A propaganda exercida nos termos da legislação eleitoral não poderá ser objeto de multa nem cerceada sob alegação do exercício do poder de polícia ou de violação de postura municipal, casos em que se deve proceder na forma prevista no art. 40. (Redação dada pela Lei nº 12.034, de 2009)

§ 1º O poder de polícia sobre a propaganda eleitoral será exercido pelos juízes eleitorais e pelos juízes designados pelos Tribunais Regionais Eleitorais. (Incluído pela Lei nº 12.034, de 2009)

§ 2º O poder de polícia se restringe às providências necessárias para inibir práticas ilegais, vedada a censura prévia sobre o teor dos programas a serem exibidos na televisão, no rádio ou na internet. (Incluído pela Lei nº 12.034, de 2009)

Art. 41-A. Ressalvado o disposto no art. 26 e seus incisos, constitui captação de sufrágio, vedada por esta Lei, o candidato doar, oferecer, prometer, ou entregar, ao eleitor, com o fim de obter-lhe o voto, bem ou vantagem pessoal de qualquer natureza, inclusive emprego ou função pública, desde o registro da candidatura até o dia da eleição, inclusive, sob pena de multa de mil a cinqüenta mil Ufir, e cassação do registro ou do diploma, observado o procedimento previsto no art. 22 da Lei Complementar nº 64, de 18 de maio de 1990. (Incluído pela Lei nº 9.840, de 1999)

§ 1º Para a caracterização da conduta ilícita, é desnecessário o pedido explícito de votos, bastando a evidência do dolo, consistente no especial fim de agir. (Incluído pela Lei nº 12.034, de 2009)

§ 2º As sanções previstas no caput aplicam-se contra quem praticar atos de violência ou grave ameaça a pessoa, com o fim de obter-lhe o voto. (Incluído pela Lei nº 12.034, de 2009)

§ 3º A representação contra as condutas vedadas no caput poderá ser ajuizada até a data da diplomação. (Incluído pela Lei nº 12.034, de 2009)

§ 4º O prazo de recurso contra decisões proferidas com base neste artigo será de 3 (três) dias, a contar da data da publicação do julgamento no Diário Oficial. (Incluído pela Lei nº 12.034, de 2009)

Da Propaganda Eleitoral mediante *outdoors*

Art. 42. (Revogado pela Lei nº 11.300, de 2006)

Da Propaganda Eleitoral na Imprensa

Art. 43. São permitidas, até a antevéspera das eleições, a divulgação paga, na imprensa escrita, e a reprodução na internet do jornal impresso, de até 10 (dez) anúncios de propaganda eleitoral, por veículo, em datas diversas, para cada candidato, no espaço máximo, por edição, de 1/8 (um oitavo) de página de jornal padrão e de 1/4 (um quarto) de página de revista ou tabloide. (Redação dada pela Lei nº 12.034, de 2009)

§ 1º Deverá constar do anúncio, de forma visível, o valor pago pela inserção. (Incluído pela Lei nº 12.034, de 2009)

§ 2º A inobservância do disposto neste artigo sujeita os responsáveis pelos veículos de divulgação e os partidos, coligações ou candidatos beneficiados a multa no valor de R$ 1.000,00 (mil reais) a R$ 10.000,00 (dez mil reais) ou equivalente ao da divulgação da propaganda paga, se este for maior. (Renumerado do parágrafo único pela Lei nº 12.034, de 2009)

Da Propaganda Eleitoral no Rádio e na Televisão

Art. 44. A propaganda eleitoral no rádio e na televisão restringe-se ao horário gratuito definido nesta Lei, vedada a veiculação de propaganda paga.

§ 1º A propaganda eleitoral gratuita na televisão deverá utilizar a Linguagem Brasileira de Sinais - LIBRAS ou o recurso de legenda, que deverão constar obrigatoriamente do material entregue às emissoras. (Incluído pela Lei nº 12.034, de 2009)

§ 2º No horário reservado para a propaganda eleitoral, não se permitirá utilização comercial ou propaganda realizada com a intenção, ainda que disfarçada ou subliminar, de promover marca ou produto. (Incluído pela Lei nº 12.034, de 2009)

§ 3º Será punida, nos termos do § 1º do art. 37, a emissora que, não autorizada a funcionar pelo poder competente, veicular propaganda eleitoral. (Incluído pela Lei nº 12.034, de 2009)

Art. 45. Encerrado o prazo para a realização das convenções no ano das eleições, é vedado às emissoras de rádio e televisão, em sua programação normal e em seu noticiário: (Redação dada pela Lei nº 13.165, de 2015)

I - transmitir, ainda que sob a forma de entrevista jornalística, imagens de realização de pesquisa ou qualquer outro tipo de consulta popular de natureza eleitoral em que seja possível identificar o entrevistado ou em que haja manipulação de dados;

II - usar trucagem, montagem ou outro recurso de áudio ou vídeo que, de qualquer forma, degradem ou ridicularizem candidato, partido ou coligação, ou produzir ou veicular programa com esse efeito; (Vide ADIN 4.451)

III - veicular propaganda política ou difundir opinião favorável ou contrária a candidato, partido, coligação, a seus órgãos ou representantes; (Vide ADIN 4.451)

IV - dar tratamento privilegiado a candidato, partido ou coligação;

V - veicular ou divulgar filmes, novelas, minisséries ou qualquer outro programa com alusão ou crítica a candidato ou partido político, mesmo que dissimuladamente, exceto programas jornalísticos ou debates políticos;

VI - divulgar nome de programa que se refira a candidato escolhido em convenção, ainda quando preexistente, inclusive se coincidente com o nome do candidato ou com a variação nominal por ele adotada. Sendo o nome do programa o mesmo que o do candidato, fica proibida a sua divulgação, sob pena de cancelamento do respectivo registro.

§ 1º A partir de 30 de junho do ano da eleição, é vedado, ainda, às emissoras transmitir programa apresentado ou comentado por pré-candidato, sob pena, no caso de sua escolha na convenção partidária, de imposição da multa prevista no § 2º e de cancelamento do registro da candidatura do beneficiário. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º Sem prejuízo do disposto no parágrafo único do art. 55, a inobservância do disposto neste artigo sujeita a emissora ao pagamento de multa no valor de vinte mil a cem mil UFIR, duplicada em caso de reincidência.

§ 3º . (Revogado pela Lei nº 12.034, de 2009)

§ 4º Entende-se por trucagem todo e qualquer efeito realizado em áudio ou vídeo que degradar ou ridicularizar candidato, partido político ou coligação, ou que desvirtuar a realidade e beneficiar ou prejudicar qualquer candidato, partido político ou coligação. (Incluído pela Lei nº 12.034, de 2009) (Vide ADIN 4.451)

§ 5º Entende-se por montagem toda e qualquer junção de registros de áudio ou vídeo que degradar ou ridicularizar candidato, partido político ou coligação, ou que desvirtuar a realidade e beneficiar ou prejudicar qualquer candidato, partido político ou coligação. (Incluído pela Lei nº 12.034, de 2009) (Vide ADIN 4.451)

§ 6º É permitido ao partido político utilizar na propaganda eleitoral de seus candidatos em âmbito regional, inclusive no horário eleitoral gratuito, a imagem e a voz de candidato ou militante de partido político que integre a sua coligação em âmbito nacional. (Incluído pela Lei nº 12.034, de 2009)

Art. 46. Independentemente da veiculação de propaganda eleitoral gratuita no horário definido nesta Lei, é facultada a transmissão por emissora de rádio ou televisão de debates sobre as eleições majoritária ou proporcional, assegurada a participação de candidatos dos partidos com representação no Congresso Nacional, de, no mínimo, cinco parlamentares, e facultada a dos demais, observado o seguinte: (Redação dada pela Lei nº 13.488, de 2017)

I - nas eleições majoritárias, a apresentação dos debates poderá ser feita:

a) em conjunto, estando presentes todos os candidatos a um mesmo cargo eletivo;

b) em grupos, estando presentes, no mínimo, três candidatos;

II - nas eleições proporcionais, os debates deverão ser organizados de modo que assegurem a presença de número equivalente de candidatos de todos os partidos a um mesmo cargo eletivo e poderão desdobrar-se em mais de um dia, respeitada a proporção de homens e mulheres estabelecida no § 3º do art. 10 desta Lei; (Redação dada pela Lei nº 14.211, de 2021)

III - os debates deverão ser parte de programação previamente estabelecida e divulgada pela emissora, fazendo-se mediante sorteio a escolha do dia e da ordem de fala de cada candidato, salvo se celebrado acordo em outro sentido entre os partidos e coligações interessados.

§ 1º Será admitida a realização de debate sem a presença de candidato de algum partido, desde que o veículo de comunicação responsável comprove havê-lo convidado com a antecedência mínima de setenta e duas horas da realização do debate.

§ 2º É vedada a presença de um mesmo candidato a eleição proporcional em mais de um debate da mesma emissora.

§ 3º O descumprimento do disposto neste artigo sujeita a empresa infratora às penalidades previstas no art. 56.

§ 4º O debate será realizado segundo as regras estabelecidas em acordo celebrado entre os partidos políticos e a pessoa jurídica interessada na realização do evento, dando-se ciência à Justiça Eleitoral. (Incluído pela Lei nº 12.034, de 2009)

§ 5º Para os debates que se realizarem no primeiro turno das eleições, serão consideradas aprovadas as regras, inclusive as que definirem o número de participantes, que obtiverem a concordância de pelo menos 2/3 (dois terços) dos candidatos aptos, no caso de eleição majoritária, e de pelo menos 2/3 (dois terços) dos partidos com candidatos aptos, no caso de eleição proporcional. (Redação dada pela Lei nº 14.211, de 2021)

Art. 47. As emissoras de rádio e de televisão e os canais de televisão por assinatura mencionados no art. 57 reservarão, nos trinta e cinco dias anteriores à antevéspera das eleições, horário destinado à divulgação, em rede, da propaganda eleitoral gratuita, na forma estabelecida neste artigo. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º A propaganda será feita:

I - na eleição para Presidente da República, às terças e quintas-feiras e aos sábados:

a) das sete horas às sete horas e doze minutos e trinta segundos e das doze horas às doze horas e doze minutos e trinta segundos, no rádio; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas às treze horas e doze minutos e trinta segundos e das vinte horas e trinta minutos às vinte horas e quarenta e dois minutos e trinta segundos, na televisão; (Redação dada pela Lei nº 13.165, de 2015)

II - nas eleições para Deputado Federal, às terças e quintas-feiras e aos sábados:

a) das sete horas e doze minutos e trinta segundos às sete horas e vinte e cinco minutos e das doze horas e doze minutos e trinta segundos às doze horas e vinte e cinco minutos, no rádio; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas e doze minutos e trinta segundos às treze horas e vinte e cinco minutos e das vinte horas e quarenta e dois minutos e trinta segundos às vinte horas e cinquenta e cinco minutos, na televisão; (Redação dada pela Lei nº 13.165, de 2015)

III - nas eleições para Senador, às segundas, quartas e sextas-feiras: (Redação dada pela Lei nº 13.165, de 2015)

a) das sete horas às sete horas e cinco minutos e das doze horas às doze horas e cinco minutos, no rádio, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas às treze horas e cinco minutos e das vinte horas e trinta minutos às vinte horas e trinta e cinco minutos, na televisão, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

c) das sete horas às sete horas e sete minutos e das doze horas às doze horas e sete minutos, no rádio, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

d) das treze horas às treze horas e sete minutos e das vinte horas e trinta minutos às vinte horas e trinta e sete minutos, na televisão, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

IV - nas eleições para Deputado Estadual e Deputado Distrital, às segundas, quartas e sextas-feiras:

a) das sete horas e cinco minutos às sete horas e quinze minutos e das doze horas e cinco minutos às doze horas e quinze minutos, no rádio, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas e cinco minutos às treze horas e quinze minutos e das vinte horas e trinta e cinco minutos às vinte horas e quarenta e cinco minutos, na televisão, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

c) das sete horas e sete minutos às sete horas e dezesseis minutos e das doze horas e sete minutos às doze horas e dezesseis minutos, no rádio, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

d) das treze horas e sete minutos às treze horas e dezesseis minutos e das vinte horas e trinta e sete minutos às vinte horas e quarenta e seis minutos, na televisão, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

V - na eleição para Governador de Estado e do Distrito Federal, às segundas, quartas e sextas-feiras: (Redação dada pela Lei nº 13.165, de 2015)

a) das sete horas e quinze minutos às sete horas e vinte e cinco minutos e das doze horas e quinze minutos às doze horas e vinte e cinco minutos, no rádio, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas e quinze minutos às treze horas e vinte e cinco minutos e das vinte horas e quarenta e cinco minutos às vinte horas e cinquenta e cinco minutos, na televisão, nos anos em que a renovação do Senado Federal se der por um terço; (Redação dada pela Lei nº 13.165, de 2015)

c) das sete horas e dezesseis minutos às sete horas e vinte e cinco minutos e das doze horas e dezesseis minutos às doze horas e vinte e cinco minutos, no rádio, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

d) das treze horas e dezesseis minutos às treze horas e vinte e cinco minutos e das vinte horas e quarenta e seis minutos às vinte horas e cinquenta e cinco minutos, na televisão, nos anos em que a renovação do Senado Federal se der por dois terços; (Redação dada pela Lei nº 13.165, de 2015)

VI - nas eleições para Prefeito, de segunda a sábado: (Redação dada pela Lei nº 13.165, de 2015)

a) das sete horas às sete horas e dez minutos e das doze horas às doze horas e dez minutos, no rádio; (Redação dada pela Lei nº 13.165, de 2015)

b) das treze horas às treze horas e dez minutos e das vinte horas e trinta minutos às vinte horas e quarenta minutos, na televisão; (Redação dada pela Lei nº 13.165, de 2015)

VII - ainda nas eleições para Prefeito, e também nas de Vereador, mediante inserções de trinta e sessenta segundos, no rádio e na televisão, totalizando setenta minutos diários, de segunda-feira a domingo, distribuídas ao longo da programação veiculada entre as cinco e as vinte e quatro horas, na proporção de 60% (sessenta por cento) para Prefeito e 40% (quarenta por cento) para Vereador. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º-A Somente serão exibidas as inserções de televisão a que se refere o inciso VII do § 1º nos Municípios em que houver estação geradora de serviços de radiodifusão de sons e imagens. (Incluído pela Lei nº 13.165, de 2015)

§ 2º Os horários reservados à propaganda de cada eleição, nos termos do § 1º, serão distribuídos entre todos os partidos e coligações que tenham candidato, observados os seguintes critérios: (Redação dada pela Lei nº 12.875, de 2013) (Vide ADI-5105)

I - 90% (noventa por cento) distribuídos proporcionalmente ao número de representantes na Câmara dos Deputados, considerado, no caso de coligação para as eleições majoritárias, o resultado da soma do número de representantes dos 6 (seis) maiores partidos que a integrem; (Redação dada pela Lei nº 14.211, de 2021)

II - 10% (dez por cento) distribuídos igualitariamente. (Redação dada pela Lei nº 13.165, de 2015)

§ 3º Para efeito do disposto neste artigo, a representação de cada partido na Câmara dos Deputados é a resultante da eleição. (Redação dada pela Lei nº 11.300, de 2006)

§ 4º O número de representantes de partido que tenha resultado de fusão ou a que se tenha incorporado outro corresponderá à soma dos representantes que os partidos de origem possuíam na data mencionada no parágrafo anterior.

§ 5º Se o candidato a Presidente ou a Governador deixar de concorrer, em qualquer etapa do pleito, e não havendo a substituição prevista no art. 13 desta Lei, far-se-á nova distribuição do tempo entre os candidatos remanescentes.

§ 6º Aos partidos e coligações que, após a aplicação dos critérios de distribuição referidos no *caput*, obtiverem direito a parcela do horário eleitoral inferior a trinta segundos, será assegurado o direito de acumulá-lo para uso em tempo equivalente.

§ 7º Para efeito do disposto no § 2º, serão desconsideradas as mudanças de filiação partidária em quaisquer hipóteses. (Redação dada pela Lei nº 13.107, de 2015)

§ 8º As mídias com as gravações da propaganda eleitoral no rádio e na televisão serão entregues às emissoras, inclusive nos sábados, domingos e feriados, com a antecedência mínima: (Incluído pela Lei nº 12.891, de 2013)

I - de 6 (seis) horas do horário previsto para o início da transmissão, no caso dos programas em rede; (Incluído pela Lei nº 12.891, de 2013)

II - de 12 (doze) horas do horário previsto para o início da transmissão, no caso das inserções. (Incluído pela Lei nº 12.891, de 2013)

§ 9º As emissoras de rádio sob responsabilidade do Senado Federal e da Câmara dos Deputados instaladas em localidades fora do Distrito Federal são dispensadas da veiculação da propaganda eleitoral gratuita dos pleitos referidos nos incisos II a VI do § 1º. (Incluído pela Lei nº 13.165, de 2015)

Art. 48. Nas eleições para Prefeitos e Vereadores, nos Municípios em que não haja emissora de rádio e televisão, a Justiça Eleitoral garantirá aos Partidos Políticos participantes do pleito a veiculação de propaganda eleitoral gratuita nas localidades aptas à realização de segundo turno de eleições e nas quais seja operacionalmente viável realizar a retransmissão. (Redação dada pela Lei nº 12.034, de 2009)

§ 1º (Revogado pela Lei nº 13.165, de 2015)

§ 2º (Revogado pela Lei nº 13.165, de 2015)

Art. 49. Se houver segundo turno, as emissoras de rádio e televisão reservarão, a partir da sexta-feira seguinte à realização do primeiro turno e até a antevéspera da eleição, horário destinado à divulgação da propaganda eleitoral gratuita, dividida em dois blocos diários de dez minutos para cada eleição, e os blocos terão início às sete e às doze horas, no rádio, e às treze e às vinte horas e trinta minutos, na televisão. (Redação dada pela Lei nº 13.488, de 2017)

§ 1º Em circunscrição onde houver segundo turno para Presidente e Governador, o horário reservado à propaganda deste iniciar-se-á imediatamente após o término do horário reservado ao primeiro.

§ 2º O tempo de cada período diário será dividido igualitariamente entre os candidatos.

Art. 50. A Justiça Eleitoral efetuará sorteio para a escolha da ordem de veiculação da propaganda de cada partido ou coligação no primeiro dia do horário eleitoral gratuito; a cada dia que se seguir, a propaganda veiculada por último, na véspera, será a primeira, apresentando-se as demais na ordem do sorteio.

Art.51. Durante o período previsto no art. 47 desta Lei, as emissoras de rádio e televisão e os canais por assinatura mencionados no art. 57 desta Lei reservarão setenta minutos diários para a propaganda eleitoral gratuita, a serem usados em inserções de trinta e de sessenta segundos, a critério do respectivo partido ou coligação, assinadas obrigatoriamente pelo partido ou coligação, e distribuídas, ao longo da programação veiculada entre as cinco e as vinte quatro horas, nos termos do § 2º do art. 47 desta Lei, obedecido o seguinte: (Redação dada pela Lei nº 13.488, de 2017)

I - o tempo será dividido em partes iguais para a utilização nas campanhas dos candidatos às eleições majoritárias e proporcionais, bem como de suas legendas partidárias ou das que componham a coligação, quando for o caso;

II - (revogado); (Redação dada pela Lei nº 13.165, de 2015)

III - a distribuição levará em conta os blocos de audiência entre as cinco e as onze horas, as onze e as dezoito horas, e as dezoito e as vinte e quatro horas; (Redação dada pela Lei nº 13.165, de 2015)

IV - na veiculação das inserções, é vedada a divulgação de mensagens que possam degradar ou ridicularizar candidato, partido ou coligação, aplicando-se-lhes, ainda, todas as demais regras aplicadas ao horário de propaganda eleitoral, previstas no art. 47. (Redação dada pela Lei nº 12.891, de 2013)

§ 1º É vedada a veiculação de inserções idênticas no mesmo intervalo de programação, exceto se o número de inserções de que dispuser o partido exceder os intervalos disponíveis, sendo vedada a transmissão em sequência para o mesmo partido político (Redação dada pela Lei nº 13.488, de 2017)

§ 2º Durante o período previsto no art. 49 desta Lei, onde houver segundo turno, as emissoras de rádio e televisão e os canais de televisão por assinatura mencionados no art. 57 desta Lei reservarão, por cada cargo em disputa, vinte e cinco minutos para serem usados em inserções de trinta e de sessenta segundos, observadas as disposições deste artigo. (Incluído pela Lei nº 13.488, de 2017)

Art. 52. A partir do dia 15 de agosto do ano da eleição, a Justiça Eleitoral convocará os partidos e a representação das emissoras de televisão para elaborarem plano de mídia, nos termos do art. 51, para o uso da parcela do horário eleitoral gratuito a que tenham direito, garantida a todos participação nos horários de maior e menor audiência. (Redação dada pela Lei nº 13.165, de 2015)

Art. 53. Não serão admitidos cortes instantâneos ou qualquer tipo de censura prévia nos programas eleitorais gratuitos.

§ 1º É vedada a veiculação de propaganda que possa degradar ou ridicularizar candidatos, sujeitando-se o partido ou coligação infratores à perda do direito à veiculação de propaganda no horário eleitoral gratuito do dia seguinte.

§ 2º Sem prejuízo do disposto no parágrafo anterior, a requerimento de partido, coligação ou candidato, a Justiça Eleitoral impedirá a reapresentação de propaganda ofensiva à honra de candidato, à moral e aos bons costumes.

Art. 53-A. É vedado aos partidos políticos e às coligações incluir no horário destinado aos candidatos às eleições proporcionais propaganda das candidaturas a eleições majoritárias ou vice-versa, ressalvada a utilização, durante a exibição do programa, de legendas com referência aos candidatos majoritários ou, ao fundo, de cartazes ou fotografias desses candidatos, ficando autorizada a menção ao nome e ao número de qualquer candidato do partido ou da coligação. (Redação dada pela Lei nº 12.891, de 2013)

§ 1º É facultada a inserção de depoimento de candidatos a eleições proporcionais no horário da propaganda das candidaturas majoritárias e vice-versa, registrados sob o mesmo partido ou coligação, desde que o depoimento consista exclusivamente em pedido de voto ao candidato que cedeu o tempo. (Incluído pela Lei nº 12.034, de 2009)

§ 2º Fica vedada a utilização da propaganda de candidaturas proporcionais como propaganda de candidaturas majoritárias e vice-versa. (Incluído pela Lei nº 12.034, de 2009)

§ 3º O partido político ou a coligação que não observar a regra contida neste artigo perderá, em seu horário de propaganda gratuita, tempo equivalente no horário reservado à propaganda da eleição disputada pelo candidato beneficiado. (Incluído pela Lei nº 12.034, de 2009)

Art. 54. Nos programas e inserções de rádio e televisão destinados à propaganda eleitoral gratuita de cada partido ou coligação só poderão aparecer, em gravações internas e externas, observado o disposto no § 2º, candidatos, caracteres com propostas, fotos, **jingles**, clipes com música ou vinhetas, inclusive de passagem, com indicação do número do candidato ou do partido, bem como seus apoiadores, inclusive os candidatos de que trata o § 1º do art. 53-A, que poderão dispor de até 25% (vinte e cinco por cento) do tempo de cada programa ou inserção, sendo vedadas montagens, trucagens, computação gráfica, desenhos animados e efeitos especiais. (Redação dada pela Lei nº 13.165, de 2015)

§ 1º No segundo turno das eleições não será permitida, nos programas de que trata este artigo, a participação de filiados a partidos que tenham formalizado o apoio a outros candidatos. (Redação dada pela Lei nº 13.165, de 2015)

§ 2º Será permitida a veiculação de entrevistas com o candidato e de cenas externas nas quais ele, pessoalmente, exponha: (Incluído pela Lei nº 13.165, de 2015)

I - realizações de governo ou da administração pública; (Incluído pela Lei nº 13.165, de 2015)

II - falhas administrativas e deficiências verificadas em obras e serviços públicos em geral; (Incluído pela Lei nº 13.165, de 2015)

III - atos parlamentares e debates legislativos. (Incluído pela Lei nº 13.165, de 2015)

Art. 55. Na propaganda eleitoral no horário gratuito, são aplicáveis ao partido, coligação ou candidato as vedações indicadas nos incisos I e II do art. 45.

Parágrafo único. A inobservância do disposto neste artigo sujeita o partido ou coligação à perda de tempo equivalente ao dobro do usado na prática do ilícito, no período do horário gratuito subsequente, dobrada a cada reincidência, devendo o tempo correspondente ser veiculado após o programa dos demais candidatos com a informação de que a não veiculação do programa resulta de infração da lei eleitoral. (Redação dada pela Lei nº 12.891, de 2013)

Art. 56. A requerimento de partido, coligação ou candidato, a Justiça Eleitoral poderá determinar a suspensão, por vinte e quatro horas, da programação normal de emissora que deixar de cumprir as disposições desta Lei sobre propaganda.

§ 1º No período de suspensão a que se refere este artigo, a Justiça Eleitoral veiculará mensagem de orientação ao eleitor, intercalada, a cada 15 (quinze) minutos. (Redação dada pela Lei nº 12.891, de 2013)

§ 2º Em cada reiteração de conduta, o período de suspensão será duplicado.

Art. 57. As disposições desta Lei aplicam-se às emissoras de televisão que operam em VHF e UHF e os canais de televisão por assinatura sob a responsabilidade do Senado Federal, da Câmara dos Deputados, das Assembléias Legislativas, da Câmara Legislativa do Distrito Federal ou das Câmaras Municipais.

Propaganda na Internet
(Incluído pela Lei nº 13.488, de 2017)

Art. 57-A. É permitida a propaganda eleitoral na internet, nos termos desta Lei, após o dia 15 de agosto do ano da eleição. (Redação dada pela Lei nº 13.165, de 2015)

Art. 57-B. A propaganda eleitoral na internet poderá ser realizada nas seguintes formas: (Incluído pela Lei nº 12.034, de 2009) (Vide Lei nº 12.034, de 2009)

I - em sítio do candidato, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de serviço de internet estabelecido no País; (Incluído pela Lei nº 12.034, de 2009)

II - em sítio do partido ou da coligação, com endereço eletrônico comunicado à Justiça Eleitoral e hospedado, direta ou indiretamente, em provedor de serviço de internet estabelecido no País; (Incluído pela Lei nº 12.034, de 2009)

III - por meio de mensagem eletrônica para endereços cadastrados gratuitamente pelo candidato, partido ou coligação; (Incluído pela Lei nº 12.034, de 2009)

IV - por meio de blogs, redes sociais, sítios de mensagens instantâneas e aplicações de internet assemelhadas cujo conteúdo seja gerado ou editado por: (Redação dada pela Lei nº 13.488, de 2017)

a) candidatos, partidos ou coligações; ou (Incluído pela Lei nº 13.488, de 2017)

b) qualquer pessoa natural, desde que não contrate impulsionamento de conteúdos. (Incluído pela Lei nº 13.488, de 2017)

§ 1º Os endereços eletrônicos das aplicações de que trata este artigo, salvo aqueles de iniciativa de pessoa natural, deverão ser comunicados à Justiça Eleitoral, podendo ser mantidos durante todo o pleito eleitoral os mesmos endereços eletrônicos em uso antes do início da propaganda eleitoral. (Incluído pela Lei nº 13.488, de 2017)

§ 2º Não é admitida a veiculação de conteúdos de cunho eleitoral mediante cadastro de usuário de aplicação de internet com a intenção de falsear identidade. (Incluído pela Lei nº 13.488, de 2017)

§ 3º É vedada a utilização de impulsionamento de conteúdos e ferramentas digitais não disponibilizadas pelo provedor da aplicação de internet, ainda que gratuitas, para alterar o teor ou a repercussão de propaganda eleitoral, tanto próprios quanto de terceiros. (Incluído pela Lei nº 13.488, de 2017)

§ 4º O provedor de aplicação de internet que possibilite o impulsionamento pago de conteúdos deverá contar com canal de comunicação com seus usuários e somente poderá ser responsabilizado por danos decorrentes do conteúdo impulsionado se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente pela Justiça Eleitoral. (Incluído pela Lei nº 13.488, de 2017)

§ 5º A violação do disposto neste artigo sujeita o usuário responsável pelo conteúdo e, quando comprovado seu prévio conhecimento, o beneficiário, à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais) ou em valor equivalente ao dobro da quantia despendida, se esse cálculo superar o limite máximo da multa. (Incluído pela Lei nº 13.488, de 2017)

§ 6º (VETADO). (Incluído pela Lei nº 13.488, de 2017)

Art. 57-C. É vedada a veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos, coligações e candidatos e seus representantes. (Redação dada pela Lei nº 13.488, de 2017)

§ 1º É vedada, ainda que gratuitamente, a veiculação de propaganda eleitoral na internet, em sítios: (Incluído pela Lei nº 12.034, de 2009)

I - de pessoas jurídicas, com ou sem fins lucrativos; (Incluído pela Lei nº 12.034, de 2009)

II - oficiais ou hospedados por órgãos ou entidades da administração pública direta ou indireta da União, dos Estados, do Distrito Federal e dos Municípios. (Incluído pela Lei nº 12.034, de 2009)

§ 2º A violação do disposto neste artigo sujeita o responsável pela divulgação da propaganda ou pelo impulsionamento de conteúdos e, quando comprovado seu prévio conhecimento, o beneficiário, à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais) ou em valor equivalente ao dobro da quantia despendida, se esse cálculo superar o limite máximo da multa. (Redação dada pela Lei nº 13.488, de 2017)

§ 3º O impulsionamento de que trata o **caput** deste artigo deverá ser contratado diretamente com provedor da aplicação de internet com sede e foro no País, ou de sua filial, sucursal, escritório, estabelecimento ou representante legalmente estabelecido no País e apenas com o fim de promover ou beneficiar candidatos ou suas agremiações. (Incluído pela Lei nº 13.488, de 2017)

Art. 57-D. É livre a manifestação do pensamento, vedado o anonimato durante a campanha eleitoral, por meio da rede mundial de computadores - internet, assegurado o direito de resposta, nos termos das alíneas *a*, *b* e *c* do inciso IV do § 3º do art. 58 e do 58-A, e por outros meios de comunicação interpessoal mediante mensagem eletrônica. (Incluído pela Lei nº 12.034, de 2009)

§ 1º (VETADO) (Incluído pela Lei nº 12.034, de 2009)

§ 2º A violação do disposto neste artigo sujeitará o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais). (Incluído pela Lei nº 12.034, de 2009)

§ 3º Sem prejuízo das sanções civis e criminais aplicáveis ao responsável, a Justiça Eleitoral poderá determinar, por solicitação do ofendido, a retirada de publicações que contenham agressões ou ataques a candidatos em sítios da internet, inclusive redes sociais. (Incluído pela Lei nº 12.891, de 2013)

Art. 57-E. São vedadas às pessoas relacionadas no art. 24 a utilização, doação ou cessão de cadastro eletrônico de seus clientes, em favor de candidatos, partidos ou coligações. (Incluído pela Lei nº 12.034, de 2009)

§ 1º É proibida a venda de cadastro de endereços eletrônicos. (Incluído pela Lei nº 12.034, de 2009)

§ 2º A violação do disposto neste artigo sujeita o responsável pela divulgação da propaganda e, quando comprovado seu prévio conhecimento, o beneficiário à multa no valor de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais). (Incluído pela Lei nº 12.034, de 2009)

Art. 57-F. Aplicam-se ao provedor de conteúdo e de serviços multimídia que hospeda a divulgação da propaganda eleitoral de candidato, de partido ou de coligação as penalidades previstas nesta Lei, se, no prazo determinado pela Justiça Eleitoral, contado a partir da notificação de decisão sobre a existência de propaganda irregular, não tomar providências para a cessação dessa divulgação. (Incluído pela Lei nº 12.034, de 2009)

Parágrafo único. O provedor de conteúdo ou de serviços multimídia só será considerado responsável pela divulgação da propaganda se a publicação do material for comprovadamente de seu prévio conhecimento. (Incluído pela Lei nº 12.034, de 2009)

Art. 57-G. As mensagens eletrônicas enviadas por candidato, partido ou coligação, por qualquer meio, deverão dispor de mecanismo que permita seu descadastramento pelo destinatário, obrigado o remetente a providenciá-lo no prazo de quarenta e oito horas. (Incluído pela Lei nº 12.034, de 2009)

Parágrafo único. Mensagens eletrônicas enviadas após o término do prazo previsto no caput sujeitam os responsáveis ao pagamento de multa no valor de R$ 100,00 (cem reais), por mensagem. (Incluído pela Lei nº 12.034, de 2009)

Art. 57-H. Sem prejuízo das demais sanções legais cabíveis, será punido, com multa de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais), quem realizar propaganda eleitoral na internet, atribuindo indevidamente sua autoria a terceiro, inclusive a candidato, partido ou coligação. (Incluído pela Lei nº 12.034, de 2009)

§ 1º Constitui crime a contratação direta ou indireta de grupo de pessoas com a finalidade específica de emitir mensagens ou comentários na internet para ofender a honra ou denegrir a imagem de candidato, partido ou coligação, punível com detenção de 2 (dois) a 4 (quatro) anos e multa de R$ 15.000,00 (quinze mil reais) a R$ 50.000,00 (cinquenta mil reais). (Incluído pela Lei nº 12.891, de 2013)

§ 2º Igualmente incorrem em crime, punível com detenção de 6 (seis) meses a 1 (um) ano, com alternativa de prestação de serviços à comunidade pelo mesmo período, e multa de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais), as pessoas contratadas na forma do § 1º. (Incluído pela Lei nº 12.891, de 2013)

Art. 57-I. A requerimento de candidato, partido ou coligação, observado o rito previsto no art. 96 desta Lei, a Justiça Eleitoral poderá determinar, no âmbito e nos limites técnicos de cada aplicação de internet, a suspensão do acesso a todo conteúdo veiculado que deixar de cumprir as disposições desta Lei, devendo o número de horas de suspensão ser definida proporcionalmente à gravidade da infração cometida em cada caso, observado o limite máximo de vinte e quatro horas. (Redação dada pela Lei nº 13.488, de 2017)

§ 1º A cada reiteração de conduta, será duplicado o período de suspensão. (Incluído pela Lei nº 12.034, de 2009)

§ 2º No período de suspensão a que se refere este artigo, a empresa informará, a todos os usuários que tentarem acessar seus serviços, que se encontra temporariamente inoperante por desobediência à legislação eleitoral. (Incluído pela Lei nº 12.034, de 2009)

Art. 57-J. O Tribunal Superior Eleitoral regulamentará o disposto nos arts. 57-A a 57-I desta Lei de acordo com o cenário e as ferramentas tecnológicas existentes em cada momento eleitoral e promoverá, para os veículos, partidos e demais entidades interessadas, a formulação e a ampla divulgação de regras de boas práticas relativas a campanhas eleitorais na internet. (Incluído pela Lei nº 13.488, de 2017)

Do Direito de Resposta

Art. 58. A partir da escolha de candidatos em convenção, é assegurado o direito de resposta a candidato, partido ou coligação atingidos, ainda que de forma indireta, por conceito, imagem ou afirmação caluniosa, difamatória, injuriosa ou sabidamente inverídica, difundidos por qualquer veículo de comunicação social.

§ 1º O ofendido, ou seu representante legal, poderá pedir o exercício do direito de resposta à Justiça Eleitoral nos seguintes prazos, contados a partir da veiculação da ofensa:

I - vinte e quatro horas, quando se tratar do horário eleitoral gratuito;

II - quarenta e oito horas, quando se tratar da programação normal das emissoras de rádio e televisão;

III - setenta e duas horas, quando se tratar de órgão da imprensa escrita.

IV - a qualquer tempo, quando se tratar de conteúdo que esteja sendo divulgado na internet, ou em 72 (setenta e duas) horas, após a sua retirada. (Incluído pela Lei nº 13.165, de 2015)

§ 2º Recebido o pedido, a Justiça Eleitoral notificará imediatamente o ofensor para que se defenda em vinte e quatro horas, devendo a decisão ser prolatada no prazo máximo de setenta e duas horas da data da formulação do pedido.

§ 3º Observar-se-ão, ainda, as seguintes regras no caso de pedido de resposta relativo a ofensa veiculada:

I - em órgão da imprensa escrita:

a) o pedido deverá ser instruído com um exemplar da publicação e o texto para resposta;

b) deferido o pedido, a divulgação da resposta dar-se-á no mesmo veículo, espaço, local, página, tamanho, caracteres e outros elementos de realce usados na ofensa, em até quarenta e oito horas após a decisão ou, tratando-se de veículo com periodicidade de circulação maior que quarenta e oito horas, na primeira vez em que circular;

c) por solicitação do ofendido, a divulgação da resposta será feita no mesmo dia da semana em que a ofensa foi divulgada, ainda que fora do prazo de quarenta e oito horas;

d) se a ofensa for produzida em dia e hora que inviabilizem sua reparação dentro dos prazos estabelecidos nas alíneas anteriores, a Justiça Eleitoral determinará a imediata divulgação da resposta;

e) o ofensor deverá comprovar nos autos o cumprimento da decisão, mediante dados sobre a regular distribuição dos exemplares, a quantidade impressa e o raio de abrangência na distribuição;

II - em programação normal das emissoras de rádio e de televisão:

a) a Justiça Eleitoral, à vista do pedido, deverá notificar imediatamente o responsável pela emissora que realizou o programa para que entregue em vinte e quatro horas, sob as penas do art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral, cópia da fita da transmissão, que será devolvida após a decisão;

b) o responsável pela emissora, ao ser notificado pela Justiça Eleitoral ou informado pelo reclamante ou representante, por cópia protocolada do pedido de resposta, preservará a gravação até a decisão final do processo;

c) deferido o pedido, a resposta será dada em até quarenta e oito horas após a decisão, em tempo igual ao da ofensa, porém nunca inferior a um minuto;

III - no horário eleitoral gratuito:

a) o ofendido usará, para a resposta, tempo igual ao da ofensa, nunca inferior, porém, a um minuto;

b) a resposta será veiculada no horário destinado ao partido ou coligação responsável pela ofensa, devendo necessariamente dirigir-se aos fatos nela veiculados;

c) se o tempo reservado ao partido ou coligação responsável pela ofensa for inferior a um minuto, a resposta será levada ao ar tantas vezes quantas sejam necessárias para a sua complementação;

d) deferido o pedido para resposta, a emissora geradora e o partido ou coligação atingidos deverão ser notificados imediatamente da decisão, na qual deverão estar indicados quais os períodos, diurno ou noturno, para a veiculação da resposta, que deverá ter lugar no início do programa do partido ou coligação;

e) o meio magnético com a resposta deverá ser entregue à emissora geradora, até trinta e seis horas após a ciência da decisão, para veiculação no programa subseqüente do partido ou coligação em cujo horário se praticou a ofensa;

f) se o ofendido for candidato, partido ou coligação que tenha usado o tempo concedido sem responder aos fatos veiculados na ofensa, terá subtraído tempo idêntico do respectivo programa eleitoral; tratando-se de terceiros, ficarão sujeitos à suspensão de igual tempo em eventuais novos pedidos de resposta e à multa no valor de duas mil a cinco mil UFIR.

IV - em propaganda eleitoral na internet: (Incluído pela Lei nº 12.034, de 2009)

a) deferido o pedido, o usuário ofensor deverá divulgar a resposta do ofendido em até quarenta e oito horas após sua entrega em mídia física, e deverá empregar nessa divulgação o mesmo impulsionamento de conteúdo eventualmente contratado nos termos referidos no art. 57-C desta Lei e o mesmo veículo, espaço, local, horário, página eletrônica, tamanho, caracteres e outros elementos de realce usados na ofensa; (Redação dada pela Lei nº 13.488, de 2017)

b) a resposta ficará disponível para acesso pelos usuários do serviço de internet por tempo não inferior ao dobro em que esteve disponível a mensagem considerada ofensiva; (Incluído pela Lei nº 12.034, de 2009)

c) os custos de veiculação da resposta correrão por conta do responsável pela propaganda original. (Incluído pela Lei nº 12.034, de 2009)

§ 4º Se a ofensa ocorrer em dia e hora que inviabilizem sua reparação dentro dos prazos estabelecidos nos parágrafos anteriores, a resposta será divulgada nos horários que a Justiça Eleitoral determinar, ainda que nas quarenta e oito horas anteriores ao pleito, em termos e forma previamente aprovados, de modo a não ensejar tréplica.

§ 5º Da decisão sobre o exercício do direito de resposta cabe recurso às instâncias superiores, em vinte e quatro horas da data de sua publicação em cartório ou sessão, assegurado ao recorrido oferecer contra-razões em igual prazo, a contar da sua notificação.

§ 6º A Justiça Eleitoral deve proferir suas decisões no prazo máximo de vinte e quatro horas, observando-se o disposto nas alíneas *d* e *e* do inciso III do § 3º para a restituição do tempo em caso de provimento de recurso.

§ 7º A inobservância do prazo previsto no parágrafo anterior sujeita a autoridade judiciária às penas previstas no art. 345 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

§ 8º O não-cumprimento integral ou em parte da decisão que conceder a resposta sujeitará o infrator ao pagamento de multa no valor de cinco mil a quinze mil UFIR, duplicada em caso de reiteração de conduta, sem prejuízo do disposto no art. 347 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

§ 9º Caso a decisão de que trata o § 2º não seja prolatada em 72 (setenta e duas) horas da data da formulação do pedido, a Justiça Eleitoral, de ofício, providenciará a alocação de Juiz auxiliar. (Incluído pela Lei nº 12.891, de 2013)

Art. 58-A. Os pedidos de direito de resposta e as representações por propaganda eleitoral irregular em rádio, televisão e internet tramitarão preferencialmente em relação aos demais processos em curso na Justiça Eleitoral. (Incluído pela Lei nº 12.034, de 2009)

Do Sistema Eletrônico de Votação e da Totalização dos Votos

Art. 59. A votação e a totalização dos votos serão feitas por sistema eletrônico, podendo o Tribunal Superior Eleitoral autorizar, em caráter excepcional, a aplicação das regras fixadas nos arts. 83 a 89.

§ 1º A votação eletrônica será feita no número do candidato ou da legenda partidária, devendo o nome e fotografia do candidato e o nome do partido ou a legenda partidária aparecer no painel da urna eletrônica, com a expressão designadora do cargo disputado no masculino ou feminino, conforme o caso.

§ 2º Na votação para as eleições proporcionais, serão computados para a legenda partidária os votos em que não seja possível a identificação do candidato, desde que o número identificador do partido seja digitado de forma correta.

§ 3º A urna eletrônica exibirá para o eleitor os painéis na seguinte ordem: (Redação dada pela Lei nº 12.976, de 2014)

I - para as eleições de que trata o inciso I do parágrafo único do art. 1º, Deputado Federal, Deputado Estadual ou Distrital, Senador, Governador e Vice-Governador de Estado ou do Distrito Federal, Presidente e Vice-Presidente da República; (Incluído pela Lei nº 12.976, de 2014)

II - para as eleições de que trata o inciso II do parágrafo único do art. 1º, Vereador, Prefeito e Vice-Prefeito. (Incluído pela Lei nº 12.976, de 2014)

§ 4º A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor. (Redação dada pela Lei nº 10.740, de 2003)

§ 5º Caberá à Justiça Eleitoral definir a chave de segurança e a identificação da urna eletrônica de que trata o § 4º. (Redação dada pela Lei nº 10.740, de 2003)

§ 6º Ao final da eleição, a urna eletrônica procederá à assinatura digital do arquivo de votos, com aplicação do registro de horário e do arquivo do boletim de urna, de maneira a impedir a substituição de votos e a alteração dos registros dos termos de início e término da votação. (Redação dada pela Lei nº 10.740, de 2003)

§ 7º O Tribunal Superior Eleitoral colocará à disposição dos eleitores urnas eletrônicas destinadas a treinamento. (Redação dada pela Lei nº 10.740, de 2003)

Art. 59-A. (Declarado inconstitucional pela ADI Nº 5.889)

Parágrafo único. (Declarado inconstitucional pela ADI Nº 5.889)

Art. 60. No sistema eletrônico de votação considerar-se-á voto de legenda quando o eleitor assinalar o número do partido no momento de votar para determinado cargo e somente para este será computado.

Art 61. A urna eletrônica contabilizará cada voto, assegurando-lhe o sigilo e inviolabilidade, garantida aos partidos políticos, coligações e candidatos ampla fiscalização.

Art. 61A. (Revogada pela Lei nº 10.740, de 2003)

Art. 62. Nas Seções em que for adotada a urna eletrônica, somente poderão votar eleitores cujos nomes estiverem nas respectivas folhas de votação, não se aplicando a ressalva a que se refere o art. 148, § 1º Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Parágrafo único. O Tribunal Superior Eleitoral disciplinará a hipótese de falha na urna eletrônica que prejudique o regular processo de votação.

Das Mesas Receptoras

Art. 63. Qualquer partido pode reclamar ao Juiz Eleitoral, no prazo de cinco dias, da nomeação da Mesa Receptora, devendo a decisão ser proferida em 48 horas.

§ 1º Da decisão do Juiz Eleitoral caberá recurso para o Tribunal Regional, interposto dentro de três dias, devendo ser resolvido em igual prazo.

§ 2º Não podem ser nomeados presidentes e mesários os menores de dezoito anos.

Art. 64. É vedada a participação de parentes em qualquer grau ou de servidores da mesma repartição pública ou empresa privada na mesma Mesa, Turma ou Junta Eleitoral.

Da Fiscalização das Eleições

Art. 65. A escolha de fiscais e delegados, pelos partidos ou coligações, não poderá recair em menor de dezoito anos ou em quem, por nomeação do Juiz Eleitoral, já faça parte de Mesa Receptora.

§ 1º O fiscal poderá ser nomeado para fiscalizar mais de uma Seção Eleitoral, no mesmo local de votação.

§ 2º As credenciais de fiscais e delegados serão expedidas, exclusivamente, pelos partidos ou coligações.

§ 3º Para efeito do disposto no parágrafo anterior, o presidente do partido ou o representante da coligação deverá registrar na Justiça Eleitoral o nome das pessoas autorizadas a expedir as credenciais dos fiscais e delegados.

§ 4º Para o acompanhamento dos trabalhos de votação, só será permitido o credenciamento de, no máximo, 2 (dois) fiscais de cada partido ou coligação por seção eleitoral. (Incluído pela Lei nº 12.891, de 2013)

Art. 66. Os partidos e coligações poderão fiscalizar todas as fases do processo de votação e apuração das eleições e o processamento eletrônico da totalização dos resultados. (Redação dada pela Lei nº 10.408, de 2002)

§ 1º Todos os programas de computador de propriedade do Tribunal Superior Eleitoral, desenvolvidos por ele ou sob sua encomenda, utilizados nas urnas eletrônicas para os processos de votação, apuração e totalização, poderão ter suas fases de especificação e de desenvolvimento acompanhadas por técnicos indicados pelos partidos políticos, Ordem dos Advogados do Brasil e Ministério Público, até seis meses antes das eleições. (Redação dada pela Lei nº 10.740, de 2003)

§ 2º Uma vez concluídos os programas a que se refere o § 1º, serão eles apresentados, para análise, aos representantes credenciados dos partidos políticos e coligações, até vinte dias antes das eleições, nas dependências do Tribunal Superior Eleitoral, na forma de programas-fonte e de programas executáveis, inclusive os sistemas aplicativo e de segurança e as bibliotecas especiais, sendo que as chaves eletrônicas privadas e senhas eletrônicas de acesso manter-se-ão no sigilo da Justiça Eleitoral. Após a apresentação e conferência, serão lacradas cópias dos programas-fonte e dos programas compilados. (Redação dada pela Lei nº 10.740, de 2003)

§ 3º No prazo de cinco dias a contar da data da apresentação referida no § 2º, o partido político e a coligação poderão apresentar impugnação fundamentada à Justiça Eleitoral. (Redação dada pela Lei nº 10.740, de 2003)

§ 4º Havendo a necessidade de qualquer alteração nos programas, após a apresentação de que trata o § 3º, dar-se-á conhecimento do fato aos representantes dos partidos políticos e das coligações, para que sejam novamente analisados e lacrados. (Redação dada pela Lei nº 10.740, de 2003)

§ 5º A carga ou preparação das urnas eletrônicas será feita em sessão pública, com prévia convocação dos fiscais dos partidos e coligações para a assistirem e procederem aos atos de fiscalização, inclusive para verificarem se os programas carregados nas urnas são idênticos aos que foram lacrados na sessão referida no § 2º deste artigo, após o que as urnas serão lacradas. (Incluído pela Lei nº 10.408, de 2002)

§ 6º No dia da eleição, será realizada, por amostragem, auditoria de verificação do funcionamento das urnas eletrônicas, através de votação paralela, na presença dos fiscais dos partidos e coligações, nos moldes fixados em resolução do Tribunal Superior Eleitoral. (Incluído pela Lei nº 10.408, de 2002)

§ 7º Os partidos concorrentes ao pleito poderão constituir sistema próprio de fiscalização, apuração e totalização dos resultados contratando, inclusive, empresas de auditoria de sistemas, que, credenciadas junto à Justiça Eleitoral, receberão, previamente, os programas de computador e os mesmos dados alimentadores do sistema oficial de apuração e totalização. (Incluído pela Lei nº 10.408, de 2002)

Art. 67. Os órgãos encarregados do processamento eletrônico de dados são obrigados a fornecer aos partidos ou coligações, no momento da entrega ao Juiz Encarregado, cópias dos dados do processamento parcial de cada dia, contidos em meio magnético.

Art. 68. O boletim de urna, segundo modelo aprovado pelo Tribunal Superior Eleitoral, conterá os nomes e os números dos candidatos nela votados.

§ 1º O Presidente da Mesa Receptora é obrigado a entregar cópia do boletim de urna aos partidos e coligações concorrentes ao pleito cujos representantes o requeiram até uma hora após a expedição.

§ 2º O descumprimento do disposto no parágrafo anterior constitui crime, punível com detenção, de um a três meses, com a alternativa de prestação de serviço à comunidade pelo mesmo período, e multa no valor de um mil a cinco mil UFIR.

Art. 69. A impugnação não recebida pela Junta Eleitoral pode ser apresentada diretamente ao Tribunal Regional Eleitoral, em quarenta e oito horas, acompanhada de declaração de duas testemunhas.

Parágrafo único. O Tribunal decidirá sobre o recebimento em quarenta e oito horas, publicando o acórdão na própria sessão de julgamento e transmitindo imediatamente à Junta, via telex, fax ou qualquer outro meio eletrônico, o inteiro teor da decisão e da impugnação.

Art. 70. O Presidente de Junta Eleitoral que deixar de receber ou de mencionar em ata os protestos recebidos, ou ainda, impedir o exercício de fiscalização, pelos partidos ou coligações, deverá ser imediatamente afastado, além de responder pelos crimes previstos na Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

Art. 71. Cumpre aos partidos e coligações, por seus fiscais e delegados devidamente credenciados, e aos candidatos, proceder à instrução dos recursos interpostos contra a apuração, juntando, para tanto, cópia do boletim relativo à urna impugnada.

Parágrafo único. Na hipótese de surgirem obstáculos à obtenção do boletim, caberá ao recorrente requerer, mediante a indicação dos dados necessários, que o órgão da Justiça Eleitoral perante o qual foi interposto o recurso o instrua, anexando o respectivo boletim de urna.

Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:

I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;

II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;

III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Das Condutas Vedadas aos Agentes Públicos em Campanhas Eleitorais

Art. 73. São proibidas aos agentes públicos, servidores ou não, as seguintes condutas tendentes a afetar a igualdade de oportunidades entre candidatos nos pleitos eleitorais:

I - ceder ou usar, em benefício de candidato, partido político ou coligação, bens móveis ou imóveis pertencentes à administração direta ou indireta da União, dos Estados, do Distrito Federal, dos Territórios e dos Municípios, ressalvada a realização de convenção partidária;

II - usar materiais ou serviços, custeados pelos Governos ou Casas Legislativas, que excedam as prerrogativas consignadas nos regimentos e normas dos órgãos que integram;

III - ceder servidor público ou empregado da administração direta ou indireta federal, estadual ou municipal do Poder Executivo, ou usar de seus serviços, para comitês de campanha eleitoral de candidato, partido político ou coligação, durante o horário de expediente normal, salvo se o servidor ou empregado estiver licenciado;

IV - fazer ou permitir uso promocional em favor de candidato, partido político ou coligação, de distribuição gratuita de bens e serviços de caráter social custeados ou subvencionados pelo Poder Público;

V - nomear, contratar ou de qualquer forma admitir, demitir sem justa causa, suprimir ou readaptar vantagens ou por outros meios dificultar ou impedir o exercício funcional e, ainda, *ex officio*, remover, transferir ou exonerar servidor público, na circunscrição do pleito, nos três meses que o antecedem e até a posse dos eleitos, sob pena de nulidade de pleno direito, ressalvados:

a) a nomeação ou exoneração de cargos em comissão e designação ou dispensa de funções de confiança;

b) a nomeação para cargos do Poder Judiciário, do Ministério Público, dos Tribunais ou Conselhos de Contas e dos órgãos da Presidência da República;

c) a nomeação dos aprovados em concursos públicos homologados até o início daquele prazo;

d) a nomeação ou contratação necessária à instalação ou ao funcionamento inadiável de serviços públicos essenciais, com prévia e expressa autorização do Chefe do Poder Executivo;

e) a transferência ou remoção *ex officio* de militares, policiais civis e de agentes penitenciários;

VI - nos três meses que antecedem o pleito:

a) realizar transferência voluntária de recursos da União aos Estados e Municípios, e dos Estados aos Municípios, sob pena de nulidade de pleno direito, ressalvados os recursos destinados a cumprir obrigação formal preexistente para execução de obra ou serviço em andamento e com cronograma prefixado, e os destinados a atender situações de emergência e de calamidade pública;

b) com exceção da propaganda de produtos e serviços que tenham concorrência no mercado, autorizar publicidade institucional dos atos, programas, obras, serviços e campanhas dos órgãos públicos federais, estaduais ou municipais, ou das respectivas entidades da administração indireta, salvo em caso de grave e urgente necessidade pública, assim reconhecida pela Justiça Eleitoral;

c) fazer pronunciamento em cadeia de rádio e televisão, fora do horário eleitoral gratuito, salvo quando, a critério da Justiça Eleitoral, tratar-se de matéria urgente, relevante e característica das funções de governo;

VII - empenhar, no primeiro semestre do ano de eleição, despesas com publicidade dos órgãos públicos federais, estaduais ou municipais, ou das respectivas entidades da administração indireta, que excedam a 6 (seis) vezes a média mensal dos valores empenhados e não cancelados nos 3 (três) últimos anos que antecedem o pleito; (Redação dada pela Lei nº 14.356, de 2022) (Vide ADI 7178) (Vide ADI 7182)

VIII - fazer, na circunscrição do pleito, revisão geral da remuneração dos servidores públicos que exceda a recomposição da perda de seu poder aquisitivo ao longo do ano da eleição, a partir do início do prazo estabelecido no art. 7º desta Lei e até a posse dos eleitos.

§ 1º Reputa-se agente público, para os efeitos deste artigo, quem exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos ou entidades da administração pública direta, indireta, ou fundacional.

§ 2º A vedação do inciso I do *caput* não se aplica ao uso, em campanha, de transporte oficial pelo Presidente da República, obedecido o disposto no art. 76, nem ao uso, em campanha, pelos candidatos a reeleição de Presidente e Vice-Presidente da República, Governador e Vice-Governador de Estado e do Distrito Federal, Prefeito e Vice-Prefeito, de suas residências oficiais para realização de contatos, encontros e reuniões pertinentes à própria campanha, desde que não tenham caráter de ato público.

§ 3º As vedações do inciso VI do *caput*, alíneas b e c, aplicam-se apenas aos agentes públicos das esferas administrativas cujos cargos estejam em disputa na eleição.

§ 4º O descumprimento do disposto neste artigo acarretará a suspensão imediata da conduta vedada, quando for o caso, e sujeitará os responsáveis a multa no valor de cinco a cem mil UFIR.

§ 5º Nos casos de descumprimento do disposto nos incisos do caput e no § 10, sem prejuízo do disposto no § 4º, o candidato beneficiado, agente público ou não, ficará sujeito à cassação do registro ou do diploma. (Redação dada pela Lei nº 12.034, de 2009)

§ 6º As multas de que trata este artigo serão duplicadas a cada reincidência.

§ 7º As condutas enumeradas no *caput* caracterizam, ainda, atos de improbidade administrativa, a que se refere o art. 11, inciso I, da Lei nº 8.429, de 2 de junho de 1992, e sujeitam-se às disposições daquele diploma legal, em especial às cominações do art. 12, inciso III.

§ 8º Aplicam-se as sanções do § 4º aos agentes públicos responsáveis pelas condutas vedadas e aos partidos, coligações e candidatos que delas se beneficiarem.

§ 9º Na distribuição dos recursos do Fundo Partidário (Lei nº 9.096, de 19 de setembro de 1995) oriundos da aplicação do disposto no § 4º, deverão ser excluídos os partidos beneficiados pelos atos que originaram as multas.

§ 10. No ano em que se realizar eleição, fica proibida a distribuição gratuita de bens, valores ou benefícios por parte da Administração Pública, exceto nos casos de calamidade pública, de estado de emergência ou de programas sociais autorizados em lei e já em execução orçamentária no exercício anterior, casos em que o Ministério Público poderá promover o acompanhamento de sua execução financeira e administrativa. (Incluído pela Lei nº 11.300, de 2006)

§ 11. Nos anos eleitorais, os programas sociais de que trata o § 10 não poderão ser executados por entidade nominalmente vinculada a candidato ou por esse mantida. (Incluído pela Lei nº 12.034, de 2009)

§ 12. A representação contra a não observância do disposto neste artigo observará o rito do art. 22 da Lei Complementar nº 64, de 18 de maio de 1990, e poderá ser ajuizada até a data da diplomação. (Incluído pela Lei nº 12.034, de 2009)

§ 13. O prazo de recurso contra decisões proferidas com base neste artigo será de 3 (três) dias, a contar da data da publicação do julgamento no Diário Oficial. (Incluído pela Lei nº 12.034, de 2009)

§ 14. Para efeito de cálculo da média prevista no inciso VII do **caput** deste artigo, os gastos serão reajustados pelo IPCA, aferido pela Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), ou outro índice que venha a substituí-lo, a partir da data em que foram empenhados. (Incluído pela Lei nº 14.356, de 2022)

Art. 74. Configura abuso de autoridade, para os fins do disposto no art. 22 da Lei Complementar nº 64, de 18 de maio de 1990, a infringência do disposto no § 1º do art. 37 da Constituição Federal, ficando o responsável, se candidato, sujeito ao cancelamento do registro ou do diploma. (Redação dada pela Lei nº 12.034, de 2009)

Art. 75. Nos três meses que antecederem as eleições, na realização de inaugurações é vedada a contratação de shows artísticos pagos com recursos públicos.

Parágrafo único. Nos casos de descumprimento do disposto neste artigo, sem prejuízo da suspensão imediata da conduta, o candidato beneficiado, agente público ou não, ficará sujeito à cassação do registro ou do diploma. (Incluído pela Lei nº 12.034, de 2009)

Art. 76. O ressarcimento das despesas com o uso de transporte oficial pelo Presidente da República e sua comitiva em campanha eleitoral será de responsabilidade do partido político ou coligação a que esteja vinculado.

§ 1º O ressarcimento de que trata este artigo terá por base o tipo de transporte usado e a respectiva tarifa de mercado cobrada no trecho correspondente, ressalvado o uso do avião presidencial, cujo ressarcimento corresponderá ao aluguel de uma aeronave de propulsão a jato do tipo táxi aéreo.

§ 2º No prazo de dez dias úteis da realização do pleito, em primeiro turno, ou segundo, se houver, o órgão competente de controle interno procederá *ex officio* à cobrança dos valores devidos nos termos dos parágrafos anteriores.

§ 3º A falta do ressarcimento, no prazo estipulado, implicará a comunicação do fato ao Ministério Público Eleitoral, pelo órgão de controle interno.

§ 4º Recebida a denúncia do Ministério Público, a Justiça Eleitoral apreciará o feito no prazo de trinta dias, aplicando aos infratores pena de multa correspondente ao dobro das despesas, duplicada a cada reiteração de conduta.

Art. 77. É proibido a qualquer candidato comparecer, nos 3 (três) meses que precedem o pleito, a inaugurações de obras públicas. (Redação dada pela Lei nº 12.034, de 2009)

Parágrafo único. A inobservância do disposto neste artigo sujeita o infrator à cassação do registro ou do diploma. (Redação dada pela Lei nº 12.034, de 2009)

Art. 78. A aplicação das sanções cominadas no art. 73, §§ 4º e 5º, dar-se-á sem prejuízo de outras de caráter constitucional, administrativo ou disciplinar fixadas pelas demais leis vigentes.

Disposições Transitórias

Art. 79. O financiamento das campanhas eleitorais com recursos públicos será disciplinada em lei específica.

Art. 80. Nas eleições a serem realizadas no ano de 1998, cada partido ou coligação deverá reservar, para candidatos de cada sexo, no mínimo, vinte e cinco por cento e, no máximo, setenta e cinco por cento do número de candidaturas que puder registrar.

Art. 81. (Revogado pela Lei nº 13.165, de 2015)

Art. 82. Nas Seções Eleitorais em que não for usado o sistema eletrônico de votação e totalização de votos, serão aplicadas as regras definidas nos arts. 83 a 89 desta Lei e as pertinentes da Lei 4.737, de 15 de julho de 1965 - Código Eleitoral.

Art. 83. As cédulas oficiais serão confeccionadas pela Justiça Eleitoral, que as imprimirá com exclusividade para distribuição às Mesas Receptoras, sendo sua impressão feita em papel opaco, com tinta preta e em tipos uniformes de letras e números, identificando o gênero na denominação dos cargos em disputa.

§ 1º Haverá duas cédulas distintas, uma para as eleições majoritárias e outra para as proporcionais, a serem confeccionadas segundo modelos determinados pela Justiça Eleitoral.

§ 2º Os candidatos à eleição majoritária serão identificados pelo nome indicado no pedido de registro e pela sigla adotada pelo partido a que pertencem e deverão figurar na ordem determinada por sorteio.

§ 3º Para as eleições realizadas pelo sistema proporcional, a cédula terá espaços para que o eleitor escreva o nome ou o número do candidato escolhido, ou a sigla ou o número do partido de sua preferência.

§ 4º No prazo de quinze dias após a realização do sorteio a que se refere o § 2º, os Tribunais Regionais Eleitorais divulgarão o modelo da cédula completa com os nomes dos candidatos majoritários na ordem já definida.

§ 5° Às eleições em segundo turno aplica-se o disposto no § 2º, devendo o sorteio verificar-se até quarenta e oito horas após a proclamação do resultado do primeiro turno e a divulgação do modelo da cédula nas vinte e quatro horas seguintes.

Art. 84. No momento da votação, o eleitor dirigir-se-á à cabina duas vezes, sendo a primeira para o preenchimento da cédula destinada às eleições proporcionais, de cor branca, e a segunda para o preenchimento da cédula destinada às eleições majoritárias, de cor amarela.

Parágrafo único. A Justiça Eleitoral fixará o tempo de votação e o número de eleitores por seção, para garantir o pleno exercício do direito de voto.

Art. 85. Em caso de dúvida na apuração de votos dados a homônimos, prevalecerá o número sobre o nome do candidato.

Art. 86. No sistema de votação convencional considerar-se-á voto de legenda quando o eleitor assinalar o número do partido no local exato reservado para o cargo respectivo e somente para este será computado.

Art. 87. Na apuração, será garantido aos fiscais e delegados dos partidos e coligações o direito de observar diretamente, a distância não superior a um metro da mesa, a abertura da urna, a abertura e a contagem das cédulas e o preenchimento do boletim .

§ 1º O não-atendimento ao disposto no *caput* enseja a impugnação do resultado da urna, desde que apresentada antes da divulgação do boletim.

§ 2º Ao final da transcrição dos resultados apurados no boletim, o Presidente da Junta Eleitoral é obrigado a entregar cópia deste aos partidos e coligações concorrentes ao pleito cujos representantes o requeiram até uma hora após sua expedição.

§ 3º Para os fins do disposto no parágrafo anterior, cada partido ou coligação poderá credenciar até três fiscais perante a Junta Eleitoral, funcionando um de cada vez.

§ 4º O descumprimento de qualquer das disposições deste artigo constitui crime, punível com detenção de um a três meses, com a alternativa de prestação de serviços à comunidade pelo mesmo período e multa, no valor de um mil a cinco mil UFIR.

§ 5º O rascunho ou qualquer outro tipo de anotação fora dos boletins de urna, usados no momento da apuração dos votos, não poderão servir de prova posterior perante a Junta apuradora ou totalizadora.

§ 6º O boletim mencionado no § 2º deverá conter o nome e o número dos candidatos nas primeiras colunas, que precederão aquelas onde serão designados os votos e o partido ou coligação.

Art. 88. O Juiz Presidente da Junta Eleitoral é obrigado a recontar a urna, quando:

I - o boletim apresentar resultado não-coincidente com o número de votantes ou discrepante dos dados obtidos no momento da apuração;

II - ficar evidenciada a atribuição de votos a candidatos inexistentes, o não-fechamento da contabilidade da urna ou a apresentação de totais de votos nulos, brancos ou válidos destoantes da média geral das demais Seções do mesmo Município, Zona Eleitoral.

Art. 89. Será permitido o uso de instrumentos que auxiliem o eleitor analfabeto a votar, não sendo a Justiça Eleitoral obrigada a fornecê-los.

Disposições Finais

Art. 90. Aos crimes definidos nesta Lei, aplica-se o disposto nos arts. 287 e 355 a 364 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral.

§ 1º Para os efeitos desta Lei, respondem penalmente pelos partidos e coligações os seus representantes legais.

§ 2º Nos casos de reincidência, as penas pecuniárias previstas nesta Lei aplicam-se em dobro.

Art. 90-A. (VETADO) (Incluído pela Lei nº 11.300, de 2006)

Art. 91. Nenhum requerimento de inscrição eleitoral ou de transferência será recebido dentro dos cento e cinqüenta dias anteriores à data da eleição.

Parágrafo único. A retenção de título eleitoral ou do comprovante de alistamento eleitoral constitui crime, punível com detenção, de um a três meses, com a alternativa de prestação de serviços à comunidade por igual período, e multa no valor de cinco mil a dez mil UFIR.

Art. 91-A. No momento da votação, além da exibição do respectivo título, o eleitor deverá apresentar documento de identificação com fotografia. (Incluído pela Lei nº 12.034, de 2009) (Vide ADIN 4467)

Parágrafo único. Fica vedado portar aparelho de telefonia celular, máquinas fotográficas e filmadoras, dentro da cabina de votação. (Incluído pela Lei nº 12.034, de 2009)

Art. 92. O Tribunal Superior Eleitoral, ao conduzir o processamento dos títulos eleitorais, determinará de ofício a revisão ou correição das Zonas Eleitorais sempre que:

I - o total de transferências de eleitores ocorridas no ano em curso seja dez por cento superior ao do ano anterior;

II - o eleitorado for superior ao dobro da população entre dez e quinze anos, somada à de idade superior a setenta anos do território daquele Município;

III - o eleitorado for superior a sessenta e cinco por cento da população projetada para aquele ano pelo Instituto Brasileiro de Geografia e Estatística - IBGE.

Art. 93. O Tribunal Superior Eleitoral poderá, nos anos eleitorais, requisitar das emissoras de rádio e televisão, no período de um mês antes do início da propaganda eleitoral a que se refere o art. 36 e nos três dias anteriores à data do pleito, até dez minutos diários, contínuos ou não, que poderão ser somados e usados em dias espaçados, para a divulgação de comunicados, boletins e instruções ao eleitorado. (Redação dada pela Lei nº 13.165, de 2015)

Art. 93-A. O Tribunal Superior Eleitoral, no período compreendido entre 1º de abril e 30 de julho dos anos eleitorais, promoverá, em até cinco minutos diários, contínuos ou não, requisitados às emissoras de rádio e televisão, propaganda institucional, em rádio e televisão, destinada a incentivar a participação feminina, dos jovens e da comunidade negra na política, bem como a esclarecer os cidadãos sobre as regras e o funcionamento do sistema eleitoral brasileiro. (Redação dada pela Lei nº 13.488, de 2017)

Art. 94. Os feitos eleitorais, no período entre o registro das candidaturas até cinco dias após a realização do segundo turno das eleições, terão prioridade para a participação do Ministério Público e dos Juízes de todas as Justiças e instâncias, ressalvados os processos de *habeas corpus* e mandado de segurança.

§ 1º É defeso às autoridades mencionadas neste artigo deixar de cumprir qualquer prazo desta Lei, em razão do exercício das funções regulares.

§ 2º O descumprimento do disposto neste artigo constitui crime de responsabilidade e será objeto de anotação funcional para efeito de promoção na carreira.

§ 3º Além das polícias judiciárias, os órgãos da receita federal, estadual e municipal, os tribunais e órgãos de contas auxiliarão a Justiça Eleitoral na apuração dos delitos eleitorais, com prioridade sobre suas atribuições regulares.

§ 4º Os advogados dos candidatos ou dos partidos e coligações serão notificados para os feitos de que trata esta Lei com antecedência mínima de vinte e quatro horas, ainda que por fax, telex ou telegrama.

§ 5º Nos Tribunais Eleitorais, os advogados dos candidatos ou dos partidos e coligações serão intimados para os feitos que não versem sobre a cassação do registro ou do diploma de que trata esta Lei por meio da publicação de edital eletrônico publicado na página do respectivo Tribunal na internet, iniciando-se a contagem do prazo no dia seguinte ao da divulgação. (Incluído pela Lei nº 13.165, de 2015)

Art. 94-A. Os órgãos e entidades da Administração Pública direta e indireta poderão, quando solicitados, em casos específicos e de forma motivada, pelos Tribunais Eleitorais: (Incluído pela Lei nº 11.300, de 2006)

I - fornecer informações na área de sua competência; (Incluído pela Lei nº 11.300, de 2006)

II - ceder funcionários no período de 3 (três) meses antes a 3 (três) meses depois de cada eleição. (Incluído pela Lei nº 11.300, de 2006)

Art. 94-B. (VETADO) (Incluído pela Lei nº 11.300, de 2006)

Art. 95. Ao Juiz Eleitoral que seja parte em ações judiciais que envolvam determinado candidato é defeso exercer suas funções em processo eleitoral no qual o mesmo candidato seja interessado.

Art. 96. Salvo disposições específicas em contrário desta Lei, as reclamações ou representações relativas ao seu descumprimento podem ser feitas por qualquer partido político, coligação ou candidato, e devem dirigir-se:

I - aos Juízes Eleitorais, nas eleições municipais;

II - aos Tribunais Regionais Eleitorais, nas eleições federais, estaduais e distritais;

III - ao Tribunal Superior Eleitoral, na eleição presidencial.

§ 1º As reclamações e representações devem relatar fatos, indicando provas, indícios e circunstâncias.

§ 2º Nas eleições municipais, quando a circunscrição abranger mais de uma Zona Eleitoral, o Tribunal Regional designará um Juiz para apreciar as reclamações ou representações.

§ 3º Os Tribunais Eleitorais designarão três juízes auxiliares para a apreciação das reclamações ou representações que lhes forem dirigidas.

§ 4º Os recursos contra as decisões dos juízes auxiliares serão julgados pelo Plenário do Tribunal.

§ 5º Recebida a reclamação ou representação, a Justiça Eleitoral notificará imediatamente o reclamado ou representado para, querendo, apresentar defesa em quarenta e oito horas.

§ 6º (Revogado pela Lei nº 9.840, de 1999)

§ 7º Transcorrido o prazo previsto no § 5º, apresentada ou não a defesa, o órgão competente da Justiça Eleitoral decidirá e fará publicar a decisão em vinte e quatro horas.

§ 8º Quando cabível recurso contra a decisão, este deverá ser apresentado no prazo de vinte e quatro horas da publicação da decisão em cartório ou sessão, assegurado ao recorrido o oferecimento de contra-razões, em igual prazo, a contar da sua notificação.

§ 9º Os Tribunais julgarão o recurso no prazo de quarenta e oito horas.

§ 10. Não sendo o feito julgado nos prazos fixados, o pedido pode ser dirigido ao órgão superior, devendo a decisão ocorrer de acordo com o rito definido neste artigo.

§ 11. As sanções aplicadas a candidato em razão do descumprimento de disposições desta Lei não se estendem ao respectivo partido, mesmo na hipótese de esse ter se beneficiado da conduta, salvo quando comprovada a sua participação. (Incluído pela Lei nº 13.165, de 2015)

Art. 96-A. Durante o período eleitoral, as intimações via fac-símile encaminhadas pela Justiça Eleitoral a candidato deverão ser exclusivamente realizadas na linha telefônica por ele previamente cadastrada, por ocasião do preenchimento do requerimento de registro de candidatura. (Incluído pela Lei nº 12.034, de 2009)

Parágrafo único. O prazo de cumprimento da determinação prevista no caput é de quarenta e oito horas, a contar do recebimento do fac-símile. (Incluído pela Lei nº 12.034, de 2009)

Art. 96-B. Serão reunidas para julgamento comum as ações eleitorais propostas por partes diversas sobre o mesmo fato, sendo competente para apreciá-las o juiz ou relator que tiver recebido a primeira. (Incluído pela Lei nº 13.165, de 2015)

§ 1º O ajuizamento de ação eleitoral por candidato ou partido político não impede ação do Ministério Público no mesmo sentido. (Incluído pela Lei nº 13.165, de 2015)

§ 2º Se proposta ação sobre o mesmo fato apreciado em outra cuja decisão ainda não transitou em julgado, será ela apensada ao processo anterior na instância em que ele se encontrar, figurando a parte como litisconsorte no feito principal. (Incluído pela Lei nº 13.165, de 2015) (Vide ADI 5507)

§ 3º Se proposta ação sobre o mesmo fato apreciado em outra cuja decisão já tenha transitado em julgado, não será ela conhecida pelo juiz, ressalvada a apresentação de outras ou novas provas. (Incluído pela Lei nº 13.165, de 2015)

Art. 97. Poderá o candidato, partido ou coligação representar ao Tribunal Regional Eleitoral contra o Juiz Eleitoral que descumprir as disposições desta Lei ou der causa ao seu descumprimento, inclusive quanto aos prazos processuais; neste caso, ouvido o representado em vinte e quatro horas, o Tribunal ordenará a observância do procedimento que explicitar, sob pena de incorrer o Juiz em desobediência.

§ 1º É obrigatório, para os membros dos Tribunais Eleitorais e do Ministério Público, fiscalizar o cumprimento desta Lei pelos juízes e promotores eleitorais das instâncias inferiores, determinando, quando for o caso, a abertura de procedimento disciplinar para apuração de eventuais irregularidades que verificarem. (Incluído pela Lei nº 12.034, de 2009)

§ 2º No caso de descumprimento das disposições desta Lei por Tribunal Regional Eleitoral, a representação poderá ser feita ao Tribunal Superior Eleitoral, observado o disposto neste artigo. (Renumerado do parágrafo único pela Lei nº 12.034, de 2009)

Art. 97-A. Nos termos do inciso LXXVIII do art. 5º da Constituição Federal, considera-se duração razoável do processo que possa resultar em perda de mandato eletivo o período máximo de 1 (um) ano, contado da sua apresentação à Justiça Eleitoral. (Incluído pela Lei nº 12.034, de 2009)

§ 1º A duração do processo de que trata o caput abrange a tramitação em todas as instâncias da Justiça Eleitoral. (Incluído pela Lei nº 12.034, de 2009)

§ 2º Vencido o prazo de que trata o caput, será aplicável o disposto no art. 97, sem prejuízo de representação ao Conselho Nacional de Justiça. (Incluído pela Lei nº 12.034, de 2009)

Art. 98. Os eleitores nomeados para compor as Mesas Receptoras ou Juntas Eleitorais e os requisitados para auxiliar seus trabalhos serão dispensados do serviço, mediante declaração expedida pela Justiça Eleitoral, sem prejuízo do salário, vencimento ou qualquer outra vantagem, pelo dobro dos dias de convocação.

Art. 99. As emissoras de rádio e televisão terão direito a compensação fiscal pela cedência do horário gratuito previsto nesta Lei. Regulamento Regulamento Regulamento

§ 1º O direito à compensação fiscal das emissoras de rádio e televisão estende-se à veiculação de propaganda gratuita de plebiscitos e referendos de que dispõe o art. 8º da Lei nº 9.709, de 18 de novembro de 1998, mantido também, a esse efeito, o entendimento de que: (Redação dada pela Lei nº 13.487, de 2017)

I – (VETADO); (Incluído pela Lei nº 12.034, de 2009)

II – a compensação fiscal consiste na apuração do valor correspondente a 0,8 (oito décimos) do resultado da multiplicação de 100% (cem por cento) ou de 25% (vinte e cinco por cento) do tempo, respectivamente, das inserções e das transmissões em bloco, pelo preço do espaço comercializável comprovadamente vigente, assim considerado aquele divulgado pelas emissoras de rádio e televisão por intermédio de tabela pública de preços de veiculação de publicidade, atendidas as disposições regulamentares e as condições de que trata o § 2º-A; (Redação dada pela Lei nº 12.350, de 2010)

III – o valor apurado na forma do inciso II poderá ser deduzido do lucro líquido para efeito de determinação do lucro real, na apuração do Imposto sobre a Renda da Pessoa Jurídica (IRPJ), inclusive da base de cálculo dos recolhimentos mensais previstos na legislação fiscal (art. 2º da Lei nº 9.430, de 27 de dezembro de 1996), bem como da base de cálculo do lucro presumido. (Incluído pela Lei nº 12.350, de 2010)

§ 2º (VETADO) (Incluído pela Lei nº 12.034, de 2009)

§ 2º-A. A aplicação das tabelas públicas de preços de veiculação de publicidade, para fins de compensação fiscal, deverá atender ao seguinte: (Incluído pela Lei nº 12.350, de 2010)

I – deverá ser apurada mensalmente a variação percentual entre a soma dos preços efetivamente praticados, assim considerados os valores devidos às emissoras de rádio e televisão pelas veiculações comerciais locais, e o correspondente a 0,8 (oito décimos) da soma dos respectivos preços constantes da tabela pública de veiculação de publicidade; (Incluído pela Lei nº 12.350, de 2010)

II – a variação percentual apurada no inciso I deverá ser deduzida dos preços constantes da tabela pública a que se refere o inciso II do § 1º. (Incluído pela Lei nº 12.350, de 2010)

§ 3º No caso de microempresas e empresas de pequeno porte optantes pelo Regime Especial Unificado de Arrecadação de Tributos e Contribuições (Simples Nacional), o valor integral da compensação fiscal apurado na forma do inciso II do § 1º será deduzido da base de cálculo de imposto e contribuições federais devidos pela emissora, seguindo os critérios definidos pelo Comitê Gestor do Simples Nacional (CGSN). (Redação dada pela Lei nº 12.350, de 2010)

Art. 100. A contratação de pessoal para prestação de serviços nas campanhas eleitorais não gera vínculo empregatício com o candidato ou partido contratantes, aplicando-se à pessoa física contratada o disposto na alínea *h* do inciso V do art. 12 da Lei nº 8.212, de 24 de julho de 1991. (Redação dada pela Lei nº 13.165, de 2015)

Parágrafo único. Não se aplica aos partidos políticos, para fins da contratação de que trata o **caput**, o disposto no parágrafo único do art. 15 da Lei nº 8.212, de 24 de julho de 1991. (Incluído pela Lei nº 13.165, de 2015)

Art. 100-A. A contratação direta ou terceirizada de pessoal para prestação de serviços referentes a atividades de militância e mobilização de rua nas campanhas eleitorais observará os seguintes limites, impostos a cada candidato: (Incluído pela Lei nº 12.891, de 2013)

I - em Municípios com até 30.000 (trinta mil) eleitores, não excederá a 1% (um por cento) do eleitorado; (Incluído pela Lei nº 12.891, de 2013)

II - nos demais Municípios e no Distrito Federal, corresponderá ao número máximo apurado no inciso I, acrescido de 1 (uma) contratação para cada 1.000 (mil) eleitores que exceder o número de 30.000 (trinta mil). (Incluído pela Lei nº 12.891, de 2013)

§ 1º As contratações observarão ainda os seguintes limites nas candidaturas aos cargos a: (Incluído pela Lei nº 12.891, de 2013)

I - Presidente da República e Senador: em cada Estado, o número estabelecido para o Município com o maior número de eleitores; (Incluído pela Lei nº 12.891, de 2013)

II - Governador de Estado e do Distrito Federal: no Estado, o dobro do limite estabelecido para o Município com o maior número de eleitores, e, no Distrito Federal, o dobro do número alcançado no inciso II do **caput**; (Incluído pela Lei nº 12.891, de 2013)

III - Deputado Federal: na circunscrição, 70% (setenta por cento) do limite estabelecido para o Município com o maior número de eleitores, e, no Distrito Federal, esse mesmo percentual aplicado sobre o limite calculado na forma do inciso II do **caput**, considerado o eleitorado da maior região administrativa; (Incluído pela Lei nº 12.891, de 2013)

IV - Deputado Estadual ou Distrital: na circunscrição, 50% (cinquenta por cento) do limite estabelecido para Deputados Federais; (Incluído pela Lei nº 12.891, de 2013)

V - Prefeito: nos limites previstos nos incisos I e II do **caput**; (Incluído pela Lei nº 12.891, de 2013)

VI - Vereador: 50% (cinquenta por cento) dos limites previstos nos incisos I e II do **caput**, até o máximo de 80% (oitenta por cento) do limite estabelecido para Deputados Estaduais. (Incluído pela Lei nº 12.891, de 2013)

§ 2º Nos cálculos previstos nos incisos I e II do **caput** e no § 1º, a fração será desprezada, se inferior a 0,5 (meio), e igualada a 1 (um), se igual ou superior. (Incluído pela Lei nº 12.891, de 2013)

§ 3º A contratação de pessoal por candidatos a Vice-Presidente, Vice-Governador, Suplente de Senador e Vice-Prefeito é, para todos os efeitos, contabilizada como contratação pelo titular, e a contratação por partidos fica vinculada aos limites impostos aos seus candidatos. (Incluído pela Lei nº 12.891, de 2013)

§ 4º (Revogado pela Lei nº 13.165, de 2015)

§ 5º O descumprimento dos limites previstos nesta Lei sujeitará o candidato às penas previstas no art. 299 da Lei nº 4.737, de 15 de julho de 1965. (Incluído pela Lei nº 12.891, de 2013)

§ 6º São excluídos dos limites fixados por esta Lei a militância não remunerada, pessoal contratado para apoio administrativo e operacional, fiscais e delegados credenciados para trabalhar nas eleições e os advogados dos candidatos ou dos partidos e coligações. (Incluído pela Lei nº 12.891, de 2013)

Art. 101. (VETADO)

Art. 102. O parágrafo único do art. 145 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral passa a vigorar acrescido do seguinte inciso IX:

"Art. 145.....

Parágrafo único.....

IX - os policiais militares em serviço."

Art. 103. O art. 19, *caput,* da Lei nº 9.096, de 19 de setembro de 1995 - Lei dos Partidos, passa a vigorar com a seguinte redação:

"Art. 19. Na segunda semana dos meses de abril e outubro de cada ano, o partido, por seus órgãos de direção municipais, regionais ou nacional, deverá remeter, aos juízes eleitorais, para arquivamento, publicação e cumprimento dos prazos de filiação partidária para efeito de candidatura a cargos eletivos, a relação dos nomes de todos os seus filiados, da qual constará a data de filiação, o número dos títulos eleitorais e das seções em que estão inscritos.

....."

Art. 104. O art. 44 da Lei nº 9.096, de 19 de setembro de 1995, passa a vigorar acrescido do seguinte § 3º:

"Art. 44.....

.....

§ 3º Os recursos de que trata este artigo não estão sujeitos ao regime da Lei nº 8.666, de 21 de junho de 1993."

Art. 105. Até o dia 5 de março do ano da eleição, o Tribunal Superior Eleitoral, atendendo ao caráter regulamentar e sem restringir direitos ou estabelecer sanções distintas das previstas nesta Lei, poderá expedir todas as instruções necessárias para sua fiel execução, ouvidos, previamente, em audiência pública, os delegados ou representantes dos partidos políticos. (Redação dada pela Lei nº 12.034, de 2009)

§ 1º O Tribunal Superior Eleitoral publicará o código orçamentário para o recolhimento das multas eleitorais ao Fundo Partidário, mediante documento de arrecadação correspondente.

§ 2º Havendo substituição da UFIR por outro índice oficial, o Tribunal Superior Eleitoral procederá à alteração dos valores estabelecidos nesta Lei pelo novo índice.

§ 3º Serão aplicáveis ao pleito eleitoral imediatamente seguinte apenas as resoluções publicadas até a data referida no caput. (Incluído pela Lei nº 12.034, de 2009)

Art. 105-A. Em matéria eleitoral, não são aplicáveis os procedimentos previstos na Lei nº 7.347, de 24 de julho de 1985. (Incluído pela Lei nº 12.034, de 2009)

Art. 106. Esta Lei entra em vigor na data de sua publicação.

Art. 107. Revogam-se os arts. 92, 246, 247, 250, 322, 328, 329, 333 e o parágrafo único do art. 106 da Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral; o § 4º do art. 39 da Lei nº 9.096, de 19 de setembro de 1995; o § 2º do art. 50 e o § 1º do art. 64 da Lei nº 9.100, de 29 de setembro de 1995; e o § 2º do art. 7º do Decreto-Lei nº 201, de 27 de fevereiro de 1967.

Brasília, 30 de setembro de 1997; 176º da Independência e 109º da República.

MARCO ANTONIO DE OLIVEIRA MACIEL
Iris Rezende

Este texto não substitui o publicado no D.O.U. de 1º.10.1997

Anexo

Sigla e nº do Partido/série	nome do partido
Recebemos de	Recibo Eleitoral
Endereço:	U.F. |R$ |
Mun. CEP	Município | UFIR |
CPF ou CGC nº	Valor por extenso
a quantia de R$	em moeda corrente
correspondente a UFIR	doação para campanha eleitoral das eleições municipais
Data / /	Data / /
Nome do Responsável	(Assinatura do responsável)
CPF nº	Nome do Resp.
	CPF Nº
	Série: sigla e nº do partido/ numeração seqüencial

FICHA DE QUALIFICAÇÃO DO CANDIDATO

(Modelo 1)

Nome:_____Nº _____

Nº do CPF:_____
Nº da Identidade:_____Órgão Expedidor:_____

Endereço Residencial:_____Telefone:_____

Endereço Comercial:_____Telefone:_____

Partido Político:_____
Comitê Financeiro:_____

Eleição: _____Circunscrição:_____

Conta Bancária nº: _____Banco:_____Agência:_____

Limite de Gastos em REAL: _____

DADOS PESSOAIS DO RESPONSÁVEL PELA ADMINISTRAÇÃO FINANCEIRA DA CAMPANHA

Nome:_____Nº _____

Nº do CPF:_____
Nº da Identidade:_____Órgão Expedidor: _____

Endereço Residencial:_____Telefone:_____

Endereço Comercial:_____Telefone:_____

LOCAL _____DATA_____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

a) - DADOS DO CANDIDATO

1 - **Nome** - informar o nome completo do candidato;

2 - **Nº** - informar o número atribuído ao candidato para concorrer às eleições;

3 - **Nº do** CPF - informar o número do documento de identificação do candidato no Cadastro de Pessoas Físicas;

4 - **N º da Identidade** - informar o número da carteira de identidade do candidato;

5 - **Órgão Expedidor** - informar o órgão expedidor da Carteira de Identidade;

6 - **Endereço Residencial** - informar o endereço residencial completo do candidato;

7 - **Telefone** - informar o número do telefone residencial do candidato, inclusive DDD;

8 - **Endereço Comercial** - informar o endereço comercial completo do candidato;

9 - **Telefone** - informar o número do telefone comercial do candidato, inclusive DDD;

10 - **Partido Político** - informar o nome do partido político pelo qual concorre às eleições;

11 - **Comitê Financeiro** - informar o nome do comitê financeiro ao qual está vinculado o candidato;

12 - **Eleição** - informar a eleição para a qual o candidato concorre (cargo eletivo);

13 - **Circunscrição** - informar a circunscrição à qual está jurisdicionado o Comitê;

14 - **Conta Bancária Nº** - informar o número da conta-corrente da campanha, caso tenha sido aberta pelo Candidato;

15 - **Banco** - se o campo anterior foi preenchido, informar o banco onde abriu a conta-corrente;

16 - **Agência** - informar a agência bancária onde foi aberta a conta-corrente;

17 - **Limite de Gastos em REAL** - informar, em REAL, o limite de gastos estabelecidos pelo Partido;

b) DADOS DO RESPONSÁVEL PELA ADMINISTRAÇÃO FINANCEIRA DA CAMPANHA

1 - **Nome** - informar o nome do Responsável indicado pelo candidato para administrar os recursos de sua campanha;

2 - **Nº do CPF** - informar o número do documento de identificação do Responsável no Cadastro de Pessoas Físicas;

3 - **Nº da Identidade** - informar o número da carteira de identidade do Responsável;

4 - **Órgão Expedidor** - informar o órgão expedidor da Carteira de Identidade;

5 - **Endereço Residencial** - informar o endereço residencial completo do Responsável;

6 - **Telefone** - informar o número do telefone residencial, inclusive DDD;

7 - **Endereço Comercial** - informar o endereço comercial completo do Responsável;

8 - **Telefone** - informar o número do telefone comercial, inclusive DDD;

9 - indicar local e data do preenchimento;

10 - assinaturas do Candidato e do Responsável pela Administração Financeira da Campanha.

DEMONSTRAÇÃO DOS RECIBOS ELEITORAIS RECEBIDOS

(Modelo 2)

Direção Nacional/Estadual do Partido/Comitê Financeiro/Candidato_____

Eleição:_____UF/MUNICÍPIO_____

DATA	NUMERAÇÃO	QUANTIDADE	RECEBIDOS DE

LOCAL _____DATA_____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - DIREÇÃO NACIONAL/ESTADUAL DO PARTIDO/COMITÊ FINANCEIRO/CANDIDATO - informar o nome de quem está apresentando a Demonstração: se Direção Nacional do partido político, Direção Estadual, Comitê Financeiro ou Candidato;

2 - ELEIÇÃO - informar a eleição de que se trata (cargo eletivo);

3 - UF/MUNICÍPIO - informar a Unidade da Federação e Município;

4 - DATA - informar a data em que os Recibos Eleitorais foram recebidos, no formato dia, mês e ano;

5 - NUMERAÇÃO - informar a numeração e série dos Recibos Eleitorais Recebidos;

6 - QUANTIDADE - informar a quantidade de Recibos Eleitorais Recebidos;

7 - RECEBIDOS DE - informar o nome do Órgão repassador dos Recibos;

8 - indicar local e data do preenchimento;

9 - assinatura dos responsáveis.

DEMONSTRAÇÃO DOS RECURSOS ARRECADADOS

(Modelo 3)

Direção Nacional do Partido/Estadual/Comitê/Candidato
_____

Eleição
_____UF/MUNICÍPIO
_____

DATA	NÚMERO DOS RECIBOS	ESPÉCIE DO RECURSO	DOADOR/ CONTRIBUINTE	CGC/CPF	VALORES	
					UFIR	R$
TOTAL/TRANSPORTAR						

LOCAL _____DATA_____/_____/_____

ASSINATURA _____ASSINATURA_____

INSTRUÇÕES DE PREENCHIMENTO

1 - Direção Nacional do Partido/Comitê Financeiro/Candidato - informar o nome de quem está apresentando a Demonstração: se Direção Nacional/Estadual do partido político, Comitê ou Candidato;

2 - Eleição - informar a eleição de que se trata (cargo eletivo);

3 - UF/MUNICÍPIO - informar a Unidade da Federação e Município;

4 - DATA - informar a data em que a doação/contribuição foi recebida, no formato dia, mês e ano;

5 - NÚMERO DOS RECIBOS - informar a numeração e série dos Recibos Eleitorais entregues aos doadores/contribuintes;

6 - ESPÉCIE DO RECURSO - informar o tipo de recurso recebido, se em moeda corrente ou estimável em dinheiro;

7 - DOADOR/CONTRIBUINTE - informar o nome completo de quem doou os recursos, inclusive no caso de recursos próprios do candidato;

8 - CGC/CPF - informar o número do CGC ou do CPF do doador/contribuinte, conforme seja pessoa jurídica ou pessoa física;

9 - VALORES

9-a - UFIR - informar o valor das arrecadações em UFIR, dividindo o valor em R$ pelo valor da UFIR do mês da doação em moeda corrente;

9-b - R$ - informar o valor da doação em moeda corrente;

10 - TOTAL/TRANSPORTAR - informar o total em UFIR e R$ dos valores arrecadados;

11 - indicar local e data do preenchimento;

12 - assinatura dos responsáveis.

RELAÇÃO DE CHEQUES RECEBIDOS

(Modelo 4)

Direção Nacional/Estadual do Partido/Comitê/Candidato
_____

Eleição
_____UF/MUNICÍPIO
_____

DATA DO RECEBIMENTO	IDENTIFICAÇÃO EMITENTE/DOADOR		IDENTIFICAÇÃO DO CHEQUE				VALORES
	NOME	CGC/CPF	DATA DA EMISSÃO	Nº BCO	Nº AG.	Nº CHEQUE	R$

TOTAL/TRANSPORTAR							

LOCAL _____ DATA _____/_____/_____

ASSINATURA _____ ASSINATURA _____

INSTRUÇÕES DE PREENCHIMENTO

1 - DIREÇÃO NACIONAL/ESTADUAL DO PARTIDO/COMITÊ FINANCEIRO/CANDIDATO - informar o nome de quem está apresentando a Demonstração: se Direção Nacional/Estadual do Partido Político, Comitê ou Candidato;

2 - ELEIÇÃO - informar a eleição de que se trata (cargo eletivo);

3 - UF/MUNICÍPIO - informar a Unidade da Federação e Município;

4 - DATA DO RECEBIMENTO - informar a data em que os cheques foram recebidos, no formato dia, mês e ano;

5 - IDENTIFICAÇÃO DO EMITENTE/DOADOR

5-a - NOME - informar o nome do emitente do cheque;

5-b - CGC/CPF - informar o número do CGC ou CPF do emitente do cheque, conforme seja pessoa jurídica ou pessoa física;

6 - IDENTIFICAÇÃO DO CHEQUE

6-a - DATA DA EMISSÃO - informar a data em que o cheque foi emitido pelo doador, no formato dia, mês e ano;

6-b - Nº DO BANCO - informar o número do Banco sacado;

6-c - Nº DA AGÊNCIA - informar o número da Agência;

6-d - Nº DO CHEQUE - informar o número do cheque;

7 - VALORES - R$ - informar o valor dos cheques em moeda corrente;

8 - TOTAL/TRANSPORTAR - informar o total em R$ dos Cheques recebidos.

9 - indicar local e data do preenchimento;

10 - assinatura dos responsáveis.

MODELO 5

DEMONSTRAÇÃO DAS ORIGENS E APLICAÇÕES DOS RECURSOS

PARTIDO/COMITÊ/CANDIDATO:			
ELEIÇÃO:		**UF/MUNICÍPIO**	
TÍTULO DA CONTA			**TOTAL -R$**
1 - RECEITAS			
DOAÇÕES E CONTRIBUIÇÕES			
Recursos Próprios			
Recursos de Pessoas Físicas			
Recursos de Pessoas Jurídicas			
Transferências Financeiras Recebidas			
FUNDO PARTIDÁRIO			
Cotas Recebidas			
RECEITAS FINANCEIRAS			
Variações Monetárias Ativas			
Rendas de Aplicações			
OUTRAS RECEITAS			
Vendas de Bens de Uso			
	F.PARTIDÁRIO	**O. RECURSOS**	**TOTAL - R$**
2 - DESPESAS			

Despesas com Pessoal			
Encargos Sociais			
Impostos			
Aluguéis			
Despesas de Viagens			
Honorários Profissionais			
Locações de Bens Móveis			
Despesas Postais			
Materiais de Expediente			
Despesas com Veículos			
Propagandas e Publicidade			
Serviços Prestados por Terceiros			
Cachês de Artistas ou Animadores			
Materiais Impressos			
Lanches e Refeições			
Energia Elétrica			
Despesas de Manutenção e Reparo			
Montagem de Palanques e Equipamentos			
Despesas com Pesquisas ou Testes Eleitorais			
Despesas de Eventos Promocionais			
Despesas Financeiras			
Produção Audiovisuais			
Outras Despesas			
3 - TRANSFERÊNCIAS FINANCEIRAS EFETUADAS			
4- IMOBILIZAÇÕES - TOTAL			
Bens Móveis			
Bens Imóveis			
SALDO (+1-2-3-4=5) TOTAL			
Saldo em Caixa			
Saldo em Banco			
Banco (...)			

Obs.: As Obrigações a Pagar deverão ser deduzidas dos saldos financeiros (caixa e banco), sendo demonstradas mediante Demonstração de Obrigações a Pagar (Modelo 11) devidamente assinada pelo Tesoureiro.

FICHA DE QUALIFICAÇÃO DO COMITÊ FINANCEIRO

(MODELO 6)

Partido:_____

Direção/Comitê Financeiro/Candidato:_____Único? Sim:_____Não :____

Eleição:_____
UF/Município:_____

Número da Conta Bancária:_____Banco:_____Agência _____

Endereço: _____

NOME DOS MEMBROS	FUNÇÕES

LOCAL _____DATA_____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - NOME DO PARTIDO - informar o nome do partido político;

2 - DIREÇÃO/COMITÊ/CANDIDATO - informar se é da Direção Nacional/Estadual/ Comitê Financeiro ou Candidato;

2-a - ÚNICO? SIM? NÃO? - marcar um X no campo correspondente, conforme se trate, no caso de Comitê Estadual/Municipal, de Comitê Único do Partido para as eleições de toda a circunscrição ou de Comitê específico para determinada eleição;

3 - ELEIÇÃO - informar a eleição de que se trata (cargo eletivo);

4 - UF/MUNICÍPIO - informar a Unidade da Federação e Município;

5 - CONTA BANCÁRIA - informar o número da conta-corrente do Comitê Financeiro;

6 - BANCO - informar o banco onde foi aberta a conta-corrente do Comitê;

7 - AGÊNCIA - informar a agência bancária;

8 - NOMES DOS MEMBROS - informar o nome completo dos membros do Comitê Financeiro;

9 - FUNÇÕES - informar as funções (tipo de responsabilidade) por eles exercidas, na mesma ordem da citação dos nomes;

10 - indicar local e data do preenchimento;

11 - assinatura dos responsáveis.

DEMONSTRAÇÃO DO LIMITE DE GASTOS

(Modelo 7)

Nome do Partido: _____

Direção/Comitê Financeiro/Candidato:_____

ELEIÇÃO

CANDIDATO		LIMITE EM R$
NOME	NÚMERO	
TOTAL / TRANSPORTAR		

LOCAL _____ DATA _____/____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - NOME DO PARTIDO - informar o nome do partido político;

2 - COMITÊ FINANCEIRO/DIREÇÃO/CANDIDATO - informar o nome: se da direção Nacional/Estadual, do Comitê e Candidato que está apresentando a Demonstração;

3 - ELEIÇÃO - informar a eleição de que se trata (cargo eletivo);

4 - CANDIDATO

4-a - NOME - informar o nome completo do Candidato;

4-b - NÚMERO - informar o número atribuído ao candidato, com o qual concorre à eleição;

5 - LIMITE EM R$ - informar o valor em Real do limite de gastos atribuído ao Candidato, pelo partido;

6 - TOTAL / TRANSPORTAR - informar o total em REAL;

7 - indicar o local e a data do preenchimento;

8 - assinatura dos responsáveis.

DEMONSTRAÇÃO DOS RECIBOS ELEITORAIS DISTRIBUÍDOS

(Modelo 8)

Direção Nacional/Estadual/Comitê Financeiro:_____

Eleição:_____

DATA	NUMERAÇÃO	QUANTIDADE	DISTRIBUÍDO A

LOCAL _____ DATA _____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - DIREÇÃO NACIONAL/ESTADUAL DO PARTIDO/COMITÊ FINANCEIRO - informar o nome de quem está apresentando a Demonstração: se Direção Nacional/Estadual do Partido Político ou Comitê Financeiro;

2 - ELEIÇÃO - informar a eleição de que se trata (cargo eletivo);

3 - DATA - informar a data da entrega dos Recibos Eleitorais, no formato dia, mês e ano;

4 - NUMERAÇÃO - informar a numeração dos Recibos Eleitorais Distribuídos, inclusive com a sua série;

5 - QUANTIDADE - informar a quantidade de Recibos Eleitorais Distribuídos, separados por valor de face;

6 - DISTRIBUÍDO A - informar o nome da Direção (Nacional/Estadual) ou do Comitê ou Candidato que recebeu os Recibos Eleitorais;

7 - indicar local e data do preenchimento;

8 - assinatura dos responsáveis.

DEMONSTRAÇÃO DE TRANSFERÊNCIAS FINANCEIRAS

(Modelo 9)

Direção Nacional/Estadual do Partido / Comitê Financeiro:_____

DATA	NOME DO PARTIDO/COMITÊ/CANDIDATO BENEFICIÁRIO	VALORES R$

TOTAL / TRANSPORTAR		

LOCAL _____ DATA _____/____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - DIREÇÃO NACIONAL/ESTADUAL DO PARTIDO / COMITÊ FINANCEIRO - informar o nome de quem realizou as transferências: se Direção Nacional/Estadual do Partido ou Comitê Financeiro, inclusive no caso de coligações;

2 - DATA - informar a data em que ocorreu a transferência financeira, no formato dia, mês e ano;

3 - NOME DO PARTIDO / COMITÊ / CANDIDATO -informar o nome do Partido (Direção Nacional/Estadual) do Comitê ou do Candidato beneficiário da transferência dos recursos, inclusive no caso de coligações;

4 - VALORES - R$ - informar o valor das transferências em moeda corrente;

5 - TOTAL / TRANSPORTAR - informar o total e em R$ das transferências efetuadas;

6 - indicar local e data do preenchimento;

7 - assinatura dos responsáveis.

DEMONSTRAÇÃO FINANCEIRA CONSOLIDADA

(Modelo 10)

Nome do Partido:_____

Direção Nacional:_____

COMITÊS FINANCEIROS VINCULADOS	VALORES R$		
	ARRECADADOS	APLICADOS	SALDOS
TOTAIS/TRANSPORTAR			

LOCAL _____ DATA _____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - NOME DO PARTIDO - informar o nome do partido político;

2 - COMITÊS FINANCEIROS VINCULADOS - informar o nome da Direção Estadual ou Comitês Estadual ou Municipal vinculados à Campanha para Prefeito;

3 - VALORES/R$

3 -a - ARRECADADOS - informar o total, em moeda corrente, dos valores arrecadados para cada Comitê;

3 -b - APLICADOS - informar o total, em moeda corrente, dos valores aplicados para cada comitê;

3 -c - SALDOS - informar os saldos financeiros apresentados, de cada Comitê.

4 - TOTAIS/TRANSPORTAR - informar os totais dos recursos arrecadados, aplicados e dos respectivos saldos, representando o movimento financeiro de toda a campanha para Prefeito;

5 - indicar o local e data do preenchimento;

6 - assinatura dos responsáveis.

DEMONSTRAÇÃO CONSOLIDADA DO LIMITE DE GASTOS

(Modelo 11)

Direção Nacional do Partido Político:_____

CIRCUNSCRIÇÃO	VALORES EM R$
TOTAL/TRANSPORTAR	

LOCAL _____ DATA _____/_____/_____

_____ _____

ASSINATURA ASSINATURA

INSTRUÇÕES DE PREENCHIMENTO

1 - DIREÇÃO NACIONAL DO PARTIDO POLÍTICO - informar o nome do partido político;

2 - Nº - informar o número com o qual o Partido Político concorreu às eleições;

3 - CIRCUNSCRIÇÃO - informar a circunscrição em relação à qual foi estabelecido o limite de gastos;

4 - VALORES REAL - informar o valor em REAL do limite de gastos atribuído pelo Partido, para cada circunscrição;

5 - TOTAL / TRANSPORTAR - informar o total em REAL;

6 - indicar local e data do preenchimento;

7 - assinaturas dos responsáveis.

*

7.3 Anexo C – Res.-TSE n. 23.542/2017

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

RESOLUÇÃO Nº 23.542, DE 18 DE DEZEMBRO DE 2017.

Altera a Resolução-TSE nº 23.444, de 30 de abril de 2015 e dispõe sobre a realização periódica do Teste Público de Segurança(TPS) nos sistemas eleitorais que especifica.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das atribuições que lhe conferem o art. 23, inciso IX, do Código Eleitoral (http://www.planalto.gov.br/ccivil_03/leis/L4737.htm#art23) e o art. 105 da Lei nº 9.504 (http://www.planalto.gov.br/ccivil_03/leis/L9504.htm#art105) , de 30 de setembro de 1997, RESOLVE:

Art. 1º O art. 21 da Resolução-TSE nº 23.444 (https://www.tse.jus.br/legislacao/compilada/res/2015/resolucao-no-23-444-de-30-de-abril-de-2015) , de 30 de abril de 2015, passa a vigorar acrescido de parágrafo único com a seguinte redação:

> Parágrafo único. Os partidos políticos, as coligações, a Ordem dos Advogados do Brasil, o Ministério Público, o Congresso Nacional, o Supremo Tribunal Federal, o Ministério da Transparência e Controladoria-Geral da União, o Departamento de Polícia Federal, a Sociedade Brasileira de Computação, o Conselho Federal de Engenharia e Agronomia serão formalmente convocados para, querendo, participar e acompanhar o TPS na forma regulamentada nesta Resolução.

Art. 2º Esta resolução entra em vigor na data de sua publicação.

Brasília, 18 de dezembro de 2017.

Composição: Ministros Gilmar Mendes (presidente), Luiz Fux, Rosa Weber, Napoleão Nunes Maia Filho, Jorge Mussi, Admar Gonzaga e Tarcisio Vieira de Carvalho Neto. Vice-Procurador-Geral Eleitoral: Humberto Jacques de Medeiros.

Este texto não substitui o publicado no DJE-TSE, nº 245, de 19.12.2017, p. 94. (http://sintse.tse.jus.br/documentos/2017/Dez/19/diario-da-justica-eletronico-tse/resolucao-no-23-542-de-18-de-dezembro-de-2017-altera-a-resolucao-tse-no-23-444-de-30-de-abril-de-2015-e-dispoe-sobre-a-realizacao-periodica-do-teste-publico-de-seguranca-tps-nos-sistemas-eleitorais-que-especifica)

7.4 Anexo D – Portarias das comissões

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

PORTARIA Nº 672, DE 30 DE AGOSTO DE 2023.

Institui as Comissões Organizadora, Reguladora e de Comunicação Institucional, referentes ao Teste Público de Segurança - 2023.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto nos arts. 8º, 9º e 11 da Resolução-TSE nº 23.444, de 30 de abril de 2015,

RESOLVE:

Art. 1º Instituir as Comissões Organizadora, Reguladora e de Comunicação Institucional, que atuarão no Teste Público de Segurança - 2023, nos termos previstos na Resolução-TSE nº 23.444, de 30 de abril de 2015, com a seguinte composição:

I - COMISSÃO ORGANIZADORA:

a) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral, como coordenador dos trabalhos;

b) Simone Ferreira de Almeida Siqueira (Cosen/SAD), representante da Secretaria de Administração;

c) Geni Maria Péres Lobato (Gab-SAD), representante da Secretaria de Administração;

d) João Rodrigues de Magalhães (SPJ), representante da Secretaria de Polícia Judicial;

e) Giselly Siqueira (Secom), representante titular da Secretaria de Comunicação e Multimídia;

f) Cecília Malheiros de Melo (Secom), representante suplente da Secretaria de Comunicação e Multimídia;

g) Luciano Teixeira Andrade (Coinf/STI), representante da Secretaria de Tecnologia da Informação;

h) Andréa Gonçalves Barbosa (Neci/STI), representante da Secretaria de Tecnologia da Informação;

i) Renato Barros de Carvalho (ACP), representante da Assessoria de Cerimonial da Presidência;

j) Washington Luiz de Oliveira (Cedip/SGIC), representante da Secretaria de Gestão da Informação e do Conhecimento;

k) Isabella Dantas Sinotti (Cedip/SGIC), representante da Secretaria de Gestão da Informação e do Conhecimento; e

l) Maurício Miranda Sá (Seeve/COEDE), representante da Secretaria de Gestão de Pessoas.

II - COMISSÃO REGULADORA:

a) Júlio Valente da Costa Júnior (STI), representante da Secretaria de Tecnologia da Informação, como coordenador dos trabalhos;

b) Cristiano Moreira Andrade (Coinf/STI);

c) Elmano Amâncio de Sá Alves (AGC/STI);

d) Rafael Fernandes de Barros Costa Azevedo (Cotel/STI);

e) José de Melo Cruz (CSele/STI);

f) Rodrigo Carneiro Munhoz Coimbra (Sevin/Cotel/STI);

g) Marcelo Carneiro Rodrigues (SDCIBER/Coinf/STI);

h) Ivanildo Ferreira Gomes (Sesap/COINF/STI);

i) Alberto Araújo Cavalcante Neto (Setot/CSELE/STI);

j) Vinícius Salustiano Alves dos Santos (Seint/CSELE/STI);

k) Carlos Eduardo Miranda Zottmann (Nesc/STI); e

l) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral.

III - COMISSÃO DE COMUNICAÇÃO INSTITUCIONAL:

a) Giselly Siqueira (Secom), representante da Secretaria de Comunicação e Multimídia, como coordenadora dos trabalhos;

b) Cecília Malheiros de Melo (Cimp/Secom), representante da Secretaria de Comunicação e Multimídia;

c) Júlio Valente da Costa Júnior (STI), representante da Secretaria de Tecnologia da Informação;

d) Andréa Gonçalves Barbosa (Neci/STI), representante da Secretaria de Tecnologia da Informação; e

e) Thiago Fini Kanashiro (Agel/DG), representante da Diretoria-Geral.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Ministro ALEXANDRE DE MORAES

Este texto não substitui o publicado no DJE-TSE, nº 192, de 28.9.2023, p. 166-168.

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

PORTARIA Nº 701, DE 6 DE SETEMBRO DE 2023.

Institui a Comissão Avaliadora para atuar no Teste Público de Segurança - 2023.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 10 da Resolução-TSE nº 23.444, de 30 de abril de 2015,

RESOLVE:

Art. 1º Fica instituída a Comissão Avaliadora para atuar na realização do Teste Público de Segurança - 2023, com a seguinte composição:

I - representantes da Presidência do TSE:

a) Rogério Marrone de Castro Sampaio - Juiz Auxiliar da Presidência, que a presidirá; e

b) Paulo Rogério Bonini - Juiz Auxiliar da Presidência.

II - membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:

a) Jamil Salem Barbar - Professor Doutor;

b) Mamede Lima-Marques - Professor Doutor;

c) Osvaldo Catsumi Imamura - Professor Doutor; e

d) Antonio Esio Marcondes Salgado - Professor Mestre;

III - representantes do Ministério Público Federal: (Redação dada pela Portaria nº 950/2023)

a) Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas; e (Incluído pela Portaria nº 950/2023)

b) Thiago Henrique Fernandes - Analista do MPU/Desenvolvimento de Sistemas; (Incluído pela Portaria nº 950/2023)

IV - representante da Ordem dos Advogados do Brasil: Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico; (Redação dada pela Portaria nº 950/2023)

V - representante do Congresso Nacional: Veneziano Vital do Rêgo - Senador da República;

VI - representante do Departamento de Polícia Federal: Paulo César Herrmann Wanner - Perito Criminal Federal e Coordenador da CCAT/CGCIBER/DCIBER;

VII - representante do Tribunal de Contas da União: André Luiz Furtado Pacheco - Auditor Federal de Controle Externo;

VIII - representante do Conselho Federal de Engenharia e Agronomia: Rodrigo de Souza Borges - Engenheiro de Computação e Gerente de Tecnologia da Informação; e

IX - representante da Sociedade Brasileira de Computação: Roberto Samarone dos Santos Araújo - Professor Doutor.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

MINISTRO ALEXANDRE DE MORAES

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

PORTARIA Nº 950, DE 04 DE DEZEMBRO DE 2023

Altera a composição da Comissão Avaliadora para atuar no Teste Público de Segurança - 2023.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 10 da Resolução-TSE nº 23.444, de 30 de abril de 2015,

RESOLVE:

Art. 1º O art. 1º da Portaria TSE nº 701, de 6 de setembro de 2023, que institui a Comissão Avaliadora para atuar no Teste Público de Segurança - 2023, passa a vigorar com a seguinte redação:

"Art. 1º .....
.....
III - representantes do Ministério Público Federal:
a) Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas; e
b) Thiago Henrique Fernandes - Analista do MPU/Desenvolvimento de Sistemas;
IV - representante da Ordem dos Advogados do Brasil: Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico;
....." (NR)

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Ministro ALEXANDRE DE MORAES

Este texto não substitui o publicado no DJE-TSE, nº 252, de 21.12.2023, p. 1-2.

TRIBUNAL SUPERIOR ELEITORAL

Portaria TSE nº 397 de 3 de junho de 2024.

Altera a composição da Comissão Avaliadora para atuar no Teste Público de Segurança – 2023.

O PRESIDENTE DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições e tendo em vista o disposto no art. 10 da Resolução-TSE nº 23.444, de 30 de abril de 2015,

RESOLVE

Art. 1º O artigo 1º da Portaria TSE nº 701, de 6 de setembro de 2023, que institui a Comissão Avaliadora para atuar no Teste Público de Segurança – 2023, passa a vigorar com a seguinte redação:

"Art. 1º .....

VI - representantes do Departamento de Polícia Federal:

.....; e

b) Flávio Silveira da Silva - Perito Criminal.

VIII - representantes do Conselho Federal de Engenharia e Agronomia:

.....; e

b) Fernando Batista da Silva - Assessor de TI do CONFEA.

....." (NR)

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Ministro ALEXANDRE DE MORAES
Presidente

7.5 Anexo E – Aviso de audiência pública

TESTE PÚBLICO DE SEGURANÇA DA URNA

AVISO DE AUDIÊNCIA PÚBLICA

A Comissão Organizadora do Teste Público de Segurança da Urna 2023, no uso de suas atribuições, comunica aos interessados que, em cumprimento ao disposto no art. 18, inciso I, da Resolução TSE nº 23.444/2015, será realizada audiência pública com o objetivo exclusivo de esclarecer as regras do teste, definidas na mencionada norma e no Edital, das 10:00 às 11:00, do dia 15 de setembro de 2023, transmitida pelo canal oficial do TSE no Youtube (https://www.youtube.com/justicaeleitoral).

O envio de dúvidas poderá ser realizado até o início do evento, para o e-mail tps2023@tse.jus.br.

7.6 Anexo F – Editais

DIÁRIO DA JUSTIÇA ELETRÔNICO

DO TRIBUNAL SUPERIOR ELEITORAL

Ano: 2023, nº 164 **Disponibilização**: terça-feira, 22 de agosto de 2023

Edição Extraordinária **Publicação**: quarta-feira, 23 de agosto de 2023

Tribunal Superior Eleitoral

Ministro Alexandre de Moraes
Presidente

Ministra Cármen Lúcia
Vice-Presidente

Rui Moreira de Oliveira
Diretor-Geral

Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2
Brasília/DF
CEP: 70070-600

Contato
(61) 3030-8800
sjd@tse.jus.br

SUMÁRIO

Atos da Presidência 1

ATOS DA PRESIDÊNCIA

EDITAL

EDITAL DE CONVOCAÇÃO - TPS 2023

Nº 1/2023

TESTE PÚBLICO DE SEGURANÇA - TPS 2023

A Comissão Reguladora comunica às interessadas e aos interessados que, conforme estabelecido na Resolução-TSE nº 23.444, de 30 de abril de 2015, será realizado o Teste Público de Segurança no sistema eletrônico de votação e apuração, no período de 27 de novembro a 1º de dezembro de 2023, nos horários estabelecidos no art. 31 deste edital, na sede do Tribunal Superior Eleitoral (Setor de Administração Federal Sul - SAFS, Quadra 7, lotes 1/2, Brasília/DF).

CAPÍTULO I

DO OBJETO

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

Art. 1º Constitui objeto deste edital a realização do Teste Público de Segurança (TPS) no sistema eletrônico de votação e apuração que será utilizado nas eleições municipais de 2024.

Parágrafo único. O TPS de que trata este edital constitui parte integrante do ciclo de desenvolvimento dos sistemas eleitorais de votação, apuração, transmissão, recebimento de arquivos e apoio aos processos de auditoria da urna eletrônica.

Art. 2º Os sistemas eleitorais que serão objetos do TPS são aqueles utilizados para a geração de mídias, votação, apuração, transmissão e o recebimento de arquivos, lacrados em cerimônia pública, incluindo o *hardware* da urna eletrônica, seus *softwares* embarcados e os sistemas de apoio aos processos de auditoria sobre *software* da urna.

§ 1º Os componentes de *software* e *hardware* que serão objeto do TPS consistem em:

I - Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE);

II - *Software* Básico da Urna Eletrônica, *Software* de Carga (SCUE), Gerenciador de Aplicativos (GAP), *Software* de Votação (VOTA), Recuperador de Dados (RED) e Sistema de Apuração (SA);

III - Sistemas Transportador, RecArquivos e InfoArquivos;

IV - Subsistema de Instalação e Segurança (SIS) e *Kit* JEConnect;

V - Urnas modelos 2020 e 2022, com seus respectivos *firmwares* e mídias eletrônicas;

VI - Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação;

VII - Verificador Pré/Pós-Eleição (VPP);

VIII - Verificador de integridade e autenticidade de sistemas eleitorais (AVPART).

§ 2º Não serão objetos do TPS os seguintes sistemas, ambientes, procedimentos e elementos abaixo relacionados:

I - identificação e verificação biométrica do eleitor;

II - preparação e infraestrutura para o *Kit* JEConnect;

III - processamento dos arquivos de urna eletrônica (fase posterior às fases de transmissão e de recebimento dos arquivos gerados pela urna após o encerramento da votação na seção);

IV - sistema da totalização (Sistot e seus módulos);

V - acesso aos equipamentos servidores;

VI - acesso aos bancos de dados;

VII - ataques de negação de serviço;

VIII - ataque destrutivo à urna eletrônica e aos demais recursos computacionais da Justiça Eleitoral;

IX - sistema de geração de chaves criptográficas;

X - alteração do código-fonte dos sistemas;

XI - ambiente de compilação dos sistemas;

XII - lacre físico: selos autoadesivos utilizados na urna eletrônica com a finalidade de detectar eventuais violações ao equipamento.

§ 3º Conforme o § 2º do art. 66 da Lei nº 9.504, de 30 de setembro de 1997, as chaves eletrônicas privadas e senhas eletrônicas de acesso serão mantidas sob sigilo da Justiça Eleitoral.

§ 4º A versão dos sistemas a ser utilizada no TPS será gerada com observância dos procedimentos da Cerimônia de Assinatura Digital e Lacração dos Sistemas, no que couber.

CAPÍTULO II

DO OBJETIVO

Art. 3º O TPS tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos, bem como propiciar o aperfeiçoamento do processo eleitoral.

Parágrafo único. O TPS contempla ações controladas com o objetivo de identificar vulnerabilidades e/ou falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição, além de apresentar as respectivas sugestões de melhoria.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

CAPÍTULO III
DAS DEFINIÇÕES
Art. 4º Para fins deste edital considera-se:
I - falha: evento em que se observa que um sistema violou sua especificação por ter entrado em estado inconsistente, ocasionado por uma imperfeição (defeito) em determinado *software* ou *hardware*, impedindo seu bom funcionamento, sem interferir na destinação e/ou no anonimato dos votos das eleitoras e dos eleitores;
II - vulnerabilidade explorada: ato intencional que tenha explorado uma fragilidade que comprometa uma barreira de segurança, mas que não seja condição suficiente para violar a destinação ou o sigilo dos votos, ou, caso sejam alcançados, que deixe a existência de vestígios;
III - fraude: ato intencional que tenha alterado informações e/ou causado danos, interferindo na destinação e/ou no anonimato dos votos, e que tenha sido efetuado de forma a não restarem vestígios perceptíveis;
IV - plano de teste: documento que será fornecido para identificação e descrição das ações a serem desenvolvidas por investigadora, investigador e/ou grupo de investigadores na realização do teste;
V - ambiente de execução de plano de teste: ambiente com acesso controlado, monitorado por câmeras, onde serão dispostos microcomputadores e urnas eletrônicas para que a investigadora, o investigador e/ou grupo de investigadores possam preparar e realizar os testes;
VI - ambiente de apresentação dos códigos-fonte: área interna ao ambiente de execução do plano de teste preparada para que a investigadora, o investigador e/ou grupo de investigadores possam avaliar os códigos-fonte;
VII - teste de confirmação: reprodução, executada por investigadora, investigador e/ou grupo de investigadores, do teste realizado durante o TPS - no qual foi identificada falha, vulnerabilidade explorada ou fraude - em uma nova versão do sistema eleitoral que contempla as devidas correções, com o intuito de avaliar a melhoria implementada.
CAPÍTULO IV
DA COORDENAÇÃO E DA ATUAÇÃO NO TESTE PÚBLICO DE SEGURANÇA
Art. 5º O TPS será coordenado pelo Ministro Presidente do Tribunal Superior Eleitoral (TSE).
Art. 6º Conforme estabelecido no art. 6º da Resolução-TSE nº 23.444/2015, atuarão no TPS:
I - a Comissão Organizadora;
II - a Comissão Reguladora;
III - a Comissão Avaliadora;
IV - a Comissão de Comunicação Institucional; e
V - a investigadora, o investigador e/ou grupo de investigadores.
CAPÍTULO V
DA COMUNICAÇÃO E DOS PRAZOS
Art. 7º Todos os formulários e documentos a serem remetidos ao TSE, para fins de pré-inscrição, inscrição, manifestação e recurso, deverão ser:
I - encaminhados, preferencialmente, para o *e-mail* tps2023@tse.jus.br; ou
II - encaminhados por SEDEX ou carta registrada, endereçados à Secretaria de Tecnologia da Informação do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF, CEP 70070-600); ou
III - protocolizados no Protocolo Administrativo, na sede do TSE (SAFS, Quadra 7, lotes 1/2, Brasília/DF), que funciona ordinariamente de segunda a sexta-feira, das 11 às 19 horas.
§ 1º O TSE confirmará o recebimento de *e-mail* imediatamente após proceder à leitura da mensagem.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

§ 2º No caso de a investigadora, o investigador ou o grupo de investigadores não receberem a confirmação de leitura ou de recebimento pelo TSE, no prazo por ela/ele julgado conveniente, o conteúdo da mensagem e/ou material anexo deverá ser encaminhado por SEDEX ou protocolizado no Tribunal, respeitando-se os prazos estabelecidos neste edital.

Art. 8º O sítio oficial do TPS será www.justicaeleitoral.jus.br/tps/.

§ 1º As informações relacionadas ao evento serão publicadas no sítio oficial do TPS.

§ 2º Mensagens eletrônicas (*e-mail*) recebidas de investigadora, investigador ou grupo de investigadores serão respondidas por *e-mail*, exceto se a resposta for de interesse geral, quando poderá ser publicada no sítio oficial do TPS.

Art. 9º As datas e os prazos que norteiam o Teste Público de Segurança estão informados no Calendário do Evento, anexo a este edital, e TPS na internet.

§ 1º Os prazos poderão ser prorrogados a critério do TSE.

§ 2º Quaisquer alterações de datas serão informadas no sítio oficial do TPS, no prazo mínimo de 2 (dois) dias úteis de antecedência do marco estabelecido no Calendário do Evento.

CAPÍTULO VI

DA PARTICIPAÇÃO

Art. 10. Serão admitidas até 15 (quinze) inscrições para o TPS, individuais ou compostas por grupo de investigadores, observando-se o seguinte:

I - a participação poderá ser individual ou em grupo, estes integrados por até 5 (cinco) membros;

II - a/o participante não pode possuir mais de uma inscrição, seja em grupo ou individual;

III - a participação presencial, nos eventos do TPS, será limitada a 45 (quarenta e cinco) investigadores de forma simultânea, a fim de garantir o bom andamento dos trabalhos.

Parágrafo único. É vedada a participação, na condição de investigadora, investigador e/ou de grupo de investigadores, de componentes das comissões definidas no art. 6º da Resolução-TSE nº 23.444/2015.

Art. 11. A participação, na condição de investigadora, investigador ou de grupo de investigadores, está condicionada à seleção prévia, que será realizada em 3 (três) etapas:

I - aprovação da pré-inscrição;

II - aprovação da inscrição; e

III - disponibilidade orçamentária e sorteio público.

Parágrafo único. A Comissão Avaliadora poderá, a seu critério, selecionar os planos de testes de até 2 (dois) participantes (investigadora, investigador ou grupo de investigadores) que não foram sorteados.

CAPÍTULO VII

DA PRÉ-INSCRIÇÃO

Art. 12. A pré-inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Pré-Inscrição, que será obtido no sítio oficial do TPS.

Art. 13. O formulário Pré-Inscrição preenchido e os documentos comprobatórios exigidos deverão ser encaminhados, postados ou protocolizados no TSE, respeitados os prazos estabelecidos no Marco 1 do Calendário do Evento em anexo.

Art. 14. Terão sua pré-inscrição aprovada, na condição de investigadora, investigador ou grupo de investigadores, as cidadãs ou os cidadãos brasileiros maiores de 18 anos que preencham os requisitos constantes do formulário de pré-inscrição.

§ 1º Cada grupo de investigadores deverá designar 1 (um) de seus componentes para representá-lo.

§ 2º Deverão constar das pré-inscrições os dados referentes a todas/todos as/os componentes do grupo.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

§ 3º Caso um dos membros do grupo de investigadores não atenda aos requisitos do formulário de pré-inscrição, o grupo terá sua pré-inscrição aprovada parcialmente.
§ 4º A investigadora, o investigador ou grupo de investigadores deverão informar, no momento do preenchimento do formulário de pré-inscrição, se desejam fazer uso de recursos financeiros do TSE para o custeio de diárias e passagens.
§ 5º Pessoa jurídica poderá pré-inscrever-se, observando-se que:
I - terá sua pré-inscrição aprovada a pessoa jurídica (investigadora, investigador ou grupo de investigadores que a represente no TPS) que cumpra todas as exigências do edital;
II - não serão aceitas pré-inscrições de empresas sem registro no Cadastro Nacional de Pessoa Jurídica (CNPJ).
Art. 15. Serão publicadas, no sítio oficial do TPS e na data estabelecida no Marco 2 do Calendário do Evento (anexo), as pré-inscrições aprovadas.
§ 1º A investigadora, o investigador e/ou grupo de investigadores que não tiverem sua pré-inscrição aprovada poderão apresentar recurso ao TSE.
§ 2º O recurso deverá ser encaminhado, postado ou protocolizado no TSE, direcionado à Comissão Reguladora do TPS, respeitado o prazo estabelecido no Marco 3 do Calendário do Evento (anexo).
§ 3º O resultado do recurso será apresentado no sítio oficial do TPS, na data prevista no Marco 4 do Calendário do Evento (anexo).
Art. 16. A palestra de que trata o art. 18, III, da Resolução-TSE nº 23.444/2012, será realizada por meio de vídeos explicativos, conforme o Marco 5 do Calendário do Evento.
Art. 17. A investigadora, o investigador e/ou grupo de investigadores com a pré-inscrição aprovada poderão agendar, com antecedência mínima de 48 (quarenta e oito) horas, respeitado o prazo estabelecido no Marco 6 do Calendário do Evento, visita à sede do TSE para inspeção dos códigos-fonte.
§ 1º A investigadora, o investigador e/ou grupo de investigadores terão acesso aos códigos-fonte por meio de ferramenta de visualização fornecida pelo TSE.
§ 2º Só terão acesso aos códigos-fonte a investigadora, o investigador e/ou grupo de investigadores que assinarem o termo de responsabilidade.
§ 3º A investigadora, o investigador e/ou grupo de investigadores deverão assinar o termo de responsabilidade para ingressarem no ambiente de apresentação dos códigos-fonte.
§ 4º A assinatura do termo de responsabilidade se dará no momento de ingresso no ambiente de apresentação dos códigos-fonte.
§ 5º Serão publicados no sítio oficial do TPS:
I - o modelo do termo de responsabilidade, para fins de conhecimento prévio da investigadora, do investigador e/ou grupo de investigadores; e
II - o período reservado para a inspeção dos códigos-fonte.
§ 6º O tempo destinado para inspeção dos códigos-fonte será estabelecido pelo TSE e divulgado na página do evento, conforme a capacidade do ambiente e a quantidade de interessadas(os), em até 2 (dois) dias antes do período de inspeção.
§ 7º A assinatura digital dos códigos-fonte a serem inspecionados será realizada no primeiro dia do período estabelecido no Marco 6 do Calendário do Evento, sendo facultada à investigadora, ao investigador e/ou ao grupo de investigadores presentes, desde que estejam de posse de certificado digital padrão ICP Brasil.
§ 8º O Tribunal avaliará eventual pedido de custeio de diárias e passagens para essa fase do evento, que se sujeitará à disponibilidade orçamentária prevista para o TPS.
CAPÍTULO VIII
DA INSCRIÇÃO

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

Art. 18. A inscrição deverá ser realizada por meio do preenchimento de formulário específico, denominado Plano de Teste, que será obtido no sítio oficial do TPS.

§ 1º Poderão apresentar plano de teste a investigadora, o investigador e/ou grupo de investigadores com pré-inscrição aprovada.

§ 2º Cada investigadora, investigador e/ou grupo de investigadores poderá apresentar mais de um plano de teste.

Art. 19. O formulário Plano de Teste preenchido e os documentos complementares, caso existentes, deverão ser encaminhados, postados ou protocolizados no TSE, respeitado o prazo estabelecido no Marco 7 do Calendário do Evento em anexo.

Art. 20. Terão sua inscrição aprovada, na condição de investigadora, investigador e/ou de grupo de investigadores, as/os participantes que tiverem seu plano de teste aprovado pela Comissão Reguladora.

Parágrafo único. Não serão aprovados os planos de testes que:

I - não atenderem aos objetivos específicos de alterar a destinação dos votos ou fragilizar o sigilo do voto;

II - não atenderem ao objeto estabelecido no art. 2º deste edital;

III - não demonstrarem clareza quanto ao(s) objetivo(s) ou objeto(s) a ser(em) atendido(s); ou

IV - forem entregues após o prazo estipulado no Marco 7 do Calendário do Evento.

Art. 21. Na data estabelecida no Marco 8 do Calendário do Evento, serão publicadas as inscrições aprovadas no sítio oficial do TPS.

§ 1º A investigadora, o investigador e/ou grupo de investigadores que não tiverem sua inscrição aprovada poderá apresentar recurso ao TSE, respeitado o prazo estabelecido no Marco 9 do Calendário do Evento.

§ 2º O recurso deverá ser encaminhado, postado ou protocolizado no TSE, direcionado à Comissão Reguladora do TPS.

§ 3º O resultado do recurso será apresentado no sítio oficial do TPS, na data prevista no Marco 10 do Calendário do Evento.

Art. 22. A aprovação pelo TSE da inscrição da investigadora, do investigador e/ou do grupo de investigadores não garante a participação nos testes públicos de segurança, tendo em vista que essa está condicionada ao quantitativo de inscritos, cuja seleção final obedecerá ao disposto no art. 23 deste edital.

CAPÍTULO IX

DO EXCESSO DE INSCRIÇÕES E DO SORTEIO PÚBLICO

Art. 23. Caso a quantidade de participantes com inscrição aprovada seja superior à estipulada no art. 10 deste edital, a Comissão Reguladora fará a seleção entre as inscrições aprovadas e levará em consideração a relevância dos planos de testes para o aprimoramento do sistema eletrônico de votação, podendo, ainda, recorrer a sorteio público.

Parágrafo único. O processo de seleção de inscrições está sujeito à disponibilidade orçamentária prevista para o evento.

Art. 24. Caso haja necessidade de sorteio público, este será realizado nas instalações do TSE, em data estabelecida no Marco 11 do Calendário do Evento.

§ 1ª O sorteio público será transmitido ao vivo pelo canal oficial do TSE, no YouTube, em horário informado no sítio do evento.

Art. 25. O resultado das inscrições será publicado no sítio oficial do TPS, conforme data estabelecida no Marco 12 do Calendário do Evento.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

§ 1º A investigadora, o investigador e/ou grupo de investigadores que não tiverem sua inscrição selecionada poderão apresentar recurso ao TSE, respeitado o prazo estabelecido no Marco 13 do Calendário do Evento.

§ 2º O recurso deverá ser encaminhado, postado ou protocolizado no TSE, direcionado à Comissão Reguladora do TPS.

§ 3º O resultado do recurso será apresentado, no sítio oficial do TPS, na data estabelecida no Marco 14 do Calendário do Evento.

CAPÍTULO X

DAS INSCRIÇÕES SELECIONADAS

Art. 26. A investigadora, o investigador e/ou grupo de investigadores que tiverem sua inscrição selecionada e que optarem pelo custeio de deslocamento pelo TSE, deverão requerer passagens e diárias ao Tribunal.

§ 1º As passagens e diárias deverão ser requeridas até a data estabelecida no Marco 15 do Calendário do Evento, utilizando-se do formulário Solicitação de Diárias e Passagens, disponível no sítio oficial do TPS.

§ 2º As regras para emissão de passagens e diárias observarão o disposto em resolução específica da Justiça Eleitoral.

§ 3º O custeio de diárias compreenderá o período equivalente às fases de realização do TPS e do Teste de Confirmação (Resolução-TSE nº 23.444/2015, art. 14 e art. 16, respectivamente), conforme estabelecido nos Marcos 17 e 20 do Calendário do Evento.

§ 4º Será aferida a presença por meio de lista, a ser assinada pelas/pelos participantes durante o evento.

§ 5º O TSE deverá requerer o reembolso da investigadora, do investigador e/ou do integrante do grupo de investigadores que:

I - tiverem passagens e/ou diárias custeadas pelo TSE e não comparecerem ao evento;

II - receberem quantidade de diárias maior do que o período de comparecimento ao evento; e

III - outros casos em que a Comissão Reguladora entender que o plano de teste não foi executado conforme definido e por responsabilidade exclusiva da investigadora, do investigador ou grupo de investigadores.

Art. 27. A investigadora, o investigador ou grupo de investigadores selecionados declaram ter ciência de que:

I - devem disponibilizar à Comissão Reguladora toda a documentação e materiais utilizados, bem como os procedimentos realizados durante as atividades, independentemente do resultado obtido no TPS; e

II - autorizam o uso de sua imagem pela Justiça Eleitoral, com a finalidade de divulgar o processo do TPS realizado pelo TSE, entendendo-se como imagem qualquer forma de representação, inclusive a fotográfica, bem como o processo audiovisual, que resulta da fixação de imagens, com ou sem som, que tenha a finalidade de criar, por meio de sua reprodução, a impressão de movimento, independentemente dos processos de sua captação, do suporte usado inicial ou posteriormente para fixá-lo e dos meios utilizados para sua veiculação.

CAPÍTULO XI

DO TESTE PÚBLICO DE SEGURANÇA

Art. 28. O TSE disponibilizará no ambiente do TPS os seguintes materiais e equipamentos:

I - folhas de papel em branco;

II - canetas esferográficas;

III - mesas;

IV - cadeiras;

V - microcomputadores padrão IBM-PC com plataforma Windows e/ou

Ubuntu Linux 64 *bits*, que não poderão ser conectados à internet;
VI - impressoras;
VII - chave Philips;
VIII - urnas eletrônicas, conforme art. 2º, inciso V;
IX - suprimentos de urnas e mídias; e
X - *Kit* JEConnect.
Parágrafo único. Será de responsabilidade da investigadora, do investigador e/ou grupo de investigadores a configuração dos equipamentos necessários à realização de seu plano de testes de segurança.
Art. 29. O microcomputador disponibilizado pelo TSE (art. 28, V), a urna eletrônica (art. 28, VIII) e os demais equipamentos, eventualmente preparados pela investigadora, pelo investigador e/ou grupo de investigadores, serão lacrados ao término da preparação.
§ 1º Os equipamentos referidos no *caput* deste artigo terão sua integridade verificada, no dia do teste, pela investigadora, pelo investigador e/ou grupo de investigadores, ou ainda por integrante(s) das comissões referidas no art. 6º deste edital.
§ 2º Eventual alteração no plano de testes, já entregue pela investigadora, pelo investigador e/ou grupo de investigadores, e aprovado pela Comissão Reguladora, ficará sujeita à nova aceitação.
Art. 30. Durante a realização do TPS, os códigos-fonte estarão disponíveis para consulta no ambiente de apresentação, observando-se as seguintes condições:
I - é vedada a extração, impressão e/ou reprodução, mesmo que parcial, dos códigos-fonte;
II - é vedado ingressar no ambiente de apresentação com qualquer instrumento que permita a cópia dos códigos-fonte;
III - são permitidas anotações que não confrontem o termo de responsabilidade:
a) as anotações estarão sujeitas à análise da Comissão Reguladora;
b) compete à investigadora, ao investigador ou grupo de investigadores responsabilizar-se por suas anotações; e
c) as anotações serão de uso restrito ao ambiente do TPS.
Parágrafo único. As vedações referidas nos incisos I e II deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente de apresentação dos códigos-fonte.
Art. 31. O Teste Público de Segurança realizar-se-á em período estabelecido no Marco 17 do Calendário do Evento, na sede do TSE.
§ 1º. O evento terá início às 13 horas do primeiro dia e findará às 17 horas, e, nos demais dias, das 9 às 18 horas.
§ 2°. Excepcionalmente, as/os participantes poderão submeter, por escrito, pedido fundamentado de extensão do prazo por 1 (um) dia adicional, o qual será prontamente analisado pela Comissão Avaliadora e permitirá, caso deferido, a continuidade da execução do respectivo plano de teste durante o primeiro dia subsequente ao final do TPS.
Art. 32. Somente serão executados os planos de testes da investigadora, do investigador e/ou grupos de investigadores que:
I - tiverem sua inscrição aprovada e selecionada; e
II - estiverem presentes no momento da realização dos testes.
§ 1º Somente serão autorizados os planos de testes que forem aprovados e atendam aos requisitos deste edital, que não causem danos físicos aos equipamentos e às instalações disponibilizados para os citados testes, bem como forem tecnicamente viáveis, sendo proferida decisão fundamentada pela Comissão Reguladora do TPS.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

§ 2º Para fins do inciso II deste artigo, os grupos de investigadores poderão ter apenas uma/um representante, exceto se houver, no grupo, mais de uma/um integrante que recebeu diárias e passagens custeadas pelo TSE, cuja presença é obrigatória, sob pena de devolução dos valores.

Art. 33. Ao final da fase de realização do TPS, cada investigadora, investigador ou grupo de investigadores deverá apresentar relatório referente às ações executadas e aos resultados alcançados, de acordo com as regras definidas neste edital.

Art. 34. A investigadora, o investigador e/ou grupo de investigadores, caso identifiquem alguma falha, vulnerabilidade explorada ou fraude, nos termos do parágrafo único do art. 3º deste edital, deverá apresentar as respectivas sugestões de melhoria, para avaliação do TSE.

§ 1º Em data estabelecida pelo TSE, anterior à Cerimônia Oficial de Assinatura Digital e Lacração dos Sistemas que serão utilizados nas eleições de 2024, a investigadora, o investigador e/ou grupo de investigadores, que alcançarem os objetivos descritos no parágrafo único do art. 3º, serão convocados pelo TSE para repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude, conforme estabelecido no Capítulo XIII.

§ 2º A investigadora, o investigador e/ou grupo de investigadores somente poderão manifestar-se publicamente sobre a falha ou vulnerabilidade encontrada após a divulgação do relatório da Comissão Avaliadora.

CAPÍTULO XII

DA DIVULGAÇÃO DOS RESULTADOS

Art. 35. Em data estabelecida no Marco 18 do Calendário do Evento, após o encerramento dos trabalhos, será realizada divulgação preliminar dos resultados obtidos com o TPS e entregue o certificado de participação à investigadora, ao investigador e grupo de investigadores, na sede do TSE.

§ 1º Será concedido o certificado à investigadora, ao investigador e/ou grupos de investigadores que tiverem seus planos de testes devidamente executados, independentemente do resultado.

§ 2º Além do disposto no § 1º deste artigo, somente será concedido o certificado às/aos integrantes dos grupos que estiveram presentes na ocasião da realização do respectivo teste de segurança.

§ 3º O local dos testes públicos será no edifício sede do Tribunal Superior Eleitoral.

Art. 36. Em data estabelecida no Marco 19 do Calendário do Evento, em horário divulgado no sítio do TPS, será realizada ampla divulgação de relatório final dos resultados e das conclusões do TPS, elaborado pela Comissão Avaliadora, bem como relatório de avaliação geral elaborado pelo TSE.

CAPÍTULO XIII

DO TESTE DE CONFIRMAÇÃO

Art. 37. Em data estabelecida no Marco 20 do Calendário do Evento, a investigadora, o investigador e/ou grupo de investigadores que alcançarem os objetivos descritos no parágrafo único do art. 3º, serão convocados pelo TSE para repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

§ 1º Na hipótese prevista no *caput,* a investigadora, o investigador e/ou grupo de investigadores serão notificados para comparecer ao Teste de Confirmação, via carta registrada ou *e-mail* com aviso de recebimento, devendo ser justificada possível ausência.

§ 2º Durante o Teste de Confirmação será disponibilizada visualização dos códigos-fonte no ambiente de apresentação, conforme o art. 17 deste edital.

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

§ 3º A nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano que identificou a falha, vulnerabilidade explorada ou fraude, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.
§ 4º As modificações serão apresentadas no período de realização do Teste de Confirmação, conforme o Marco 20 do Calendário de Eventos.
§ 5º Os grupos de investigadores poderão ter apenas 1 (um/uma) representante, exceto se houver, no grupo, mais de uma/um integrante que recebeu diárias e passagens custeadas pelo TSE, cuja presença é obrigatória, sob pena de devolução dos valores recebidos.
§ 6º Uma vez realizados os novos testes e tendo sido comprovado o saneamento das falhas e/ou vulnerabilidades anteriormente encontradas, a investigadora, o investigador e/ou grupo de investigadores deverão assinar termo com a confirmação das correções feitas pelo TSE ou submeter nova manifestação, à qual o TSE responderá tecnicamente até o Marco 21 do Calendário do Evento.
Art. 38. Em data estabelecida no Marco 21 do Calendário do Evento, em horário divulgado no sítio do TPS, será realizada ampla divulgação de relatório final dos resultados e das conclusões do TPS, elaborado pela Comissão Avaliadora, bem como relatório de avaliação geral elaborado pelo TSE.
CAPÍTULO XIV
DAS DISPOSIÇÕES GERAIS
Art. 39. As atividades executadas durante a inspeção dos códigos-fonte, a realização do TPS e o Teste de Confirmação poderão ser registradas pelo TSE em áudio e vídeo.
Art. 40. Para ingresso no ambiente destinado à realização do TPS, deverá ser observado que:
I - a entrada de outros equipamentos ou dispositivos, desde que não tenham acesso à internet, está sujeita à autorização do representante da Comissão Reguladora, não sendo permitida a entrada de aparelhos celulares;
II - a investigadora, o investigador e/ou grupo de investigadores poderão utilizar os *softwares* que julgarem necessários e instalá-los no microcomputador disponibilizado pelo TSE, observando-se o disposto no inciso I deste artigo;
III - o ingresso com materiais impressos será permitido;
IV - os equipamentos, dispositivos eletrônicos e materiais citados nos incisos I e II deste artigo, quando aprovados, poderão ficar retidos no TSE até que seja divulgado o resultado final do TPS, definido no Marco 19 do Calendário do Evento.
§ 1º Os equipamentos ou dispositivos que tenham ficado retidos no TSE para uso durante os testes, nos termos do inciso I, estarão à disposição das/dos participantes após o prazo citado no inciso IV deste artigo.
§ 2º As vedações referidas nos incisos I a IV deste artigo aplicam-se a quaisquer pessoas que tenham acesso ao ambiente destinado à realização do TPS.
Art. 41. O ingresso no ambiente do TPS e no ambiente de apresentação dos códigos-fonte será restrito:
I - à investigadora, ao investigador e/ou grupo de investigadores;
II - às/aos integrantes das comissões referidas no art. 6º deste edital;
III - às demais pessoas autorizadas pela Comissão Reguladora.
Art. 42. Haverá, no ambiente do TPS, computadores conectados à internet para eventuais consultas por investigadora, investigador e/ou grupo de investigadores, sob supervisão da Comissão Reguladora.
I - os computadores referidos no *caput* deste artigo terão acesso a um *drive* de rede disponibilizado pela Comissão Organizadora, onde poderão ser salvos arquivos com conteúdo baixado da internet;

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

II - a investigadora, investigador e/ou grupo de investigadores que salvarem arquivos no *drive* de rede referido no inciso I deste artigo deverão informar à Comissão Organizadora, solicitando que tais arquivos sejam gravados em mídia digital de sua propriedade (previamente entregues à Comissão Reguladora, conforme disposto no art. 40, inciso I);

III - as mídias gravadas, conforme disposto no inciso II deste artigo, serão imediatamente entregues à investigadora, ao investigador e/ou grupo de investigadores;

IV - eventuais mídias digitais não utilizadas somente serão devolvidas à investigadora, ao investigador e/ou grupo de investigadores quando estes deixarem o ambiente destinado à realização do TPS;

V - os computadores referidos no *caput* deste artigo terão acesso a uma impressora conectada em rede para eventuais impressões de documentos baixados da internet, não sendo permitido:

a) imprimir qualquer outro conteúdo;

b) editar o conteúdo baixado antes da respectiva impressão; e

c) deixar o ambiente destinado à realização do TPS portando qualquer uma destas folhas impressas.

VI - as folhas impressas nos termos do inciso V deste artigo deverão ser solicitadas à Comissão Reguladora, que, após verificar sua conformidade com as limitações definidas nas alíneas 'a' e 'b' do inciso V deste artigo, as disponibilizará imediatamente.

Art. 43. A Comissão Avaliadora poderá ter acesso aos códigos-fonte, em caso de necessidade, sendo o acesso autorizado pela Comissão Reguladora, mediante a assinatura de termo de responsabilidade.

Art. 44. Este edital será publicado no DJE/TSE e divulgado no sítio eletrônico do TSE e na página oficial do TPS.

Art. 45. Será dada publicidade à composição das comissões referidas no art. 6º deste edital por meio do DJE/TSE e de divulgação no sítio oficial do TPS.

Art. 46. Integra este edital o Calendário do Evento, em anexo.

Art. 47. Os casos omissos serão dirimidos pelo Presidente do TSE, que poderá delegar a atribuição a ministra ou ministro, magistrada ou magistrado ou a servidora ou servidor do Tribunal.

ANEXO

CALENDÁRIO DO EVENTO

Marco	Referência	Descrição do Marco	Prazo/período
1	Art. 13	Encaminhamento do formulário de pré-inscrição preenchido e dos documentos comprobatórios exigidos	23/08 a 08/09/2023
6	Art. 17	Assinatura e inspeção dos códigos-fonte	/2023
7	Art. 19	Encaminhamento do formulário Plano de Teste preenchido e dos documentos complementares, caso haja	09/10/2023 a 03/11/2023
8	Art. 21	Publicação das inscrições aprovadas	06/11/2023

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

9	§ 1º do art. 21	Apresentação de recursos referentes à fase de inscrição aprovada	06 a 09/11/2023
10	§ 3º do art. 21	Publicação do resultado do recurso referente à fase de inscrição aprovada	13/11/2023
11	Art. 24	Sorteio público para seleção de inscrições, se necessário	14/11/2023
12	Art. 25	Publicação dos resultados das inscrições selecionadas	14/11/2023
13	§ 1º do art. 25	Apresentação de recursos referentes à fase de inscrição selecionada	15 a 17/11/2023
14	§ 3º do art. 25	Publicação do resultado do recurso referente à fase de inscrição selecionada	18/11/2023
15	§ 1º do art. 26	Requisição de passagens e diárias	10 a 14/11/2023
16	Art. 32	Abertura dos testes públicos de segurança e credenciamento dos investigadores	27/11/2023
17	Art. 32	Realização dos testes públicos de segurança	27/11 a 01/12/2023
18	Art. 36	Divulgação preliminar dos resultados do Teste Público de Segurança e entrega dos certificados de participação	01/12/2023
19	Art. 37	Divulgação do resultado final do Teste Público de Segurança	15/12/2023
20	Art. 38	Realização do Teste de Confirmação	15 a 17/05/2024
21	Art. 39	Divulgação do resultado final da confirmação do Teste Público de Segurança	30/05/2024

Ministro ALEXANDRE DE MORAES

Documento assinado eletronicamente em 22/08/2023, às 14:53, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2569613&crc=DD58BB92, informando, caso não preenchido, o código verificador 2569613 e o código CRC DD58BB92.

2023.00.000010049-9

ÍNDICE DE ADVOGADOS

ÍNDICE DE PARTES

ÍNDICE DE PROCESSOS

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

Ano 2023 - n. 206 Brasília, quarta-feira, 18 de outubro de 2023 112

ATOS DA PRESIDÊNCIA

EDITAL

EDITAL DE CONVOCAÇÃO - TPS 2023

EDITAL Nº 2/2023

TESTE PÚBLICO DE SEGURANÇA - TPS 2023

Art. 1º A Comissão Reguladora comunica às interessadas e aos interessados, no uso de suas atribuições legais, previstas na Resolução-TSE nº 23.444, de 30 de abril de 2015, que o Anexo do Edital nº 1/2023 do Público de Segurança - TPS 2023 - passa a vigorar com as seguintes alterações:

ANEXO

CALENDÁRIO DO EVENTO

Marco	Referência	Descrição do Marco	Prazo/período
1	Art. 13	Encaminhamento do formulário de pré-inscrição preenchido e dos documentos comprobatórios exigidos	23/08 a 08/09/2023
2	Art. 15	Publicação das pré-inscrições aprovadas	08/09/2023
3	§ 2º do art. 15	Apresentação de recurso referente à fase de pré-inscrição	08/09 a 12/09/2023
4	§ 3º do art. 15	Publicação do resultado do recurso referente à fase de pré-inscrição	13/09/2023
5	Art. 16	Disponibilização de vídeos explicativos sobre o processo eleitoral	13/09/2023
6	Art. 17	Assinatura e inspeção dos códigos-fonte	09 a 13/10/2023 16 a 20/10/2023
7	Art. 19	Encaminhamento do formulário Plano de Teste preenchido e dos documentos complementares, caso haja	09/10/2023 a 27/10/2023
8	Art. 21	Publicação das inscrições aprovadas	03/11/2023
9	§ 1º do art. 21	Apresentação de recursos referentes à fase de inscrição aprovada	03 a 06/11/2023
10	§ 3º do art. 21	Publicação do resultado do recurso referente à fase de inscrição aprovada	08/11/2023

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

11	Art. 24	Seleção das inscrições aprovadas por relevância técnica e, se necessário, sorteio	09 a 10/11/2023
12	Art. 25	Publicação dos resultados das inscrições selecionadas	10/11/2023
13	§ 1º do art. 25	Apresentação de recursos referentes à fase de inscrição selecionada	11 a 14/11/2023
14	§ 3º do art. 25	Publicação do resultado do recurso referente à fase de inscrição selecionada	16/11/2023
15	§ 1º do art. 26	Requisição de passagens e diárias	10 a 16/11/2023
16	Art. 32	Abertura dos testes públicos de segurança e credenciamento dos investigadores	27/11/2023
17	Art. 32	Realização dos testes públicos de segurança	27/11 a 01/12/2023
18	Art. 36	Divulgação preliminar dos resultados do Teste Público de Segurança e entrega dos certificados de participação	01/12/2023
19	Art. 37	Divulgação do resultado final do Teste Público de Segurança	15/12/2023
20	Art. 38	Realização do Teste de Confirmação	15 a 17/05/2024
21	Art. 39	Divulgação do resultado final da confirmação do Teste Público de Segurança	30/05/2024

Ministro ALEXANDRE DE MORAES

Documento assinado eletronicamente em 17/10/2023, às 16:59, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=2609741&crc=CCCFC37B, informando, caso não preenchido, o código verificador 2609741 e o código CRC CCCFC37B

2023.00.000010049-9

Diário da Justiça Eletrônico do Tribunal Superior Eleitoral (DJE/TSE). Documento assinado digitalmente conforme MP n. 2.200-2/2001 de 24.8.2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, podendo ser acessado no endereço eletrônico http://www.tse.jus.br/

7.7 Anexo G – Lista de pré-inscrições

TESTE PÚBLICO DE SEGURANÇA DA URNA

Nome do(a) pré-inscrito(a)	Tipo de Inscrição	Situação da pré-inscrição
Filipe Cunha Barreto Gomes Franca	Individual	Aprovada
Guilherme Henrique dos Santos	Individual	Aprovada
Nicholas Barros dos Santos	Individual	Aprovada
Gilson Gonçalves Trindade	Individual	Aprovada
Hyago Santana Mariano	Individual	Aprovada
Luciano Estevam Santos	Individual	Aprovada
Daniel Bento de Castro	Individual	Aprovada
Diego Ferry Torrent	Individual	Aprovada
Adailton Souza dos Santos	Individual	Aprovada
Victor Masashi dos Santos Ofugi	Individual	Aprovada
Gabriel Brito da Cruz	Individual	Aprovada
Faberson de Melo	Individual	Aprovada
Marcelo da Silva Rodrigues	Individual	Aprovada
Janaína Santos Nascimento	Individual	Aprovada
João Vitor Santana	Individual	Aprovada
Lucio Santos de Sá	Individual	Aprovada
Eliel Mota de Souza	Individual	Aprovada
Douglas Ribeiro Garcia	Individual	Aprovada
Carlos Adão Barbosa Marcelino	Individual	Aprovada
Jhonatha William Fernandes Souto	Individual	Aprovada
Ricardo Antônio Pralon Santos	Individual	Aprovada
Daniel Paulo Zan SIlva	Individual	Aprovada
Jefesson Leite Alves	Individual	Aprovada
Érika Maria Rodrigues de Castro	Individual	Aprovada
Joao Benedito dos Santos Junior	Individual	Aprovada
Marcelo Amarante Ferreira Gomes	Individual	Aprovada
Aline Barbosa da Silva	Individual	Aprovada
Guilherme Djrdjrjan Santos	Individual	Aprovada
Márcia Aparecida Reis	Individual	Aprovada
Tatiana dos Santos Gomes Franca	Grupo	Aprovada
Mariana Lagares de Paula	Grupo	Aprovada
Maria Helena Lopes Sales	Grupo	Aprovada
Thayser Stanys Coelho Berwian Schineider	Grupo	Aprovada
Iracila de Nazaré Moraes da Silva	Grupo	Aprovada
Marcos Roberto dos Santos	Grupo	Aprovada
Leandro Caletti	Grupo	Aprovada
Rafael Noll da Silva	Grupo	Aprovada
Eduardo Bido	Grupo	Aprovada
Rhayara Rodrigues Fiorentin	Grupo	Aprovada
Rafael Basso Reis	Grupo	Aprovada
Stefano Augusto Mossi	Grupo	Aprovada

Gabriel Viecili	Grupo	Aprovada
André Izolani Rien	Grupo	Aprovada
Brayan Vanz de Oliveira	Grupo	Aprovada
Gabriel Leonardo de Sena Santos	Grupo	Aprovada
Tamires da Silva Ferreira	Grupo	Aprovada
Maria Luceilda de Lima Santos	Grupo	Aprovada
Maria Aparecida de Sena Santos	Grupo	Aprovada
Gabriel Sordi Damo	Grupo	Aprovada
Augusto Zanini	Grupo	Aprovada
Vitor Aloisio do Nascimento Guia	Grupo	Aprovada
Hitatiana M.S.F.S Guia	Grupo	Aprovada
Carlos Alberto da Silva	Grupo	Aprovada
Ian Martinez Zimmermann	Grupo	Aprovada
Matheus Vianna Silveira	Grupo	Aprovada
Mário de Araújo Carvalho	Grupo	Aprovada
Eloisa Pétala Valerio	Grupo	Aprovada
Maicon Soares Carlos	Grupo	Aprovada
Wesley de Oliveira Gerônimo	Grupo	Aprovada
Galileu Batista de Sousa	Grupo	Aprovada
Maria Isabel Vasconcelos Lima	Grupo	Aprovada
Breno Rangel Borges Marchetti	Grupo	Aprovada
João Paulo Vieira Almeida	Grupo	Aprovada
João Vitor de Sá Hauck	Grupo	Aprovada
Breno Henrique Pelegrin da Silva	Grupo	Aprovada
Yuri Martins	Grupo	Aprovada
Pedro Martins Oliveira	Grupo	Aprovada
Nayara Ayres	Grupo	Aprovada
Aline Diniz de Oliveira	Grupo	Aprovada
Luis Antonio Brasil Kowada	Grupo	Aprovada
Gabriel Cardoso de Carvalho	Grupo	Aprovada
Caubi de Souza Loureiro Rosa	Grupo	Aprovada
Camila Ferreira Alves	Grupo	Aprovada
André Mário dos Reis dos Santos	Grupo	Aprovada
Alexandre Zago Boava	Grupo	Aprovada
Diego Vergaças de Sousa Carvalho	Grupo	Aprovada
Victor Antunes Ignácio de Medeiros Pereira da Silva	Grupo	Aprovada
Gabriel Lima Sertão	Grupo	Aprovada
Charles Willian Biesseki	Grupo	Aprovada
Alan Papafamurakis Heleno	Grupo	Aprovada
Daniel Lima Carvalho	Grupo	Aprovada
Crischarles Delgado Arruda	Grupo	Aprovada
Avelino Francisco Zorzo	Grupo	Aprovada
Ariel Rossetto Ril	Grupo	Aprovada
Daniel Dalalana Bertoglio	Grupo	Aprovada

7.8 Anexo H – Análise dos planos de testes

TESTE PÚBLICO DE SEGURANÇA DA URNA — Tribunal Superior Eleitoral — #VOZ DA DEMOCRACIA ELEIÇÕES 2024

A Comissão Reguladora, instituída por meio da Portaria TSE nº 672/2023, publica, nos termos abaixo, o resultado da análise dos planos de teste apresentados no período de 09 a 27/10/2023.

1) A Comissão ressalta que, nos termos do art. 22 do Edital n. 2/2023, a aprovação das inscrições nesta fase **não garante** a participação da investigadora, do investigador e/ou do grupo de investigadores nos testes públicos de segurança, tendo em vista a necessidade de atender ao disposto nos artigos 10 e 23 do mencionado edital, quanto ao quantitativo de inscritos e a relevância dos planos de teste.

2) No caso das inscrições **não aprovadas**, a investigadora, o investigador ou o representante do grupo de investigadores poderá apresentar recurso, nos termos do art. 21 do Edital n. 1/2023,respeitando o prazo estabelecido no Marco 9 do Edital n. 2/2023, qual seja, **no período de 03 a 06/11/2023.**

3) A Comissão ressalta, por fim, a relevância do plano de teste demonstrar com clareza como alcançará aos objetivos específicos de alterar a destinação dos votos ou de fragilizar o sigilo do voto, nos termos do inciso I do Parágrafo Único do Art. 20 do Edital n. 1/2023.

Nome do(a) pré-inscrito(a)	Tipo de Inscrição	Plano de Teste Aprovado	Plano de Teste Reprovado	Fundamento da Reprovação
Aline Barbosa de Silva	Individual	Quebra do sigilo do voto		
		Fragilizar sigilo do voto		
		Invadir a mídia de carga da urna eletrônica		
Diego Ferry Torrent	Individual	Sigilo e Proteção do voto: Fortaleza Magnética e Defesa Eletromagnética para a Democracia		
Eliel Mota de Souza	Individual		Teste de Sigilo do Voto	Art. 20, parágrafo único, inciso III do Edital n. 1/2023
Erika Maria Rodrigues de Castro	Individual	Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia		
Gilson Gonçalves Trindade	Individual		Extração da Carga da Urna	Art. 20, parágrafo único, incisos I e III do Edital n. 1/2023
Guilherme Henrique dos Santos	Individual	*Fraus Omnia Corrumpit*		
		Nihil Autem Abiscondtum Est, Quod Non Revelabitur		
		Qui Duplicat, Videre Suffragio Potest		
		Suffragium Simulata Substantiam Veritas Mutare Possunt		
Joao Benedito dos Santos Junior	Individual	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		
João Vitor Santana	Individual	Auditoria de Integridade e Segurança na Apuração Eletrônica de Votos		

Lucio Santos de Sá	Individual		Execução de código arbitrário via JE Connect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Márcia Aparecida Reis	Individual		Formulário de teste em branco	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Nicholas Barros dos Santos	Individual		Execução do JE-Connect utilizando computador com sistema operacional inválido	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
			Criação de sistema antivandalismo para as urnas eletrônicas	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
		Comportamento do JE-Connect na execução de um bot de monitoramento no computador transmissor de dados		
Ricardo Antônio Pralon Santos	Individual	Investigação dos mecanismos de validação do Bootloader pela Bios para a proteção da carga segura do SO da UE		
Tatiana dos Santos Gomes Franca	Grupo		Habilitação do eleitor: identificar eventuais bloqueios de permissões de acesso à urna eletrônica para a votação	Art. 20, parágrafo único, incisos I e III do Edital n. 1/2023
Maria Helena Lopes Sales				
Thayser Stanys Coelho Berwian Schineider				
Iracila de Nazaré Moraes da Silva				
Marcos Roberto dos Santos	Grupo		Spy for Screenshot - quebra do sigilo do voto em ambiente de votação por análise de imagens	Art. 2º, § 1º do Edital n. 1/2023
Leandro Caletti		USBExploit – acesso a dados da urna através da porta USB		
Rafael Noll da Silva				
Eduardo Bido				
Rhayara Rodrigues Fiorentin				
Rafael Basso Reis	Grupo	Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores		
Stefano Augusto Mossi		Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de shell a partir de um dispositivo USB		
Gabriel Viecili				
André Izolani Rien				
Brayan Vanz de Oliveira				
Vitor Aloisio do Nascimento Guia	Grupo	Adulteração no JE Connect		
Hitatiana Maria Santiago Ferreira da Silva Guia				
Carlos Alberto da Silva	Grupo		Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Ian Martinez Zimmermann			Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
			Violar a confidencialidade, integridade e disponibilidade das informações na função urlib.parse do Python no Software JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
			Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023

Matheus Vianna Silveira			Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Mário de Araújo Carvalho			Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Eloisa Pétala Valerio	Grupo		Processo de Melhoria no Cadastro do eTítulo - Inclusão de Imagem	Art. 3º do Edital n. 1/2023
Maicon Soares Carlos			Produção de documentos físicos em material biodegradável	Art. 3º do Edital n. 1/2023
Wesley de Oliveira Gerônimo			Autenticação de dois fatores na urna eletrônica como fator de proteção a identidade do eleitor e do voto secreto	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Galileu Batista de Sousa	Grupo	Executar código espúrio na Urna Eletrônica modelo 2020		
Maria Isabel Vasconcelos Lima		Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020		
Breno Rangel Borges Marchetti		Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto		
João Paulo Vieira Almeida		Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI		
João Vitor de Sá Hauck		Alterar dados / programas nos sistemas SIS/GEDAI		
		Ataque de cold boot à Urna Eletrônica		
Breno Henrique Pelegrin da Silva	Grupo		Análise de CVEs em dependências da urna e software inicializador da urna	Art. 2º, § 2º, inciso X do Edital n. 1/2023
Yuri Martins				
Luis Antonio Brasil Kowada	Grupo	Tentativa de Man-in-the-Middle na comunicação do teclado com Arduino		
Gabriel Cardoso de Carvalho				
Caubi de Souza Loureiro Rosa		Tentativa de reconhecimento das teclas digitadas usando IA		
Camila Ferreira Alves				
André Mário dos Reis dos Santos	Grupo	Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas		
Alexandre Zago Boava				
Diego Vergaças de Sousa Carvalho				
tor Antunes Ignácio de Medeiros Pereira da Silva				
Charles Willian Biesseki	Grupo		Invasão ao JEConnect	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Alan Papafamurakis Heleno				
Daniel Lima Carvalho				
Crischarles Delgado Arruda				
Avelino Francisco Zorzo	Grupo	Inconsistência de Software		
Ariel Rossetto Ril			JE Connect - Validação de softwares core	Art. 20, parágrafo único, inciso I do Edital n. 1/2023
Daniel Dalalana Bertoglio			RecArquivos - Exploração de arquivos ZIP	Art. 20, parágrafo único, inciso I e art. 1º, § 2º, inciso VIII do Edital n. 1/2023

7.9 Anexo I – Resultado dos recursos

TESTE PÚBLICO DE SEGURANÇA DA URNA — Tribunal Superior Eleitoral — #VOZ DA DEMOCRACIA ELEIÇÕES 2024

A Comissão Reguladora, instituída por meio da Portaria TSE nº 672/2023, publica, nos termos do § 3º do art. 21 do Edital n. 1/2023, o resultado da análise dos recursos apresentados no período de 03 a 06/11/2023.

Nome do(a) pré-inscrito(a)	Tipo de Inscrição	Plano de Teste Recorrido	Situação do Recurso	Motivo do indeferimento do recurso
Nicholas Barros dos Santos	Individual	Execução do JE-Connect utilizando computador com sistema operacional inválido	ACATADO COM RESSALVA	O plano de teste mantém o foco em eventuais vulnerabilidades do JE-Connect. Sendo assim, considerando que os sistemas de transporte de arquivos têm como objetivo único o de transportar, para totalização, a informação já apurada e publicada (BU) pela urna eletrônica, e protegida por assinatura digital, o plano de teste deve, necessariamente, envidar ações cujo objetivo seja o de efetivamente tentar adulterar o resultado da votação ou o anonimato dos votos de uma eleição, e não se limitar à simples tentativa de vulnerar o mecanismo de transporte.
		Criação de sistema antivandalismo para as urnas eletrônicas	NÃO ACATADO	Embora o plano trate de sugestão de aprimoramento do processo eleitoral, ele não contempla nenhuma ação controlada com o objetivo de violar a integridade ou o anonimato do voto, nos termos do parágrafo único do art. 3º do Edital n. 1/2023. Sendo assim, ainda que o TPS tenha como escopo a melhoria contínua do processo eleitoral, essa deve ser decorrente da apresentação de ações que objetivem vulnerar o sigilo ou a integridade do voto. A proposta do investigador, por se tratar de sugestão de melhoria apartada de ações de teste, será submetida à análise das áreas responsáveis do TSE, para verificação quanto à viabilidade de implantação.
Carlos Alberto da Silva	Grupo	Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect	ACATADO COM RESSALVA	Os planos de testes mantêm o foco em eventuais vulnerabilidades do JE-Connect. Sendo assim, considerando que os sistemas de transporte de arquivos têm como objetivo único o de transportar, para totalização, a informação já apurada e publicada (BU) pela urna eletrônica, e protegida por assinatura digital, os planos de testes devem, necessariamente, envidar ações cujo objetivo seja o de efetivamente tentar adulterar o resultado da votação ou o anonimato dos votos de uma eleição, e não se limitar à simples tentativa de vulnerar o mecanismo de transporte.
Ian Martinez Zimmermann		Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConnect	ACATADO COM RESSALVA	
		Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JEConnect	ACATADO COM RESSALVA	
Matheus Vianna Silveira		Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConnect	ACATADO COM RESSALVA	
		Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConnect	ACATADO COM RESSALVA	
Mário de Araújo Carvalho		Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita	ACATADO COM RESSALVA	
Eloisa Pétala Valerio	Grupo	Produção de documentos físicos em material biodegradável	NÃO ACATADO	Embora os planos tratem de sugestões de aprimoramento do processo eleitoral, eles não contemplam nenhuma ação controlada com o objetivo de violar a integridade ou o anonimato do voto, nos termos do parágrafo único do art. 3º do Edital n. 1/2023. Sendo assim, ainda que o TPS tenha como escopo a melhoria contínua do processo eleitoral, essa deve ser decorrente da apresentação de ações que objetivem vulnerar o sigilo ou a integridade do voto. As propostas do grupo, por se tratarem de sugestões de melhorias apartadas de ações de teste, serão submetidas à análise das áreas responsáveis do TSE, para verificação quanto à viabilidade de implantação.
Maicon Soares Carlos				
Wesley de Oliveira Gerônimo		Autenticação de dois fatores na urna eletrônica como fator de proteção a identidade do eleitor e do voto secreto	NÃO ACATADO	
Charles Willian Bieseki	Grupo	Invasão ao JEConnect	NÃO CONHECIDO	§ 1º do art. 21 do Edital n. 1/2023 (Intempestividade)
Alan Papafamurakis Heleno				
Daniel Lima Carvalho				
Crischarles Delgado Arruda				

7.10 Anexo J – Planos de testes aprovados

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste QUEBRA DO SIGILO DO VOTO
Instituição proponente (se aplicável)
Responsável ALINE BARBOSA DA SILVA FERREIRA
Resumo do plano (máximo de 120 caracteres) No dia da Eleição, a votação se inicia normalmente. O primeiro eleitor vota, assim sucessivamente irei retirar da urna eletrônica a mídia de resultados. Ela será lida no Notebook com o kit JE-CONNECT , assim quebrando o sigilo do voto do eleitor.
Sistemas a serem testados

Softwares

(X) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(X) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
(X) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos

(X) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano: Com este plano viso, testar se a mídia de resultados contabiliza o voto mesmo sem ter encerrado a sessão no terminal do mesário. Assim quebrando o sigilo do voto do eleitor.

2 – Fundamentação teórica:

3 – Precondições para o teste: Não tenho uma precondição para realizar o teste.

4 – Escopo – Superfície de ataque: Irei me atentar as vunerabilidades no momento do teste, com o foco na urna eletrônica.

5 – Janela de atuação simulada do atacante:

6 – Pontos de intervenção:

7 – Passos a serem realizados: A votação na seção se inicia o primeiro eleitor vota e se retira da gabine de voto, sucessivamente irei retirar a mídia de resultado sem encerrar a seção no terminal do mesário, instalo a mídia no Notbook já com o programa JE CONNECT faço a transferências dos arquivos da urna (nesse momento irei testar se o voto foi computado, antes de terminar a seção). Assim tendo o voto da mídia tranferido, quebrarei o sigilo do voto do primeiro eleitor.

8 – Materiais necessários (fornecidos pelo TSE):

9 – Possíveis resultados e impacto: Vulnerabilidade no sigilo do voto, gravação de arquivo sem ter encerrado a seção.

10 – Rastreabilidade:

11 – Solução proposta: Assim que realizar o teste apresento minha proposta, se realmente encontrar alguma vulnerabilidade.

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

FRAGILIZAR SIGILO DO VOTO

Instituição proponente (se aplicável)

Responsável

ALINE BARBOSA DA SILVA FERREIRA

Resumo do plano (máximo de 120 caracteres)

No dia da Eleição na secão de votação, irei instalar um dispositivo na urna eletrônica em que ao eleitor precionar as teclas do seu voto, o dispositivo emitira o som de qual tecla foi acionada.

Sistemas a serem testados

Softwares

(X) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

2 – Fundamentação teórica:

3 – Precondições para o teste: Não tenho uma precondição para realizar o teste.

4 – Escopo – Superfície de ataque:

5 – Janela de atuação simulada do atacante:

6 – Pontos de intervenção:

7 – Passos a serem realizados:

8 – Materiais necessários (fornecidos pelo TSE):

9 – Possíveis resultados e impacto: Vulnerabilidade em fragilizar o voto do eleitor.

10 – Rastreabilidade:

11 – Solução proposta: Assim que realizar o teste apresento minha proposta, se realmente encontrar alguma vulnerabilidade.

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste INVADIR A MÍDIA DE CARGA DA URNA ELETRÔNICA
Instituição proponente (se aplicável)
Responsável ALINE BARBOSA DA SILVA FERREIRA
Resumo do plano (máximo de 120 caracteres) Invadir a mídia de carga da Urna Eletrônica, fazendo a limitação de votos aos candidatos daquela seção.
Sistemas a serem testados

Softwares

(X) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
(X) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
(X) Sistema de Apuração (SA)
(X) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

(X) Geração de mídias
(X) Carga da urna eletrônica
(X) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

2 – Fundamentação teórica:

3 – Precondições para o teste: Não tenho uma precondição para realizar o teste.

4 – Escopo – Superfície de ataque:

5 – Janela de atuação simulada do atacante:

6 – Pontos de intervenção:

7 – Passos a serem realizados:

8 – Materiais necessários (fornecidos pelo TSE):

9 – Possíveis resultados e impacto:

10 – Rastreabilidade:

11 – Solução proposta: Assim que realizar o teste apresento minha proposta, se realmente encontrar alguma vulnerabilidade.

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Sigilo e Proteção do Voto: Fortaleza Magnética e Defesa Eletroacústica para a Democracia

Instituição proponente (se aplicável)

Responsável

DIEGO FERRY TORRENT

gov.br Documento assinado digitalmente
DIEGO FERRY TORRENT
Data: 27/10/2023 23:22:32-0300
Verifique em https://validar.iti.gov.br

Resumo do plano (máximo de 120 caracteres)

Resiliência cibernética abordando magnetismo, acústica, ultrassom e escudo faraday saltando a segurança Air-Gapped.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(X) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(X) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(X) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(X) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

Sigilo e Proteção do Voto: Fortaleza Magnética e Defesa Eletroacústica para a Democracia

Resumo: Resiliência cibernética abordando magnetismo, acústica, ultrassom e escudo faraday saltando a segurança Air-Gapped.

Data: 27/10/2023

Autor: Diego Ferry Torrent

linkedin.com/in/dft

1. Descrição Geral do Plano:

Este plano de teste tem como objetivo avaliar e aprimorar a resiliência cibernética dos dispositivos eletrônicos de votação utilizados em processos eleitorais, considerando um ambiente onde os terminais de votação são air-gapped (medida de segurança em que é realizado o isolamento do dispositivo do contato com redes externas), mas não são audio-gapped e não estão contidos em uma gaiola Faraday. Além disso, os testes incluirão a avaliação da proteção contra a extração de dados por canais de áudio (incluindo sons de ultrassom) e a extração de dados por EMR (Emanações Eletromagnéticas) produzidas pelo barramento de memória RAM.

2. Fundamentação Teórica:

A resiliência cibernética é a capacidade de um sistema resistir, se recuperar e adaptar-se a ameaças cibernéticas. Em um ambiente de votação, é crucial garantir a integridade e a confiabilidade dos sistemas eletrônicos, mesmo quando há riscos adicionais devido à falta de isolamento de áudio, à presença de ventoinhas suscetíveis ao fansmitter, falta de gaiola Faraday e à ameaça de extração de dados por canais de áudio, incluindo sons de ultrassom e EMR (Eletromagnetic Radiation) gerada através do barramento de memória RAM.

Portanto, é imperativo conduzir testes de segurança que abranjam essas áreas de risco e vulnerabilidade. Os resultados desses testes não apenas identificarão vulnerabilidades, mas também permitirão a implementação de medidas corretivas específicas para mitigar as ameaças relacionadas a canais de áudio não seguros e exposição à EMR, melhorando a resiliência cibernética dos dispositivos eletrônicos de votação em um ambiente desafiador.

2.1. Resiliência Cibernética em Ambientes de Votação:

Em um ambiente de votação eletrônica, a resiliência cibernética desempenha um papel crítico na proteção dos sistemas e na garantia da integridade do processo eleitoral. A resiliência cibernética refere-se à capacidade dos sistemas de votação eletrônica de resistir, se recuperar e se adaptar a ameaças cibernéticas e físicas, garantindo que o resultado das eleições seja preciso e confiável.

2.2. Isolamento de Áudio e Canais de Áudio Não Seguros:

Um desafio significativo em dispositivos eletrônicos de votação é a ausência de isolamento de áudio, tornando-os vulneráveis a ataques de canais de áudio não seguros. Através de microfones ou sensores, um atacante pode tentar extrair dados transmitidos por meio de sons de ultrassom ou outras frequências inaudíveis para os seres humanos. Isso representa uma ameaça à integridade dos dados de votação e à privacidade do eleitor.

2.3. Extração de Dados por EMR (Eletromagnetic Radiation):

Dispositivos eletrônicos podem gerar EMR, que pode ser explorada por um atacante para extrair informações confidenciais, incluindo dados armazenados no barramento de memória RAM. A exposição a EMR não intencional pode permitir que um atacante acesse dados de votação ou informações críticas de configuração, comprometendo a segurança do sistema eletrônico de votação.

A formação de uma onda portadora de informações a partir da radiação eletromagnética (EMR) gerada pelo barramento de memória RAM é um conceito complexo e pouco comum. EMR refere-se à radiação eletromagnética, que inclui uma ampla gama de frequências, desde ondas de rádio até raios X e raios gama.

Os barramentos de memória RAM em computadores não são normalmente projetados para produzir EMR de forma intencional. No entanto, podem ocorrer emissões de EMR devido ao funcionamento normal dos componentes eletrônicos, especialmente quando há variações rápidas de corrente elétrica.

Essas emissões acidentais de EMR podem ser exploradas em cenários de segurança cibernética por meio de ataques de side-channel (canal lateral), que envolvem a observação de radiação eletromagnética ou outras formas de vazamento de informações para inferir o comportamento de um sistema. Isso é conhecido como "análise de canal lateral" e é uma técnica usada em cibersegurança para obter informações não autorizadas de um sistema, como uma chave de criptografia.

No entanto, a formação intencional de uma onda portadora de informações usando EMR gerada pelo barramento de memória RAM, especialmente para fins de comunicação de dados, não é uma aplicação comum ou convencional. O design de sistemas de comunicação geralmente envolve a geração controlada de ondas portadoras e modulação de sinal para transmitir informações de forma confiável.

2.4. Importância da Resiliência Contra Canais Não Convencionais:

A resiliência cibernética em dispositivos de votação eletrônica deve abranger a proteção contra ameaças tradicionais, como malware e ataques de negação de serviço, bem como ameaças não convencionais, como canais de áudio não seguros e a extração de dados por meio de EMR. A falta de isolamento de áudio e medidas de proteção insuficientes contra EMR representam desafios críticos que precisam ser abordados para garantir a integridade do processo eleitoral.

3. Precondições para o Teste:

- Autorização legal para realizar os testes nos dispositivos de votação.
- Acesso aos dispositivos de votação a serem testados.
- Especialistas em segurança cibernética para conduzir os testes.
- Backup dos dados de votação e sistemas de contingência em caso de falhas.

4. Escopo - Superfície de Ataque:

O escopo dos testes abrange os dispositivos de votação eletrônica, incluindo hardware, software, sistemas de comunicação e infraestrutura de suporte. Os pontos críticos incluem a integridade e confidencialidade dos votos, autenticação, criptografia e a resistência a ameaças como malware e manipulações físicas. Além disso, considera os riscos adicionais de ataques que podem explorar a falta de isolamento de áudio, incluindo sons de ultrassom, presença de ventoinhas suscetíveis ao fansmitter e a extração de dados por EMR produzidas pelo barramento de memória RAM.

O escopo dos testes abrange os dispositivos de votação eletrônica, levando em consideração a presença de diversos canais de ataque, incluindo:

- Falta de Isolamento de Áudio: Os testes avaliarão a vulnerabilidade do sistema de votação à extração de dados através de canais de áudio, incluindo a exploração de sons de ultrassom e frequências inaudíveis.
- Presença de PC Speaker Integrado à Placa Mãe: O PC speaker integrado será examinado quanto à possibilidade de ser explorado como um canal de extração de dados ou como um vetor de ataque.
- Ausência de Faraday Shield: A falta de uma gaiola Faraday será considerada como um fator de risco que permite a exposição dos dispositivos de votação a influências eletromagnéticas externas.
- Presença de Bobinas da Impressora: As bobinas da impressora dentro do dispositivo serão avaliadas quanto à possibilidade de extração de dados via emissões eletromagnéticas, conhecidas como EMR (Eletromagnetic Radiation).
- Ventoinhas Suscetíveis ao Fansmitter: As ventoinhas, mencionadas anteriormente, também serão consideradas como um canal de ataque potencial.

O escopo expandido abrange a análise dos canais de ataque tradicionais, como vulnerabilidades de segurança cibernética, juntamente com a análise de canais de áudio, emissões eletromagnéticas e componentes de hardware específicos, incluindo o PC speaker e as bobinas da impressora.

Isso garante uma avaliação completa da resiliência cibernética dos dispositivos de votação eletrônica em um ambiente onde a segurança é desafiada por diversos vetores de ataque.

5. Janela de Atuação Simulada do Atacante:

Os testes serão conduzidos ao longo de um período representativo, simulando ameaças cibernéticas durante diferentes fases do processo eleitoral, considerando riscos de extração de dados por canais de áudio e EMR.

A Janela de Atuação Simulada do Atacante será projetada para avaliar a resiliência do terminal de votação a ameaças potenciais, considerando os seguintes cenários:

5.1. Ameaças Cibernéticas Convencionais:

Durante a configuração pré-eleitoral: Testes simulando ataques cibernéticos, tentativas de comprometimento da integridade do software e exploração de vulnerabilidades conhecidas. No dia da eleição: Simulação de ataques de negação de serviço (DoS), tentativas de interrupção do processo de votação e manipulação de dados em trânsito.

5.2. Ameaças de Áudio:

Simulação de tentativas de extração de dados através de canais de áudio, incluindo sons de ultra frequência, com o uso de equipamentos sensíveis a áudio e análise do espectro sonoro.

5.3. Ameaças de EMR (Eletromagnetic Radiation):

Avaliação da emissão de EMR gerada pelo barramento de memória RAM durante a operação do terminal de votação. Monitoramento da exposição a radiações eletromagnéticas no ambiente e análise de possíveis tentativas de interceptação de dados via EMR. A Janela de Atuação Simulada do Atacante será projetada para abranger as diferentes fases do processo eleitoral, desde a configuração até a apuração dos resultados, com foco na identificação de vulnerabilidades e na resiliência do sistema contra ameaças cibernéticas tradicionais, canais de áudio e exposição de EMR. É importante que os testes sejam conduzidos de maneira controlada, supervisionados por especialistas em segurança cibernética e equipados com ferramentas de análise de áudio e detecção de EMR para avaliar a capacidade do terminal de votação em resistir a essas ameaças adicionais. A análise dos resultados desses testes ajudará a aprimorar a resiliência cibernética do terminal de votação e garantir a confiabilidade do processo eleitoral.

6. Pontos de Intervenção:

Os pontos de intervenção serão identificados com base na análise dos riscos específicos associados à falta de isolamento de áudio, à exposição a sons de ultrassom e à possibilidade de extração de dados através de EMR geradas pelo barramento de memória RAM, além de outras vulnerabilidades tradicionais. Os principais pontos de intervenção incluem:

a. Isolamento de Áudio:

Avaliação da eficácia do isolamento de áudio existente nos terminais de votação em um ambiente air-gapped. Será verificado se há vazamento acidental de sons de ultrassom ou outros canais de áudio.

Testes de penetração para avaliar a capacidade de um atacante de explorar qualquer vazamento de áudio para comprometer a integridade dos dados.

b. Sons de Ultrassom:

Identificação e avaliação da presença de sons de ultrassom gerados pelos dispositivos de votação. Isso inclui a detecção de fontes potenciais de emissão de ultrassom, como ventoinhas, conversores DC-DC, ou outros componentes eletrônicos suscetíveis.

Testes para determinar se os sons de ultrassom podem ser explorados como um meio de extração de dados ou comprometimento da segurança dos dispositivos.

c. Emissões Eletromagnéticas (EMR):

Análise das emissões eletromagnéticas geradas pelo barramento de memória RAM durante o funcionamento normal dos dispositivos de votação.

Testes para avaliar a capacidade de um atacante de capturar e interpretar as EMR para a extração de dados sensíveis ou informações sobre o processo de votação.

d. Vulnerabilidades Tradicionais:

Além das ameaças específicas mencionadas, serão realizados testes de penetração para avaliar as vulnerabilidades tradicionais dos dispositivos de votação, como vulnerabilidades de software, autenticação, criptografia e falhas físicas.

e. Comunicação com o Exterior:

Verificação da integridade das medidas de segurança que garantem que os dispositivos de votação permaneçam air-gapped, ou seja, isolados de redes externas, incluindo redes de comunicação sem fio e cabeadas.

Avaliação da possibilidade de comunicação não autorizada ou vazamento de informações através de canais não intencionais.

Os pontos de intervenção identificados neste plano de teste abrangem as ameaças potenciais de extração de dados via canais de áudio, sons de ultrassom e EMR do barramento de memória RAM. A análise e os testes em cada um desses pontos são essenciais para garantir a resiliência cibernética dos dispositivos de votação eletrônica em um ambiente complexo de segurança.

7. Passos a Serem Realizados:

- Identificação das vulnerabilidades nos dispositivos de votação, incluindo as relacionadas à falta de isolamento de áudio.
- Testes de penetração para avaliar a resiliência contra ameaças cibernéticas convencionais e a extração de dados por canais de áudio e EMR.
- Avaliação da segurança das ventoinhas e a possibilidade de extração de dados por fansmitter.
- Análise de tráfego e comportamento durante o processo de votação, considerando riscos adicionais de canais de áudio e EMR.

7.1 Testes de Penetração:

7.1.1 Testes de Penetração e Vulnerabilidades Convencionais:

- Identificação de vulnerabilidades convencionais de segurança, como falhas de software e hardware.
- Testes de penetração para avaliar a resiliência contra ameaças cibernéticas tradicionais.
- Avaliação da segurança do barramento de memória RAM e medidas de proteção adicionais.

7.1.2 Avaliação de Canais de Áudio:

- Testes de penetração para verificar a resiliência contra a extração de dados por canais de áudio, incluindo a possibilidade de vazamento de dados por meio de ultrassom (inaudíveis ao ouvido humano).
- Identificação e análise do PC speaker integrado à placa-mãe, que pode ser utilizado como um canal de saída de áudio e possivelmente, através de uma manipulação GPIO convertido em entrada de áudio.
- Monitoramento e gravação de qualquer atividade de áudio anômala que possa indicar vazamento de dados.

7.1.3 Avaliação de EMR (Eletromagnetic Radiation):

- Análise das bobinas da impressora e sua proximidade com o barramento de memória RAM.
- Testes para determinar se as bobinas da impressora geram EMR que possa ser capturada e utilizada para extração de dados.
- Monitoramento de possíveis emissões de EMR durante o processo de votação e a contagem de votos.
- Identificação de vulnerabilidades que permitiriam a extração de dados por emissões eletromagnéticas (EMR) produzidas pelo barramento de memória RAM.

7.1.4 Avaliação da Ausência de Gaiola Faraday:

- Avaliação da exposição do dispositivo terminal de votação a possíveis interferências eletromagnéticas externas.
- Testes para determinar se a ausência de uma gaiola Faraday permite a interceptação de comunicações ou a perturbação do funcionamento normal.

7.1.5 Avaliação da Segurança das Ventoinhas:

- Identificação de ventoinhas no dispositivo de votação.
- Avaliação da segurança das ventoinhas em relação à possibilidade de extração de dados via fansmitter.
- Testes para determinar se as ventoinhas podem ser exploradas para a transmissão de dados não autorizados, incluindo a detecção de qualquer atividade suspeita das ventoinhas.

7.2 Análise de Dados Capturados:

- Processamento e análise dos dados capturados durante os testes, incluindo áudio, EMR e atividade do sistema.
- Identificação de padrões suspeitos ou vazamentos de dados.
- Classificação dos riscos potenciais com base nos resultados obtidos.

7.3 Considerações Adicionais:

- Verificação da presença de bobinas da impressora dentro do dispositivo terminal de votação e sua potencial utilização como meio de extração de dados não autorizados.
- Avaliação da ausência de uma gaiola Faraday e seu possível impacto na exposição a ameaças eletromagnéticas externas.

8. Materiais Necessários (Fornecidos pelo TSE):

- Dispositivos de votação eletrônica.
- Documentação técnica e de configuração.
- Acesso aos ambientes de teste.
- Recursos de rede simulados para testes de ataque.
- Equipamento de análise de áudio, incluindo a capacidade de detectar ultrassom.
- Equipamento de detecção de EMR.

9. Possíveis Resultados e Impacto:

Os resultados dos testes identificarão vulnerabilidades relacionadas à presença de um buzzer na placa mãe (pcspeaker), à falta de isolamento de acústico, ameaças de extração de dados por canais de áudio (incluindo sons de ultrassom) e extração de dados por EMR. O impacto inclui aprimoramento da segurança cibernética empregada no dispositivo, conferindo melhor reputação no processo eleitoral e medidas corretivas específicas para mitigar os riscos adicionais.

a) Extração de Dados por Canais de Áudio (Incluindo Sons de Ultrassom):

Os testes de resiliência cibernética considerarão a possibilidade de extração de dados por canais de áudio, incluindo sons de ultrassom, que podem ser explorados como um meio de vazamento de informações a partir dos terminais de votação. Os possíveis resultados e impactos incluem:

- Vazamento de Dados Sensíveis: A exploração de canais de áudio para vazamento de informações pode resultar na exposição de dados sensíveis, como votos, configurações e chaves de criptografia.
- Risco de Manipulação de Votos: A extração de dados por canais de áudio pode permitir a manipulação não autorizada de votos, comprometendo a integridade do processo eleitoral.
- Dano à Confiança do Eleitorado: A descoberta de vulnerabilidades desse tipo pode minar a confiança do eleitorado no processo de votação eletrônica.

b) Extração de Dados por EMR (Eletromagnetic Radiation):

Os testes também considerarão a possibilidade de extração de dados por meio de EMR geradas pelas atividades no barramento de memória RAM dos dispositivos de votação. Os possíveis resultados e impactos incluem:

- Resultado Possível: Os testes podem revelar que a falta de um escudo Faraday permite a emissão de EMR a partir do barramento de memória RAM, o que possibilita a extração de dados através de técnicas de escuta eletromagnética.

- Impacto Potencial: A extração de dados por meio de EMR é uma ameaça à confidencialidade e à integridade dos dados armazenados na memória RAM dos dispositivos de votação, o que pode comprometer o resultado das eleições e a confiança do público no sistema.

A ausência de um escudo Faraday exacerba a vulnerabilidade do sistema a ameaças eletromagnéticas, tornando-o suscetível a técnicas de escuta eletromagnética, como a interceptação de EMR.

Portanto, os resultados dos testes não apenas identificarão vulnerabilidades tradicionais de segurança cibernética, mas também destacarão a importância de medidas adicionais de proteção, como a implementação de um escudo Faraday, para mitigar as ameaças de extração de dados por canais de áudio e EMR. As ações corretivas propostas devem abordar essas vulnerabilidades específicas para garantir a resiliência cibernética dos dispositivos de votação em questão.

- Exposição de Dados em Tempo Real: A extração de dados por EMR pode permitir a interceptação em tempo real de informações sensíveis durante a votação e processamento dos votos.
- Risco de Espionagem Eleitoral: A capacidade de acessar dados por EMR pode ser explorada por atores maliciosos para espionagem eleitoral e comprometimento do sigilo do voto.
- Potencial para Fraude Eleitoral: A manipulação de votos ou resultados eleitorais pode ocorrer com base na extração de dados por EMR, ameaçando a legitimidade das eleições.

Impacto Geral:

Os resultados acima mencionados podem ter um impacto significativo na confiabilidade e na integridade do processo eleitoral. Além disso, a descoberta de tais vulnerabilidades pode prejudicar a confiança do público nas eleições e nos dispositivos de votação eletrônica.

Portanto, é crucial que as medidas corretivas sejam projetadas para mitigar essas ameaças adicionais e garantir que os dispositivos de votação eletrônica sejam resilientes a ataques de extração de dados por canais de áudio e EMR. Isso incluirá a implementação de contramedidas técnicas, atualizações de software, criptografia de dados em repouso e em trânsito, e treinamento de pessoal para detectar e responder a possíveis ameaças. A segurança do processo eleitoral e a confiança do eleitorado dependem da eficácia dessas medidas.

10. Rastreabilidade:🔗

Os resultados dos testes, as vulnerabilidades identificadas e as ações corretivas propostas serão documentados e rastreados ao longo do tempo, garantindo a melhoria contínua da resiliência cibernética dos dispositivos de votação, incluindo medidas específicas para lidar com os riscos adicionais de canais de áudio e EMR.

11. Solução Proposta:🔗

Com base nos resultados dos testes, será proposta uma série de ações corretivas, que podem incluir atualizações de software, reforço de políticas de segurança e medidas específicas para mitigar os riscos relacionados à falta de isolamento de áudio, canais de áudio (incluindo sons de ultrassom), ventoinhas, componentes mecânicos disponíveis na impressora e EMR do barramento de memória RAM. A solução proposta deve ser implementada de forma a garantir a resiliência cibernética dos dispositivos de votação eletrônica em um ambiente de alto risco.

Este é um esboço revisado do plano de teste, levando em consideração as novas considerações de segurança mencionadas. É importante personalizar o plano de acordo com as especificidades dos dispositivos de votação eletrônica e os requisitos do ambiente de teste. Além disso, é altamente recomendável envolver especialistas em segurança cibernética para a elaboração e execução deste plano de teste.

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

Sigilo e Proteção do Voto: Fortaleza Magnética e Defesa Eletroacústica para a Democracia

Resumo: Resiliência cibernética abordando magnetismo, acústica, ultrassom e escudo faraday saltando a segurança Air-Gapped.

Data: 27/10/2023

Autor: Diego Ferry Torrent

linkedin.com/in/dft

@diegotorrent's 2023 TPS - Justiça Eleitoral Teste público de segurança do Tribunal Superior Eleitoral TSE

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste **Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia**
Instituição proponente (se aplicável)
Érika Maria Rodrigues de Castro
Resumo do plano (máximo de 120 caracteres) Em resumo: trata-se de análise do comportamento da Mídia de Resultado "*pen drive*" da Urna Eletrônica em algumas etapas.
Sistemas a serem testados ***Softwares*** *(X) Software Básico da Urna Eletrônica* *(X) Sistemas Transportador, RecArquivos e InfoArquivos* *(X) Kit JEConnect* *(X) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas* ***Hardwares*** *(X) Transmissão de arquivos* *(X) Carga da urna eletrônica* *(X) Votação* *(X) Teste de integridade (votação paralela)* *(X) Conferência de hash ou validação de assinaturas na urna* *(X) Recuperação de dados na urna eletrônica* *(X) Apuração de votos na urna*

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O presente plano pretende averiguar a segurança jurídica da mídia de resultado "*pen drive*" desde sua inserção na urna eletrônica, o processo de transmissão dos dados até a divulgação destes, com o objetivo de averiguar possíveis vulnerabilidades ou falhas que possam interferir na integridade ou na quebra do sigilo dos votos em uma eleição. No caso de serem identificadas, busca apresentar sugestões de melhoria, mecanismos que fortaleçam a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias em nosso sistema eleitoral.

2 – Fundamentação teórica:

Durante a análise e inspeção do código-fonte, ocorreu uma apresentação da urna eletrônica e seus componentes de hardware, dentre eles o pen drive da mídia de resultado. Neste momento, constata-se que trata-se de uma mídia externa a urna eletrônica que inserida nela, após verificação e por meio do Je-Connect passa a rodar recebendo e transmitindo os arquivos como o Boletim de Urna.

Qualquer alteração interna ou externa nessa mídia pode colocar o processo eleitoral em vulnerabilidade no que tange aos pontos específicos que estão sendo tratados no TPS-2023 quai sejam: adulterar destinação dos votos e quebra de sigilo do voto.

Nesse sentido, os planos de testes relacionados a essa mídia específica se ampara teoricamente nos princípios da confiabilidade, transparência e segurança.

Os votos são registrados em mídias eletrônicas codificadas, dotadas de várias camadas de segurança, os dados das eleições são transmitidos em redes privativas de comunicação, sem o uso da internet.

A própria seção eleitoral, logo quando se encerra a votação, às 17h do dia da eleição. Nesse momento, o presidente da seção eleitoral encerra a coleta de votos e, em seguida, a urna eletrônica imprime o Boletim de Urna (BU).

O "fiscal" do prédio do local da votacão, convocado pelo Justiça Eleitoral, escoltado pela polícia militar leva os pen-drives retirados das urnas após finalizado o horário de votacão ao Cartório Eleitoral da respectiva Zona Eleitoral, a fim de que os dados sejam transmitidos.

Num período anterior ao dia da votação, as urnas são testadas no próprio Cartório Eleitoral. Caso haja algum problema de impressão ou falha no procedimento específico relacionado ao teste, a urna será substituída por outra. Também, no dia de votação, ocorre teste de algumas urnas, as quais foram selecionadas, mediante sorteio prévio.

Antes da eleição, todas as urnas passam por teste de viabilidade nos Cartório Eleitorais. Também há uma determinada quantidade de urnas que, no dia da votação, ficam guardadas no cartório, para substituir àquelas que porventura, precisarem ser substituídas.

Importante salientar que a urna eletrônica não é conectada à rede mundial de computadores, e que os Boletins de Urnas expedido, após finalizada a votação são expostos nos locais de votação, bem como no Cartório Eleitiral para conferência.

Considerando o meu não conhecimento da engenharia e dos caminhos da informação nos chips e placas apresento os Planos de Teste para serem auditados quanto a Mídia de Resultados.

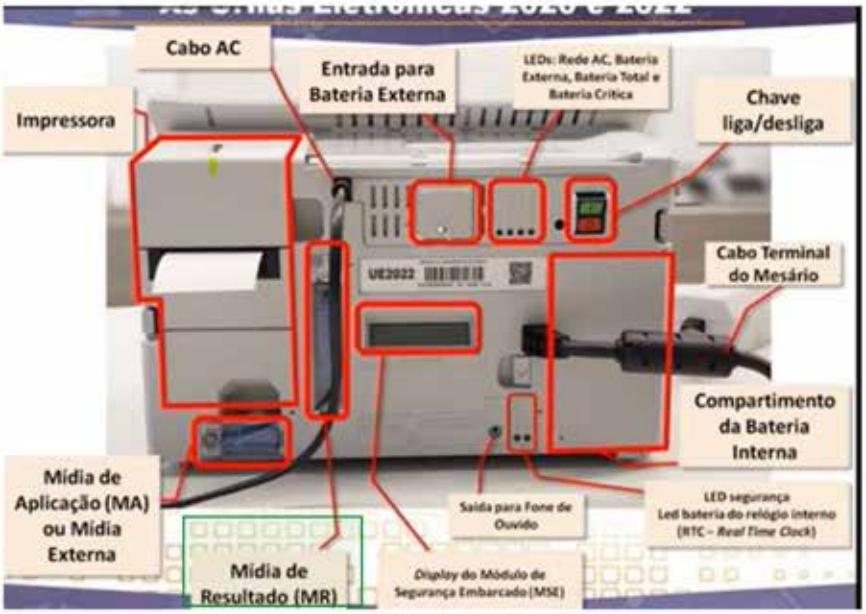
3 – Precondições para o teste:

Presença do Equipamento da Urna Eletrônica com dispositivo de votação de do mesário e internet funcionando, além de um aparelho telefônico e um pendrive "limpo" e separado, sem ser aquele que está ligado a respectiva urna que será testada.

4 – Escopo – Superfície de ataque:

A superfície de ataque estará relacionada a mídia de resultados "pen drive", focado no hardware podendo haver alguma verificação de comportamento do software, se necessário, no momento da execução dos trabalhos de testagem.

5 – Janela de atuação simulada do atacante:



6 – Pontos de intervenção:

Mídia de Resultados – pen drive

7 – Passos a serem realizados:

No Plano de Teste em Quatro Etapas – Mídia de Resultado - pen drive na Urna Eletrônica e fora da Urna Eletrônica

1. Inserção do pen drive de outra urna eletrônica (hipótese de troca), a fim de verificar o seu funcionamento, bem como a inserção de um pen-drive limpo (item 8,b) para fazer a mesma verificação.
   Caso funcione e rode o JE Connect estará verificada uma vulnerabilidade que poderá interferir na alteração da votação.

2. Inserção de um pen drive comun (item 8,b) para verificar o encaixe físico e a necessidade de uma porta física proprietária, com pinagem diferenciada.
   Caso ocorra a inserção de um pen drive que não o relacionado aquela urna específica, estará verificada uma vulnerabilidade que poderá interferir na segurança do processo eleitoral.

3. Encerrada a votação, antes da emissão do Boletim de Urna, testar a possibilidade de inserção de novos dados no pen drive – mídia de resultados. No caso do teste ser positivo, estará verificada uma vulnerabilidade que poderá interferir na adulteração dos dados referentes a adulteração da destinação dos votos e quebra do sigilo do voto

4. Caso, durante o tranporte do pen drive da mídia de resultado com o resultado da votação da respectiva urna para o Cartório Eleitoral, da Zona Eleitoral (Transportador) correpondente, essa mídia seja por um período furtada por indivíduo mal intencionado ele consiga promover alguma adulteração no Registro Digital do Voto (RDV) (software) que embaralha os votos dissociando a ordem em que os votos foram inseridos da ordem em que foram armazenados (excluindo ou inserindo votos) e considerando que o RDV está ligado ao mesmo software que produz o Boletim de Urna (BU), contendo os totais de cada candidato computados pela urna, e devolva novamente nesse trânsito, para seguimento, o ataque poderá comprometer a integridade do Boletim de Urna concomitantemente ao RDV e vice versa e, caso o RDV seja projetado e implementado de forma insegura, poderá permitir a violaçao do sigilo do voto. Essa simulação pretende verificar a vulnerabilidade dos dados serem armazenados em mídia externa, vulnerável quanto a ataques externos e internos que possam violar o sigilo e a ordem de votação.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna Eletrônica com dispositivos do eleitor e do mesário – modelo que será utilizado nas eleições 2024;

a- pen drive da respectiva urna;
b- pen drive limpo, sem qualquer arquivo;
c- telefone;
d- computador com internet.

9 – Possíveis resultados e impacto:
Como resultado pretende-se mostrar a vulnerabilidade da mídia de resultados estar em um equipamento externo e o possível impacto na adulteração da destinação dos votos ou quebra de sigilo de voto.

10 – Rastreabilidade:

Monitorar e identificar cada etapa do fluxo delimitado neste Plano de Teste (item 7),em cada etapa desde a origem dos planos apresentados até sua finalização

11 – Solução proposta:

Como soluções propostas casos as vulnerabilidades sejam comprovadas como sugestão fica a necessidade de elaboração uma porta física proprietária, com pinagem diferenciada e também que sejam

5

feitos estudos que permitam que a mídia de resultado "pen drive" seja totalmente transformada para uma mídia totalmente digital, onde os dados da urna circulem de forma íntegra, segura e sustentável; preservando o sigilo do voto, inviabilizando adulterações de voto ou outras formas de alterar o resultado das urnas, local onde o cidadão no exercício democrático, deposita em seu voto a esperança de um futuro melhor para si e para a sociedade como um todo, fortalecendo a democracia e a participação social.

Diante dos meus conhecimentos obtidos durante a inspeção do código fonte no período de 09/10 a 13/10 do corrente ano esse é o Plano de Testes apresentado, do qual aguardo esperançosamente, deferimento.

Cordialmente,

Érika Maria Rodrigues de Castro
CPF nº 337.507.068-32

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
FRAUS OMNIA CORRUMPIT

Instituição proponente (se aplicável)
Não aplicável

Responsável
Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)
Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do eleitor e com isso alterar a disposição dos votos.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(x) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(x) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

1.1 Apresentação

Considerando que a representação visual do voto é o único instrumento fornecido ao eleitor (além do áudio, para deficientes visuais) como materialização do seu voto, por obvio a hipótese do desvio entre o que é apresentado ao eleitor e o que é efetivamente registrado, é inerente a modelo de DRE. Em que pese a justiça eleitoral afirmar se tratar de um modelo Trust-DRE, isso não elimina de periféricos não associados a cadeia de confiança estejam sob controle de um ator de ameaça. Em suma, não é um modelo verificável ponta-a-ponta.

Portanto, a execução cumulativa de ataques de engenharia social pode dar aparência de veracidade a conteúdos falsos exibidos ao eleitor e associados a outros ataques fazer com que seja apresentado na tela não corresponda ao efetivamente registado no RDV.

1.2 Objetivos

Desconectar o *display* do TE e conectá-lo a um dispositivo para controlá-lo remotamente, substituir a sinalização indicativa da tecla, para que o voto seja digitado de forma incorreta pelo eleitor, todavia o retorno emitido pela tela esteja sobre controle do ator da ameaça. Assim, o voto sufragado não corresponderá a vontade do eleitor, com isso é **alterada a destinação dos votos**.

2 – Fundamentação teórica:

2.1 Análise do Processo eleitoral brasileiro

O sistema eleitoral brasileiro, por utilizar máquinas DRE, não há materialização do voto de forma impressa ou alternativa, para conferência do eleitor ou trilha de auditoria. Dessa forma, a integridade do sistema depende exclusivamente da execução corretas dos *softwares* empregados na votação e que eles sejam confiáveis. Todavia para o eleitor comum, a confirmação dada por ele para a representação visual do voto que aparece no *display* do TE é o voto propriamente dito, não se preocupando com a necessidade imperiosa de correspondência dessa representação com registro digital do voto.

Ainda que possa presumir, não há garantia de que todos os componentes da Urna Eletrônica apresentada ao eleitor estão executando os *Softwares* oficiais. Ademais, com o avanço de tecnologias *wireless*, é possível o controle remoto apenas do display do TE, sem qualquer ligação cabeada. A inicialização da urna no dia da votação ocorre com base na data e horário, não requerendo conferência de assinaturas ou *hashes*, ou ainda validação externa do sistema.

O teste de funcionalidade do *display*, se restringe a perguntar ao operador se a tela está funcionando, não sendo um *Completely Automated Public Turing test to tell Computers and Humans Apart.* Logo, caso o operador seja o ator da ameaça, o teste não terá efeito.

2.2 Controle da urna pela mesa e baixa eficácia dos testes.

A mesa receptora de votação, na condição de autoridade eleitoral, possui acesso livre a urna eletrônica recebida conforme procedimento logístico do Tribunal Regional. Na abertura das atividades e no encerramento da votação, somente os membros da mesa tem seus dados biométricos registrados, ou seja, não há registros das atividades fiscalizadoras nos arquivos gerados pelas urnas eletrônicas. Dessa forma, não há um elo entre a urna

fiscalizada e a que tem seus os seus arquivos enviados ao sistema de totalização. Eventual processo de teste de autenticidade ou integridade, depende de sorteio prévio.

Cumpre ressaltar, que na maioria dos pleitos municipais não tem qualquer urna submetida a teste de integridade ou autenticidade. Lembrando que o eleitorado e número de seções entre os municípios são distintos então um ataque a uma simples urna no município pequeno possui condão de modificar o resultado eleitoral, enquanto em um município maior dependeria de uma escala maior, visto que são pleitos independente. A amostragem da urna submetida a estes testes, não consegue ser sensível o suficiente para detecção a estes níveis, ou seja, eventual sorteio de uma urna nessa localidade seria exceção e não procedimento comum. Ainda, as urnas são sorteadas no dia anterior possibilitando que eventuais sejam abortados.

Em 2022 apenas 641 seções passaram por testes de integridade, que supondo se elas localizem em municípios diferentes, somente 0,11 das 5568 cidades foram submetidas a este tipo de auditoria. Como em 2024, o pleito é municipal essa abordagem desprezaria mais de 4900 pleitos, visto obviamente ataque a eleições em município não teria efeito em outro. (https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/teste-de-integridade-das-eleicoes-2022-comprova-eficiencia-das-urnas). Por exemplo, para obter êxito em fraudar um eleição em Damolândia basta a corrupção de uma seção da 11 existentes, há um baixa possibilidade de uma urna do município ser selecionada e é mais remota ainda a possibilidade que esta seja justamente a fraudada. Ademais, como se trata de municípios pequenos, e bem possível o conhecimento entre os mesários, visto que permanecem de uma eleição para outra, favorecendo possível conluio.

2.3 Simulacros e periféricos sob controle de ator de ameaças

O modelo de UE 2020/22 é distinto dos modelos anteriores, então para os municípios que receberão este modelo, pela primeira vez é plenamente viável aos mesários atribuir qualquer percepção de não conformidade ao novo modelo usado, ofuscando a suspeita. Contudo, o TPS não possibilita o uso de abordagens de engenharia social para realização do ataque pretendido.

Em outra frente, a substituição das indicações das teclas, induziria o eleitor a digitar a tecla errado e consequentemente suspeitar da integridade da urna como alegado em 2018, em que foram registradas reclamações quanto a destinação do voto posteriores aos digitação. Uma modificação da indicação é da tecla correspondente ainda que possa ser observada no comportamento, estes podem ser considerados pela mesa caso ela seja o ator da ameaça.

Assim a eventual substituição da urna oficial por um simulacro de urna, onde o simulacro de urna capturasse as informações e simulasse ao eleitor um processo de votação oficial. Assim os eleitores, teriam a aparência de ter votado e os fiscais de processo ter sido correto, todavia os dados capturados no sistema simulado, inclusive os biométricos, seriam utilizados na urna oficial para inserção de votos arbitrários, enquanto a vontade do eleitor registrado no sistema simulado seria descartada. Nesta hipótese, **não** seria o simulacro que produzira assinatura válida e gerar resultados válidos para a totalização, apenas capturaria informações para serem usadas para inserção de votos espúrios na urna oficial sob controle do ator da ameaça.

3 – Precondições para o teste:

- Urna Eletrônica sem lacre
- Corrupção de membros da mesa receptora.

4 – Escopo – Superfície de ataque:

4.1 Superfície de ataque física

- UE modelo 2020 ou 2022
- Mídias e suprimentos da UE.

4.2 Superfície de ataque digital

- *Software de votação*

4.3Restrições e limitações

- Engenharia social (fora do escopo, não será executado)
- Violação de lacre (fora do escopo, não será executado)

5 – Janela de atuação simulada do atacante:

- Acesso as UE oficial de contingência antes e durante a votação.
- Acesso as mídias e suprimentos da UE antes e durante a votação.

6 – Pontos de intervenção:

- Preparação da seção
- Votação (registro do voto)
- Habilitação dos eleitores
- Fluxo de uso de mídias e suprimentos.

7 – Passos a serem realizados:

As táticas, técnicas e procedimentos envolve, mas não somente, as seguintes etapas:

- Desconectar a *display* do TE.
- Conectar o *display* a dispositivo para controle remoto.
- Inserir entrada de outro display para impedir lançamento de exceção (erro crítico) e a suspensão da execução do sistema.
- Substituir a indicação da tecla do teclado por 789 456 123 ao invés de 123 456 789
- Iniciar a votação
- Emular o comportamento do display da urna oficial, com saída de vídeo enviada remotamente.
- Encerrar a votação e apurar os votos. (os votos no RDV não devem corresponder a vontade do eleitor)
- Caso não obtenha sucesso, ajustar os procedimentos e repetir o teste.

8 – Materiais necessários (fornecidos pelo TSE):

- 1 Urna eletrônica, sem lacre com teclado desmontado para substituição das teclas.
- Display sem funcionamento.
- Mídias e suprimentos da UE.

9 – Possíveis resultados e impacto:

9.1 Resultados pretendido e provável.

Além disso, cumpre salientar que o presente plano de ataque, será executado por ***ethical hackers***, em ambiente controlado e com limitação de escopo, tendo seus resultados reduzidos em comparação cenário em que um ataque real seria executado, inclusive por atacantes internos.

9.2 Análise de risco e do impacto potencial.

Quanto a viabilidade: O ataque é viável, visto que conforme discorrido no item 2 e associado a outros ataques, como de engenharia social e outros, pode ser plenamente aplicado ao cenário real.

Quanto à extensão: A extensão do ataque é a quantidade de seções em que o conteúdo da mídia com resultado for duplicado, e se comparar a diferença RDV alternativo e o RDV oficial para revelar o voto do eleitor que votou posteriormente a duplicação.

Quanto ao risco: O risco do ataque é **médio**, devido ao fato do ataque exigir aparato técnico (média probabilidade de ocorrência) e violar a previsão constitucional de sigilo do voto (alto dano causado ao ativo protegido).

10 – Rastreabilidade:

10.1 Detecção de ataques

Não se vislumbra a possibilidade de detecção do ataque. Além disso, eventual detecção não possui condão de anular os votos registrado, apenas a apuração da responsabilidade penal.

10.2 Técnicas furtivas e Antiforense

Não serão utilizadas técnicas furtivas ou antiforenses pois envolveriam sistemas, ambientes, procedimentos e elementos vedados pelo § 2 do art. 2 do edital de convocação do TPS (e.g. lacre físico)

11 – Solução proposta:

- Implementar *Completely Automated Public Turing test to tell Computers and Humans Apart,* periódicos para impeder que se passe no teste do *display* apenas por decisão do operador. Nesse caso, o operador deve informar o resultado do desafio de CAPTCHA, informado na tela, caso esteja desconectada, dificultará a solução.
- Acesso livre e irrestrito ao código-fonte, ao invés de acesso tutelado e restrito apenas antes da eleição.
- Implementar construção reprodutível (compilação determinística dos binários).

6

Data
Resultado **( ) Aprovado** **( ) Aprovado com ressalvas** **( ) Reprovado**

Justificativa

COMISSÃO REGULADORA

1

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTACÃO E APURACÃO

INFORMAÇÕES COMPLEMETARES

1. **Considerações gerais e explicação complementares a desenvolvimento do plano de teste.**
   - **Trata-se de esboço:** Os planos de teste, trata-se de esboço da pretensão de investigador, está sujeito a adaptações e alterações, ainda que conforme o edital dependa de autorização da comissão reguladora eventuais modificações. Ou seja, tendo sua execução sujeita a condições necessárias e êxito nas etapas propostas.
   - **A etapa de habilitação é distinta da votação:** O processo de habilitação do eleitor é um processo público, sujeito a impugnação, em que visa que somente eleitores hábeis consigam votar e somente 1 vez, ou seja envolve o processo de autenticação (provar quem são) e autorização para votar. Já a votação, implica na manifestação e registro da vontade do eleitor de forma sigilosa. Ou seja, processos que devem ser mantidos isolados sob pena de violar previsão constitucional de sufrágio secreto.
   - **Ordem de habilitação de eleitores**: é uma informação pública que registra os históricos, de forma sequencial, dos eleitores autorizados a votar.
   - **Associação de ataques:** Um ataque bem-sucedido a sistema eletrônico de votação, na maioria de vezes um conjunto de várias técnicas e sempre procuram atacar o elo mais fraco onde seriam invadir subverter menos camadas para obter sucesso.

2. **Considerações gerais e explicação complementares a sugestões de solução propostas**
   - **Ausência de registro da atividade de fiscalização da mesa nos arquivos gerados pela UE:** A urna não captura as digitais dos fiscais, mantendo deliberadamente, que participaram da abertura e encerramento da votação. Logo, possibilitando que uma mesa receptora corrompida consiga produzir votos mesmo que de uma votação espúrias em urna oficial.
   - **Deixar de substituir a assinatura do RDV da urna substituída:** o processo de atualização da assinatura do RDV deixa de fazer sentido em caso de continuidade de votação no processo de contingência. Neste caso, há confusão dos dados necessários para continuidade de votação, visto que apenas dados do processo de habilitação é necessário. A urna de contingência precisa saber se determinado eleitor votou ou não os votos propriamente dito destes eleitores. Não há impedimento, exceto em caso de único voto RDV, destes dados serem encaminhados diretamente a totalização.
   - **Aumentar o número de urnas submetidas a teste:** Ainda que todas as UE executem o mesmo software, são de modelos diferente e para 2024 não ocorrerá apenas uma eleição e sim mais de 5500 eleições simultâneas. Desse modo, a amostragem necessária a identificar não conformidade é diferente para cada pleito. Por isso, o censo usa frações amostrais diferentes para traçar o perfil da população municipal. Logo, a maioria dos municípios tem seus pleitos realizados sem teste de integridade efetuado. Em que pese, a justiça eleitoral, afirmar que ser trata do mesmo sistema, não é razoável presumir que o interesse de alguém em fraudar um pleito municipal se estenda ou esteja ligado ao pleito que teve a urna auditada. Ou seja, testes de integridade, atestam a regularidade amostral apenas dos pleitos que tiveram suas urnas auditadas, visto que a motivação em fraudar um pleito de um município, não contamina ou está vinculada a necessidade de fraudar o pleito em demais municípios. Ainda que se alegue, que são submetidos a mesmos controles de segurança, não estão submetidas a responsabilidades das mesmas pessoas e zonas eleitorais. Isso também torna inviável a participação de eleitores que queiram acompanhar o processo presencialmente, visto que não há como presumir que todos tenham condições orçamentária para tanto.

- **Adoção do processo de construção reprodutível:** A compilação determinística dos binários em que há aplicação de métodos que garantam que uma mesma base de código-fonte, quando compilada sobre os mesmos parâmetros, produzirá sempre os mesmos binários executáveis. É importante haver um mecanismo que agregue confiança de que há correspondência entre um código-fonte aberto para análise e um binário inserido nas urnas, visto que o processo de lacração, depende de confiança na justiça eleitoral, não oferecendo via independente de auditagem.
- **Código-fonte ser aberto e acessado de forma irrestrita**: O segredo não pode ser um requisito do segurança do sistema. O projeto do sistema deve partir do pressuposto que todos os atacantes já conhecem o sistema em seus mínimos detalhes e a segurança deve ser garantida apesar desse conhecimento. (LAGO, 2018) Não há justificativa técnica, para manutenção do acesso tutelado (limitado e com restrições, sob tutela do desenvolvedor, no caso o TSE)
- **Ausência elo entre os relatórios gerados pelas Urna**: Não há vínculo entre os relatórios gerados pela urna (BU, zerésima, etc). Ou seja, como os relatório não estão associados ao *hash* do relatório anterior, não há formação de uma cadeia de confiança distribuída que ajude, inclusive a detectar eventual extensão de um ataque. A encadeamento do *hashes*, em bloco, permitiria a reconstituição histórica dos relatórios gerados, associando BU a zerésima, a zerésima a comprovante de carga, e assim sucessivamente.

LAGO, Lucas. **Disponibilização do código fonte da urna eletrônica**. Centro de Estudos Sociedade e Tecnologia, v. 3, n. 4, 2018. Disponível em: http://www.cest.poli.usp.br/download/disponibilizacao-do-codigo-fonte-da-urna-eletronica Acesso em: 26 out. 2023.

3. Conceitos e definições utilizadas nos planos de testes.

- **Ameaça:** Evento que explore as vulnerabilidades e lhes atribua a causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização.
- **Assinatura digital:** Tecnologia vincula o certificado digital ao documento eletrônico que está sendo assinado, por meio da criptografia assimétrica.
- **Ativo**: Um recurso, processo, produto ou infraestrutura, que uma organização determinou que deve ser protegido.
- **Ator de ameaça**: Um grupo ou agente que causa o incidente malicioso, intencionalmente ou não.
- **Auditoria:** Atividade estruturada para examinar criteriosamente a situação desses controles de segurança da informação e a probabilidade de ameaças às informações críticas sobre as quais atuam esses controles.
- **Autenticidade:** Garantia de que a informação seja proveniente da fonte à qual ela é atribuída
- **Brecha:** Situação quando um mecanismo da segurança pode ser contornado por uma ameaça.
- **Confidencialidade**: Garantia de que os dados são protegidos contra acesso indevido.
- **Conformidade**: Estar de acordo, seguindo e fazendo com que se cumpram leis e regulamentos internos e externos.
- **Controles de Segurança**: Medidas ou contramedidas de segurança para evitar, impedir, detectar, neutralizar ou minimizar os riscos de segurança os ativos.
- **Defesa em profundidade**: Estratégia de adoção de diversas medidas de segurança para proteger a confidencialidade, integridade e disponibilidade da informação.
- **Disponibilidade**: Garantia de que os dados estejam disponíveis a usuários autorizados, quando necessário.
- **Engenharia social**: Arte de enganar e ludibriar pessoas, a fim de obter informações que possam comprometer a segurança da organização.
- ***Ethical Hacking***: Prática de utilizar habilidades computacionais para ajudar as organizações nos testes de segurança para verificar possíveis brechas e vulnerabilidades com permissão do proprietário do sistema ou rede e sem ter intenção de causar danos.
- **Exposição**: Suscetibilidade à perda de um ativo devido a uma ameaça.
- **Falhas**: defeito, saturação ou violação das condições de uso de equipamento ou sistema.
- ***Firmware***: conjunto de instruções operacionais embutidas no *hardware* de dispositivos.
- ***Hardware***: elementos físicos que suportam a execução automática de processos.

- ***Hash***: função criptográfica unidirecional que gera um valor ou diversos valores a partir de uma string de texto usando uma fórmula matemática.
- **Incidente de segurança:** Evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação.
- **Integridade**: Garantia de que os dados não sejam modificados ou destruídos por usuários não autorizados.
- **Invasão**: Situação em que um ator da ameaça tem acesso à infraestrutura de uma organização com a subversão dos controles de segurança e pode causar danos diretamente aos ativos
- **Log**: registro de eventos relevantes em um sistema computacional.
- ***Malware***: Termo genérico que abrange todos os tipos de *softwares* que executam ações maliciosas.
- **Não repúdio**: Proteção contra a alegação por parte de um dos participantes de uma comunicação de que não ocorreu.
- **Procedimentos:** sequência de ações realizadas para executar diferentes passos durante o ciclo de vida do ataque.
- **Risco**: É a possibilidade de que uma ameaça específica explore uma vulnerabilidade específica e cause danos a um ativo.
- ***Software***: programa, rotina ou conjunto de instruções que controlam o funcionamento do processamento de dados.
- **Táticas:** descrição do caminho que o ator de ameaças opera em diferentes fases do ataque.
- **Técnicas:** os meios ou metodologias adotadas para alcançar objetivos.
- **Vulnerabilidade**: É a falta ou a fraqueza com potencial de serem exploradas por ameaças à segurança da informação.
- ***Zero trust***: estratégia de segurança que presumi que nada é confiável e sempre necessita de verificação.

NETO, Pedro Tenório Mascarenhas; ARAÚJO, Wagner Junqueira. **Segurança Da Informação: Uma visão sistêmica para implantação nas organizações.** João Pessoa: UFPB, 2018. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1 . Acesso em 26 out. 2023.

MELO, Sandro Pereira de. **Taxonomia de técnicas furtivas e antiforenses utilizadas em ataques cibernéticos**. 2018. Tese de doutorado. Pontifícia Universidade Católica de São Paulo: São Paulo, 2018. Disponível em: https://tede2.pucsp.br/bitstream/handle/21181/2/Sandro%20Pereira%20de%20Melo.pdf Acesso em 26 out. 2023.

4. Materiais a serem usados na execução do teste

- ***Splitter USB***: cabo USB com 2 Saídas Fêmeas para 1 Saída Macho, ambas suportando conexão de dados.

(imagem meramente ilustrativa)

- ***Splitter DisplayPort***: cabo *displayport* com 2 Saídas Fêmeas para 1 Saída Macho ambas com comunicação bi-direcional.

(imagem meramente ilustrativa)

- **Transmissor de *Display* Sem Fio:** transmissor para envio de sinal ao *display* do TE, sem fio.

(imagem meramente ilustrativa)

- Smartphone para controle remoto do *display* do TE.

(imagem meramente ilustrativa)

5. **Esclarecimentos técnicos do TSE:**
Questão 1: Quais são as especificações técnicas do display do terminal do eleitor, da placa de vídeo e da Unidade de processamento gráfico?
RESPOSTA STI: A tela do terminal do eleitor é um LCD IPS colorido, com resolução de 1280 x 800 pixels. A GPU integra o SoC do processador Intel Atom x5-E3940. Trata-se da GPU Intel HD Graphics 500 (https://www.intel.com/content/www/us/en/products/sku/96485/intel-atom-x5e3940-processor-2m-cache-up-to-1-80-ghz/specifications.html).

Questão 2: A arquitetura de segurança da UE comtempla algum componente específico e dedicado somente a proteção da saída de vídeo ou a de áudio?
RESPOSTA STI: Não.

Questão 3: Qual tipo de conector utilizado para interligação display do terminal eleitor com a motherboard?
RESPOSTA STI: A interface Embedded Display Port (eDP) é utilizada, para mais informações consultar a documentação fornecida.

Questão 4: Qual são os firmwares e drivers, e suas respectivas versões usadas para saída de vídeo e interface gráfica com o eleitor?
RESPOSTA STI: É utilizado o driver de vídeo padrão do Linux, versão 6.1.35, Intel i915.

Questão 5: O perfil operacional Manutenção e inicializador, são capazes de alterar a versão do drives e firmwares utilizados pelo display?
RESPOSTA STI: Não.

Questão 6: O display da urna eletrônica é vinculado a apenas uma UE, ou podem ser intercambiados sem afetar o funcionamento da UE?

RESPOSTA STI: O display do terminal do eleitor da urna eletrônica pode ser intercambiado sem prejuízo ao funcionamento da urna.

Questão 7: A comunicação com a placa de vídeo é criptografada?
RESPOSTA STI: Não. Não há placa de vídeo dedicada. A GPU integra o SoC do processador Intel Atom.

Questão 8: A UE dispõe de componente interno ou dispositivo que indique presença de dispositivos eletrônicos próximos que visem filmar seu display?
RESPOSTA STI: Não.

Questão 9: O RDV é assinado após o registro de cada voto ou apenas a estrutura de dados que consolida os votos registrados?
RESPOSTA STI: O arquivo de RDV é assinado sempre que um novo conjunto de novo é acrescido.

Questão 10: A mídia de votação eventualmente retirada de uma urna defeituosa e inserida tem o RDV assinado por qual urna?
RESPOSTA STI: A mídia de votação contém RDV assinado pela urna que está coletando os votos. Quando ocorre a substituição da urna, o RDV assinado pela urna original passa a ser assinado pela urna substituta.

Questão 11: A Urna eletrônica de contingência é preparada de modo que apenas aceita a mídia de votação da urna defeituosa ou não?
RESPOSTA STI: A urna de contingência é programada para apenas substituir outro equipamento. Ela não é capaz de iniciar uma votação sem os dados provenientes de uma seção eleitoral, uma vez que é preparada sem dados.

Questão 12: Com a geração de mídias da Urna de contingência, ocorre a alteração da tabela de correspondência?
RESPOSTA STI: As urnas de contingência possuem correspondências, as quais são publicadas na véspera do pleito junto com as correspondências das urnas preparadas para seções eleitorais específicas. Quando ocorre a substituição da urna, a correspondência da contingência passa a ser atribuída à seção eleitoral. Essa característica é persistida na urna e na totalização, de modo que a nova correspondência passa a ser a esperada para a seção eleitoral entre diferentes turnos do mesmo processo eleitoral.

Questão 13: A inicialização da urna no dia da votação ocorre com base na data e horário, não requerendo validação por softwares externos, que assine digitalmente e/ou permita aos fiscais o registro de algo que certifique que aqueles dados não são espúrios. Nesse sentido, os mesários de uma determinada seção podem substituir a UE oficial por um simulacro, e inserir votos espúrios na urna oficial, com isso seria inserido no sistema oficiais votos irregulares, os eleitores teriam a sensação de terem votado e haveria dificuldade em identificar a falha já que são os mesário que produzem a ata. Assim, urna eletrônica possui mecanismo de registro de toda cadeia de custodia e de validação externa dos arquivos?
RESPOSTA STI: A hipótese de ataque com uso de simulacro não é factível. Há elementos de segurança que podem ser verificados por eleitores e fiscais (lacres físicos, LED de segurança). Há procedimentos de verificação de assinatura digital realizados na própria seção eleitoral (Teste de Autenticidade, estabelecido pela Resolução TSE nº 23.673/2021, Capítulo VI). Mas o elemento mais forte é a assinatura digital de todos os resultados produzidos pela urna. Há assinatura digital produzido pelo hardware de segurança da urna (chave embarcada em hardware e certificada pelo TSE). Não há como um simulacro produzir uma assinatura válida e gerar resultados válidos para a totalização.

Questão 14: O resumo da zerésima e a zerésima possuíram QR, que podem ser lidos por qualquer cidadão que desejar?
RESPOSTA STI: Esses relatórios não possuem QR Codes. Se for do interesse do cidadão obter uma cópia, basta fotografar o relatório afixado na seção eleitoral.

Questão 15: Há algum mecanismo que permite a assinatura externa dos arquivos, utilizando um software independente e troca de chaves de Diffie-Hellman, pois o uso de chaves criptográficas apenas da urna não impede ataques de alguém que tenha controle de sistema? O uso de outras assinaturas obtidas pelos métodos de troca de chave, necessitaria de chave privada emitida externamente?
RESPOSTA STI: Todos os arquivos da urna são assinados digitalmente. O software da urna é assinado durante a Cerimônia de Lacração e Assinatura Digital dos Sistemas, na qual os arquivos são assinados fora da urna. Há assinaturas para conferência pela própria urna (hardware e software), assim como assinaturas feitas para validação pela fiscalização independente (nesse caso, usando tokens ICP-Brasil). Os arquivos de dados que alimentam a urna (configuração da eleição, candidatos, eleitores, etc.) também são assinados fora da urna, no momento em que são gerados e pelos sistemas responsáveis pela guarda da respectiva informação (Configurador de Eleições, Candidaturas, Cadastro de Eleitores, etc.), com chaves privativas de cada sistema.

Questão 16: Como a Autoridade Certificadora da Ecossistema da Urna não é subordinada a Autoridade Certificadora ICP-BR, o TSE cumpre os requisitos de segurança física e lógica, compatíveis com a atividade de certificação?
RESPOSTA STI: Sim, há controles estritos de segurança física e lógica, com guarda de chaves em dispositivos HSM certificados.

Questão 17: Na troca de arquivos entres os sistemas há encadeamento dos dados por meio de alguma tecnologia de registro distribuído?
RESPOSTA STI: Os arquivos de dados que alimentam as urnas eletrônicas e que são trocados entre os sistemas eleitorais estão descritos no padrão ASN.1, codificados em formato BER e compactados no formato ZIP. Todos os arquivos de dados são assinados digitalmente por meio da biblioteca libharpia (https://sol.sbc.org.br/index.php/sbseg/article/view/21672). Não são aplicadas técnicas de registro distribuído.

Questão 18: Há algum elo entre os relatórios gerados pela urna eletrônica, por meio de encadeamento de blocos (metadados como um número único que referência o bloco, o horário de criação do bloco e um apontador para o hash do bloco anterior, além do próprio hash do bloco.)?
RESPOSTA STI: Os arquivos e relatórios impressos pela urna não são inseridos numa estrutura do tipo blockchain. Todos os produtos da urna são assinados digitalmente, incluindo o uso de chaves privativas para cada equipamento submetidas a uma infraestrutura de chaves públicas certificada. Todos os arquivos e relatórios possuem em seus cabeçalhos metadados, também assinados, que permitem a vinculação dos arquivos e relatórios entre si e com o processo eleitoral.

Questão 19: Quais os requisitos técnicos e os critérios utilizados pelo TSE para definição da versão final dos códigos-fonte dos programas do Sistema eletrônico de votação?
RESPOSTA STI: O ciclo de desenvolvimento do software da urna é de 24 meses, iniciando-se após a Cerimônia de Lacração e terminando na Lacração subsequente. Nesse período todas as evoluções realizadas no sistema são submetidas a intensa bateria de testes por equipes do TSE e dos TREs, incluindo exercícios internos e eleições simuladas junto à população. Integra o ciclo de desenvolvimento do software o próprio Teste Público de Segurança, nas suas etapas de execução e de teste de confirmação das correções. A versão final do software lacrado para uma eleição é fixada às vésperas da Cerimônia, quando da conclusão dos últimos ajustes e testes.

Questão 20: Como Modulo de Segurança Embarcado e outras barreiras de segurança impedira a execução de shellcode com ou sem assinatura digital?
RESPOSTA STI: Todos os arquivos da urna são protegidos por assinatura digital. A execução de binários ou carga de dados só é feita após a validação das assinaturas. No caso de identificação de assinaturas inválidas, a execução de todo o sistema é interrompida. Além disso, todos os dados contidos nos arquivos, inclusive cabeçalhos, são validados antes de serem utilizados. Todo o software desenvolvido pelo TSE é submetido a análise estática e testes, com vistas a identificar previamente bugs que poderiam permitir a execução arbitrária de código. Finalmente, as bibliotecas de software livre também são constantemente atualizadas.

Questão 21: Como a cadeia de segurança e outras barreiras de segurança impede a inserção de instruções arbitrárias por meio de instrumentação dinâmica de binários?
RESPOSTA STI: Um dos elos da cadeia de segurança é validação de assinatura digital feita pelo kernel do Linux sobre qualquer binário executável (driver, biblioteca ou aplicativo). As assinaturas desses binários são geradas na Cerimônia de Lacração. Binários com assinaturas inválidas não são executados e interrompem o funcionamento do kernel. O sistema da urna não possui terminal de comandos ou interpretadores de linguagens de programação ou sistemas de execução de bytecode. Portanto, não é possível produzir software válido para a urna fora da Cerimônia de Lacração, tampouco a utilização de ferramentas de instrumentação dinâmica de binários.

Questão 22: A Aplicação de criptografia sobre os binários e uso de assinaturas digitais no códigos-fontes de interfere em um eventual processo de construção reprodutível (compilação determinística dos binários), visto que atualmente o único elo de confiança entre o código-fonte auditado e os binários executáveis é a cerimônia de lacração (onde não é conferido, a grande quantidade de linhas da versão final, visto que a alteração de algumas linhas pode ser feita minutos antes).
RESPOSTA STI: A aplicação de técnicas de criptografia e assinatura digital não deve ser enxergada como um impeditivo a um trabalho de análise forense do sistema, tampouco ao emprego de construção reprodutível. Na verdade, tratam-se de mecanismos de segurança imprescindíveis à garantia da lisura do processo eleitoral. O conjunto de software do Ecossistema da Urna já conta com a aplicação de técnicas de construção reprodutível. Futuramente, a Cerimônia de Lacração terá alterações em seus procedimentos para permitir a evidenciação dessa reprodutibilidade. Ademais, destaca-se que não há alterações feitas "minutos antes" no sistema e que modificações que venham a ser feitas no código compilado são sempre aplicadas ao ambiente de inspeção, com a possibilidade de comparação das versões alteradas.

Questão 23: O Verificador Pré/Pós-Eleição e o Verificador de integridade e autenticidade de sistemas eleitorais dispõe de funcionalidade forenses de duplicação forense?
RESPOSTA STI: Não. A duplicação forense pode ser feita fora da urna, por software independente do próprio perito.

Questão 24: No ecossistema da urna eletrônica, há um software de clonagem, duplicação ou extração de dados para reconstituição e análise forense?
RESPOSTA STI: Não. A duplicação forense pode ser feita fora da urna, por software independente do próprio perito.

Questão 25: A urna registra o Snapshot (registro do estado de um sistema) do momento antes votação para posterior reconstituição forense?
RESPOSTA STI: A urna não mantém registros históricos de estado do sistema, uma vez que tal mecanismo poderia configurar uma fragilização do sigilo da votação (ao menos para o último eleitor a votar). Os votos e demais registros feitos pela urna são realizados em operações atômicas, com técnicas de tolerância a falhas e duplicação de dados entre e mídia interna e a externa (mídia de votação).

Questão 26: O TSE disponibiliza a cópia da arquivos binários disponíveis, após a eleição para análise forense ou auditoria pelas entidades fiscalizadoras?
De acordo com os artigos 51, 52 e 84 da Resolução TSE nº 23.673/2021, procedimentos de fiscalização e auditoria não previstos podem ser realizados se autorizados pelo Presidente do TSE ou TRE.

Questão 27: Os Softwares do ecossistema da Urna impedem dumps de hibernação, dumps de crash e analisar paginação de memória?
RESPOSTA STI: O kernel Linux configurado para a urna possui "crash dump" desabilitado. O sistema da urna não faz hibernação e não há demanda por memória no sistema que exija a criação de um "swapfile".

PEDIDO DE ESCLARECIMENTO 16
Primeiramente, é preciso esclarecer a dinâmica da exposição técnica realizada no último dia 18/10. Na ocasião, foi demonstrado o funcionamento do software da urna, em especial quanto aos procedimentos de carga, autoteste e votação. Em seguida, a urna foi desmontada para a exposição de seus componentes internos, dentre eles a placa-mãe. Essa exposição técnica foi feita para um público com níveis de conhecimento bem diversos e, por isso, se fez necessário encontrar uma abordagem capaz de alcançar a todos os espectadores. Ainda assim, todos os investigadores tiveram a oportunidade de solicitar aprofundamento das explicações apresentadas por meio de perguntas, as quais foram prontamente respondidas. Portanto, o não aprofundamento em qualquer tema foi uma opção do próprio investigador. O software da urna, em especial o aplicativo Vota, detecta a ausência da tela do eleitor (assim como da tela do mesário), o que provoca o lançamento de exceção (erro crítico) e a suspensão da execução do sistema. Todas as exceções são exibidas na tela do eleitor, acompanhadas de emissão de sinal sonoro (SOS em código Morse) e registro em log. A comunicação com a tela do terminal do eleitor se dá por meio de conexão Embedded Display Port padrão, sem qualquer tipo de cifração. Não há erros de montagem das mídias de aplicação (MA) ou interna (MI) sendo ignorados. Contudo, uma falha na montagem da mídia de resultados (MR) não impede o início do processo de votação. Trata-se de decisão de projeto com o intuito de priorizar a correta coleta de votos no dia da eleição, ainda que seja preciso recorrer a um procedimento de recuperação de dados ao final do dia para a extração dos resultados produzidos pela urna. O aplicativo VPP se presta a apoiar processos de auditoria da urna, mas não deve ser considerado o único instrumento a ser usado por um auditor, na medida em que é possível fazer uma análise forense das mídias da urna fora do equipamento. É importante destacar que o VPP é um software lacrado, com seu código aberto para inspeção e protegido por assinatura digital gerada na Cerimônia de Lacração. Portanto, qualquer tentativa de substituição ou inserção de comportamento malicioso seria identificada. O aplicativo de verificação externa de autenticidade (AVPart) não é mantido na mídia interna da urna. A urna mantém apenas assinaturas digitais esperadas dos aplicativos conhecidos (cada entidade fiscalizadora pode produzir o seu próprio aplicativo a apresentá-lo ao TSE). Por estar protegido por assinatura digital e também estar aberto na Cerimônia de Lacração, qualquer tentativa de substituição ou inserção de comportamento malicioso no AVPart seria identificada. A mídia de resultados (MR) deve estar formatada para receber os resultados produzidos pela urna ao final da votação.
O software da urna, em especial o aplicativo Vota, detecta a ausência ou retirada da mídia de votação (MV) – nome dado à mídia de aplicação quando esta tem a função de área de backup da votação. Caso a MV seja retirada durante a execução do Vota, ocorre o lançamento de exceção (erro crítico) e a suspensão da execução do sistema. A urna pode ser religada com a mesma mídia para prosseguir a votação normalmente. Outra MV pode ser utilizada, desde que não tenha sido utilizada por outra urna. Não é possível prosseguir com a votação sem uma MV. A urna foi projetada para que os seus periféricos sejam intercambiáveis entre unidades do mesmo modelo. Assim, independente da gestão do processo de manutenção das urnas, o teclado do eleitor que originalmente foi de uma urna poderia ser remontado em outro equipamento, por exemplo.
PEDIDO DE ESCLARECIMENTO 23
O processo de inseminação da chave kernel, embarcada no MSE, está descrito em https://sol.sbc.org.br/index.php/wte/article/view/14039 . A chave de kernel é utilizada para a

decifração da chave de SO, que é a efetivamente usada na decifração do kernel do Linux. Os arquivos ASN.1 são utilizados para a troca de dados entre os sistemas eleitorais. Eles não são cifrados. Apenas os dados biométricos dos eleitores contidos no arquivo de eleitores é protegido por criprografia assimétrica provida pela libharpia (https://sol.sbc.org.br/index.php/sbseg/article/view/21672). A mídia de resultados (MR) utilizada para a gravação de resultados é sempre formatada, não contendo qualquer arquivo. Contudo, para o 2º turno a MR pode conter os dados dos candidatos que estão disputando a eleição, uma vez que a mesma mídia é utilizada para informar os novos dados para a urna. Uma falha na montagem da mídia de resultados (MR) não impede o início do processo de votação. Trata-se de decisão de projeto com o intuito de priorizar a correta coleta de votos no dia da eleição, ainda que seja preciso recorrer a um procedimento de recuperação de dados ao final do dia para a extração dos resultados produzidos pela urna. Quando uma urna de contingência é utilizada para a substituição de uma urna original de uma seção, ela assume em definitivo os dados daquela seção eleitoral e não pode mais ser utilizada para substituir outras urnas. O objetivo da fase de inspeção de código é a análise do código-fonte. Entende-se que essa análise é suficiente para a elaboração de planos de teste de qualidade. Ademais, permitir análise dinâmica do software significaria também permitir a alteração do código-fonte, o que não é aceitável no ambiente de inspeção. Durante o desenvolvimento do conjunto de software do Ecossistema da Urna são utilizadas as ferramentas GDB, Valgrind, WinDBG e x64dbg. Para o conjunto de software do Ecossistema da Urna, é adotada uma variação do padrão de codificação do Google para C++, conforme pode ser verificado nos arquivos .clang-format que acompanham o código-fonte. O código-fonte é permanentemente formatado automaticamente com apoio da ferramenta clang-format.

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

NIHIL AUTEM ABSCONDITUM EST, QUOD NON REVELETUR

Instituição proponente (se aplicável)

Não aplicável

Responsável

Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)

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 habilitados violar o sigilo do voto.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(x) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(x) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
(x) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

1.1 Apresentação

O fluxo de uso das mídias de votação e o seu intercambio durante eventual ocorrência no decorrer da votação pode se tornar vetor de ataque. A leitura recorrente do conteúdo de *backup* para a partir das suas comparações e relacionamento com a ordem de votação é capaz de revelar os votos registrados. Dessa maneira, o sistema deve ser capaz de impedir tal prática.

A clonagem do arquivo da mídia de votação, quer seja pelo uso de *splitter* quer pela clonagem de binários tem, em tese, condão para fragilizar o sigilo do voto dado que o processo de contingência faz uso do RDV gerado, mesmo esse não se tratando de informação útil para habilitação do eleitor.

1.2 Objetivos

Criar fluxo alternativo de armazenamento do registro digital do voto para possibilitar a comparação entre o armazenamento principal e o alternativo, e pela diferença entre os arquivos revelar o voto registrado e com isso **fragilizar o sigilo do voto.**

2 – Fundamentação teórica:

2.1 Análise do Processo Eleitoral brasileiro

O artigo 312 da Lei nº 4.737/1965 (Código Eleitoral) tipifica como crime "violar ou tentar violar o sigilo do voto". Dessa forma, não estipula a forma que a conduta deva ser praticada para configuração do crime. Já o § 1º do art. 59 da Lei nº 9.504 diz que "A votação eletrônica será feita no número do candidato ou da legenda partidária, devendo o nome e fotografia do candidato e o nome do partido ou a legenda partidária aparecer no painel da urna eletrônica, com a expressão designadora do cargo disputado no masculino ou feminino, conforme o caso." Este, porém não é o voto propriamente dito visto que o § 4° do mesmo artigo com redação dada pela Lei nº 10.740, de 2003) diz que "A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor."

2.2 Funcionamento do mídias de votação

Os votos e demais registros feitos pela urna são realizados em operações atômicas, com técnicas de tolerância a falhas e duplicação de dados entre e mídia interna e a externa (mídia de votação). Essas mídias, que são inseridas na UE, também usadas para carga, *backup* e envio de dados para totalização. A mídia de resultados (MR) recebe os resultados produzidos pela urna ao final da votação. Já a mídia de votação (MV) que é quando mídia de aplicação tem a função de área de backup da votação, é usada no processo de contingência. Quando ocorre a substituição da urna, o RDV assinado pela urna original passa a ser assinado pela urna substituta.

Caso a MV seja retirada durante a execução do Vota, ocorre o lançamento de exceção (erro crítico) e a suspensão da execução do sistema. A urna pode ser religada com a mesma mídia para prosseguir a votação normalmente, situação em a mídia em questão poderia ser clonada, visto que somente caso tenha sido utilizada por outra urna, não poderia ser utilizada. Estes *flashs cards* (mídias) utilizados durante a votação, possuem

apenas a lacre como barreira física a livre manipulação pelos atores de ameaças. A clonagem desse arquivo pode ocorrer de diversas formas.

Nesse contexto, a urna deve repelir uso de replicadores de sinais que possibilitariam a gravação deste conteúdo em mídia alternativa sob controle do ator da ameaça. Como um Splitter USB é um adaptador com uma entrada e muitas saídas, tendo como função replicar a conexão de dados de uma fonte para duas ou mais saídas, é uma opção disponível além da cópia binaria para outra mídia.

O plano Sequenciador de Votos do investigador João Felipe de Souza, já obteve sucesso no TPS 2016 em usar cópia das mídias, para revelar votos. Deste modo, é plenamente factível o presente plano pois em alusão a este teste o presente também visa gravar sequencialmente os arquivos do RDV e relacioná-los com o registro de comparecimento.

3 – Precondições para o teste:

- UE oficial e duas de contingência, conforme tabela de correspondência, sem lacres.
- Acesso a mídias e suprimentos da UE.

4 – Escopo – Superfície de ataque:

4.1 Superfície de ataque física

- UE modelo 2020 ou 2022
- Midias e suprimentos da UE.

4.2 Superfície de ataque digital

- *Software de votação*

4.3Restrições e limitações

- Engenharia social (fora do escopo, não será executado)
- Violação de lacre (fora do escopo, não será executado)

5 – Janela de atuação simulada do atacante:

- Acesso as UE oficial e de contingência antes e durante a votação.
- Acesso as mídias e suprimentos da UE antes e durante a votação.

6 – Pontos de intervenção:

- Habilitação do eleitor
- Votação (registro do voto)
- Apuração dos votos,
- Processo de contingência,
- Fluxo de uso das mídias e suprimentos da UE

7 – Passos a serem realizados:

As táticas, técnicas e procedimentos envolve, mas não somente, as seguintes etapas:

- Inserir cabo *splitter USB,* na saída para mídia e acoplar 2 mídias.
- Iniciar a votação.
- Retirar uma mídia e colocar na urna de contingência.
- Tentar variações procedimentos, alternado a ordem de inserção e duplicação da mídia de resultados.,
- Simultaneamente, anotar o fluxo de habilitação
- Habilitar mais um eleitor na UE oficial e após seu voto encerrar a votação em ambas as urnas.

- Comparar os resultados com entre a votação oficial e a advinda da mídia duplicada na Urna de contingência.
- Caso não obtenha sucesso, repetir os passos usando um laptop para duplicação do conteúdo da mídia de votação
- Caso não obtenha sucesso, ajustar os procedimentos e repetir o teste.

Para frustrar eventual registro de log, alguns procedimentos de retirada de mídia, poderão ser executados com a urna desligada.

8 – Materiais necessários (fornecidos pelo TSE):

- 2 Urnas eletrônicas
- Mídias e suprimentos da UE.

9 – Possíveis resultados e impacto:

9.1 Resultados pretendido e provável.

Espera-se que o plano de ataque, se executado com sucesso, consiga violar o sigilo do voto sem ser detectado, por meio da simples comparação entres RDV, um oficial e outro alternativo provindo do mesmo RDV sem o voto que se destina a revelar.

9.2 Análise de risco e do impacto potencial.

Quanto a viabilidade: O ataque é viável, visto que conforme discorrido no item 2 e associado a outros ataques, como de engenharia social e outros, pode ser plenamente aplicado ao cenário real.

Quanto à extensão: A extensão do ataque é a quantidade de seções em que o conteúdo da mídia com resultado for duplicado, e se comparar a diferença RDV alternativo e o RDV oficial para revelar o voto do eleitor que votou posteriormente a duplicação.

Quanto ao risco: O risco do ataque é **altíssimo**, devido ao fato do ataque ser facilmente reproduzível, sem uso de tecnologias ou ferramentas complexas (alta probabilidade de ocorrência) e violar a previsão constitucional de sigilo do voto (alto dano causado ao ativo protegido).

10 – Rastreabilidade:

10.1 Detecção de ataques

Não se vislumbra a possibilidade de detecção do ataque e caso seja encontrado registros de logs que estes não sejam associados a esta tática.

Além disso, cumpre salientar que o presente plano de ataque, será executado por ***ethical hackers***, em ambiente controlado e com limitação de escopo, tendo seus resultados reduzidos em comparação ao cenário em que um ataque real seria executado, inclusive por atacantes internos.

10.2 Técnicas furtivas e Antiforense

Execução de alguns procedimentos com a UE desligada para frustrar registro de log. Além disso, não serão utilizadas técnicas furtivas ou antiforenses pois envolveriam sistemas, ambientes, procedimentos e elementos vedados pelo § 2 do art. 2 do edital de convocação do TPS (e.g. lacre físico)

11 – Solução proposta:

- Levantar exceção (erro crítico) em caso de conexão com mais de uma mídia de votação.
- Manter os RDV da urna substituída segregado do RDV da urna de contingência e deixar substituir a assinatura do RDV da urna anterior pela assinatura da urna de contingência. Esta informação é

desnecessária para continuidade de votação apenas informação do processo de habilitação de eleitor e não os votos propriamente ditos são usados para continuidade da votação.

6

Data
Resultado **( ) Aprovado** **( ) Aprovado com ressalvas** **( ) Reprovado**

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
QUI DUPLICAT, VIDERE SUFFRAGIO POTEST

Instituição proponente (se aplicável)
Não aplicável

Responsável
Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)
Violar 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.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(x) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

1.1 Apresentação

Partindo da perspectiva de que é necessário apenas obter o conteúdo da saída de vídeo para visualizar como determinado eleitor votou, visto que a representação visual do voto é o único instrumento fornecido ao eleitor como materialização do seu voto, temos que a saída de vídeos e o display do terminal do eleitor é um alvo de potencial ataque que vislumbre saber quem votou em quem.

Assim, se houver uma segunda tela, cuja o eleitor e os fiscais não tenham conhecimento, esta pode ser livremente gravada pelo ator de ameaça, em alusão aos já documentados casos de *selfie* com a urna. A simples filmagem viola o segredo do voto.

1.2 Objetivos

O teste visa, obter, gravar ou espelhar a saída de vídeo do display do terminal do eleitor. Relacionar os votos apresentados no display com a eleitor habilitado que o digitou por meio da ordem de votação, observada na seção eleitoral e com isso **fragilizar o sigilo do voto**.

2 – Fundamentação teórica:

2.1 Análise do Processo Eleitoral Brasileiro

O sistema eleitoral adotado no Brasil, é amplamente suscetível a violação do sigilo do voto, visto que não há previsão de uso de detectores de metais para que o eleitor adentre a cabina de votação. A votação e o deposito (registro) de voto ocorre em espaço reservado onde o eleitor pode adentrar com uso de dispositivo eletrônico pessoal, apenas informando aos mesários que não está em posse deste. Logo, a simples filmagem do display do terminal do eleitor da urna comprova o voto em determinado candidato e fragiliza o sigilo do voto.

A votação em máquinas DRE, como a Urna Eletrônica brasileira, não permite o descarte de voto e o registro oficial do voto ocorre em espaço reservado ao contrário de outros modelos (e.g. o voto em cédula de papel apenas o preenchimento ocorre em ambiente reservado e o deposito de voto é feito diante de todos). Assim, a filmagem da tela demostrando o preenchimento e a confirmação do voto é suficiente para atentar contra o caput do art.14 da Constituição Federal, pois após isso, o software de votação, registra o RDV sem necessitar de qualquer outro procedimento.

O artigo 312 da Lei nº 4.737/1965 (Código Eleitoral) tipifica como crime "violar ou tentar violar o sigilo do voto". Dessa forma, não estipula a forma que a conduta deva ser praticada para configuração do crime. Já o § 1º do art. 59 da Lei nº 9.504 diz que "A votação eletrônica será feita no número do candidato ou da legenda partidária, devendo o nome e fotografia do candidato e o nome do partido ou a legenda partidária aparecer no painel da urna eletrônica, com a expressão designadora do cargo disputado no masculino ou feminino, conforme o caso." Este, porém não é o voto propriamente dito visto que o § 4° do mesmo artigo com redação dada pela Lei nº 10.740, de 2003) diz que "A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor."

Com isso temos uma representação visual, que mostra ao eleitor a quem ele está votando é também deve ser mantida em segredo. Qualquer registro, gravação ou espelhamento, por mínimo que seja, tem o condão de transgredir o sigilo do voto e permitir a coação eleitoral e o voto de cabresto. O simples fato de o voto ser processado eletronicamente não elimina a possibilidade de haver um voto de cabresto moderno, aliás por vezes facilita principalmente na ausência de possibilidade de descarte de votos preenchidos anteriormente e deposito de forma pública do voto preenchido secretamente.

Ademais, no plano de teste 20 do TPS 2021, os investigadores Ian Martinez Zimmermann e Carlos Alberto da Silva, tiveram êxito em armazenar a representação em áudio do voto em alguma mídia para posterior recuperação e identificação da sequência da votação de uma urna eletrônica, por meio de dispositivo acoplado. Isto corrobora a **viabilidade** e da pretensão do presente teste e sua **aplicação** em um cenário real.

2.2 O display do Terminal do Eleitor

A tela do terminal do eleitor é um LCD IPS colorido, com resolução de 1280 x 800 pixels. A GPU integra o SoC do processador Intel Atom x5-E3940. Trata-se da GPU Intel HD *Graphics* 500. A urna utiliza o driver de vídeo padrão do Linux, versão 6.1.35, Intel i915, para gerenciamento da saída de vídeo. A *interface* *Embedded Display Port (eDP)* é utilizada para interligação display do terminal eleitor com a *motherboard.*

A arquitetura de segurança da UE **não** comtempla nenhum componente específico e dedicado somente a proteção da saída de vídeo. Como não há placa de vídeo dedicada, não há comunicação criptografada. Nesse sentido, pelo fato display do terminal do eleitor da urna eletrônica pode ser intercambiado sem prejuízo ao funcionamento da urna, é factível usar o display com vetor de ataque.

O *splitter* é um adaptador com uma entrada e muitas saídas, tendo como função replicar o sinal de vídeo de uma fonte para duas ou mais saídas. Então, surge a hipótese que eventual conexão de mais de um *display*, por meio de um *splitter* não levantaria exceção (erro crítico), com grande possibilidade de êxito pelas características de intercambialidade dos periféricos da UE e a ausência de cifração da comunicação.

Tendo em vista, que em muitos casos a UE modelo 2020/22 será usada pela primeira vez é plenamente viável aos mesários atribuir qualquer percepção de não conformidade visual ao novo modelo usado, ofuscando a suspeita. Contudo, o TPS não possibilita o uso de abordagens de engenharia social para realização do ataque pretendido.

3 – Precondições para o teste:

- Urna Eletrônica sem lacre
- Corrupção de pessoas envolvida nos processos citados

4 – Escopo – Superfície de ataque:

4.1 Superfície de ataque física

- UE modelo 2020 ou 2022
- *Display* do TE.

4.2 Superfície de ataque digital

- *Firmware* da *display* do TE

4.3 Restrições e limitações

- Violação de lacre (fora do escopo, não será executado)

5 – Janela de atuação simulada do atacante:

- Acesso a urna eletrônica antes do início da votação.
- Acoplagem de outro display para gravação do conteúdo.

6 – Pontos de intervenção:

- Preparação da seção
- Votação (registro do voto)
- Habilitação dos eleitores
- Apuração dos votos

7 – Passos a serem realizados:

As táticas, técnicas e procedimentos envolve, mas não somente, as seguintes etapas:

- Inserir cabo *splitter de displayport,* e conectar dois displays, onde um fique visível e um segregado.
- Iniciar a votação.
- Anotar a sequência de eleitores habilitados.
- Gravar a sequência de tela alternativa, com uso simples de *smartphone*.
- Caso não obtenha sucesso, repetir os passos usando outras técnicas para obter o conteúdo do *display*.
- Caso não obtenha sucesso, ajustar os procedimentos e repetir o teste.

8 – Materiais necessários (fornecidos pelo TSE):

- 1 Urna eletrônicas.
- *display* do TE.
- Mídias e suprimentos da UE.

9 – Possíveis resultados e impacto:

9.1 Resultados pretendido e provável.

Espera-se que se executado com sucesso, consiga violar o sigilo do voto, tendo com extensão a quantidade de urnas objeto do ataque.

Além disso, cumpre salientar que o presente plano de ataque, será executado por **ethical hackers**, em ambiente controlado e com limitação de escopo, tendo seus resultados reduzidos em comparação ao cenário em que um ataque real seria executado, inclusive por atacantes internos.

9.2 Análise de risco e do impacto potencial.

Quanto a viabilidade: O ataque é viável, visto que conforme discorrido no item 2 e associado a outros ataques, como de de engenharia social e outros, pode ser plenamente aplicado ao cenário real.

Quanto à extensão: A extensão do ataque é a quantidade de seções que tiverem a o conteúdo do display obtido, gravado ou espelhado.

Quanto ao risco: O risco do ataque é alto se encontra devido ao fato de ser facilmente reproduzível, embora exija aparato técnico (média probabilidade de ocorrência) e violar a previsão constitucional de sigilo do voto (alto dano causado ao ativo protegido).

10 – Rastreabilidade:

10.1 Detecção de ataques

Não se vislumbra a possibilidade de detecção do ataque. Além disso, eventual detecção não possui condão de anular os votos registrado, apenas a apuração da responsabilidade penal.

10.2 Técnicas furtivas e Antiforense

Não serão utilizadas técnicas furtivas ou antiforenses pois envolveriam sistemas, ambientes, procedimentos e elementos vedados pelo § 2 do art. 2 do edital de convocação do TPS (e.g. lacre físico)

11 – Solução proposta:

- Criptografia do tráfego, de modo que somente o *display* apropriado consiga decifrar a saída de vídeo.
- Levantar exceção (erro crítico) em caso de conexão com mais de um *display*.
- Registro do número de identificação dos periféricos e explicitar todas as alterações de periféricos seja devidamente registrada.

6

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

SUFFRAGIUM SIMULATA SUBSTANTIAM VERITAS MUTARE POSSUNT

Instituição proponente (se aplicável)

Não aplicável

Responsável

Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)

Alterar a destinação dos votos, substituindo a votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(x) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(x) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
(x) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

1.1 Apresentação

O sistema eletrônico de votação, na medida que abrange processos de redundância, aumenta a superfície de ataque. Nesta seara, como é adotado um processo de atualização da assinatura do RDV a cada voto gera uma necessidade imprescindível do RDV anterior ser confiável. Tal processo permanece em caso de continuidade de votação, deixado de existir lastro entre o RDV e a urna substituída. Assim, as urnas de contingência são potenciais vetores de ataque ao sistema graça a sua característica de poder assumir em definitivo qualquer seção e em especial

1.2 Objetivos

Iniciar, de forma paralela, de uma votação oficial na UE regular e uma votação espúria na UE de contingência 1. Forçar falha na UE regular e iniciar processo de contingência onde o seriam inseridos na UE de contingência 2, a mídia da UE com votação espúria ao invés da UE oficial e com isso **alterar a destinação dos votos.**

2 – Fundamentação teórica:

2.1 Análise do processo eleitoral brasileiro

A mesa receptora de votação, na condição de autoridade eleitoral, possui acesso e executa atividade críticas cuja o sistema eletrônico de votação não dispões de funcionalidade para coibir preventivamente eventual desvio. Na abertura das atividades e no encerramento da votação, somente os membros da mesa tem seus dados biométricos registrados, ou seja, não há registros das atividades fiscalizadoras nos arquivos gerados pelas urnas eletrônicas. Dessa forma, não há um elo entre a urna fiscalizada e a que tem seus os seus arquivos enviados ao sistema de totalização. Eventual processo de teste de autenticidade ou integridade, depende da seção ser sorteada.

A inicialização da urna no dia da votação ocorre com base na data e horário, não requerendo validação por softwares externos, que assine digitalmente e/ou permita aos fiscais o registro de algo que certifique que aqueles dados não são espúrios (o teste de autenticidade depende de sorteio prévio).

2.2 Processo de Contingência

A urna de contingência é programada para apenas substituir outro equipamento e caso de ocorrência de falha. Ela é preparada sem dados e necessita dos dados provenientes de uma seção eleitoral para iniciar ou continuar uma votação. As urnas de contingência também possuem correspondências, tal como as urnas preparadas para seções eleitorais específicas. Essas tabelas são publicadas na véspera do pleito para que o sistema de totalização só receba votos de urnas previstas.

Quando ocorre a substituição da urna, a correspondência da contingência passa a ser atribuída à seção eleitoral. Essa característica é persistida na urna e na totalização, de modo que a nova correspondência passa a ser a esperada para a seção eleitoral. Quando uma urna de contingência é utilizada para a substituição de uma urna original de uma seção, ela assume em definitivo os dados daquela seção eleitoral e não deve ser utilizada para substituir outras urnas. Além disso, o RDV assinado pela urna original passa a ser assinado pela urna substituta.

Para esse processo ocorrer, são usadas as mídias ou caso não seja possível o recuperador de arquivo é inserido na UE de contingência. Nessa mídia de votação contém RDV assinado pela urna que está coletando os votos. Quando ocorre a substituição da urna, o RDV assinado pela urna original passa a ser assinado pela urna substituta. Essa é uma particularidade desnecessária, visto que **o RDV não é necessário no processo de continuidade de votação em urna de contingência,** apenas dados do processo de habilitação do eleitor. A urna de contingência precisa saber se determinado eleitor votou ou não os votos propriamente dito destes eleitores A substituição da assinatura valida o conteúdo da RDV, independente do conteúdo ser espúrio ou não.

Considerando a filosofia **Zero Trust**, nunca se poderia presumir que o conteúdo usado como *backup* é confiável ainda mais quando isso não interfere na continuidade da votação. Deveria ter dois RDV, um com os votos recuperados preservando a assinatura da Urna substituída e outro com os demais assinados pela urna de contingência onde eles foram registrados.

3 – Precondições para o teste:

- UE oficial e duas de contingência, conforme tabela de correspondência, sem lacres.
- Acesso a mídias e suprimentos da UE.
- Corrupção dos membros da mesa receptora.

4 – Escopo – Superfície de ataque:

4.1 Superfície de ataque física

- UE modelo 2020 ou 2022
- Mídias e suprimentos da UE.

4.2 Superfície de ataque digital

- *Software de votação*

4.3Restrições e limitações

- Engenharia social (fora do escopo, não será executado)
- Habilitação biométrica (fora do escopo, não será executado)

5 – Janela de atuação simulada do atacante:

- Acesso as UE oficial de contingência antes e durante a votação.
- Acesso as mídias e suprimentos da UE antes e durante a votação.

6 – Pontos de intervenção:

- Preparação de seção.
- Votação (registro do voto).
- Habilitação dos eleitores.
- Processo de contingência.
- Fluxo de uso das mídias e suprimentos da UE.

7 – Passos a serem realizados:

As táticas, técnicas e procedimentos envolve, mas não somente, as seguintes etapas:

- Iniciar votação na UE oficial.
- Iniciar votação na UE de contingência 1.

- Habilitar eleitores e inserir votos espúrios na UE de contingência 1 conforme forem habilitados e registrados pela UE oficial.
- Provocar falha na UE oficial e de contingência
- Iniciar processo de contingência na UE de contingência na UE de contingência 2.
- Inserir com votos espúrios na UE de contingência 2, ao invés da mídia de votação *(backup)* da UE oficial.
- Continuar a votação e encaminhar os votos espúrios para totalização
- Caso não seja executado com êxito, repetir os procedimentos com ajustes, visando driblar a obstáculos encontrados.
- Caso não seja executado com êxito, substituir a urna de votação oficial por simulacro destinado capturar os dados apenas do processo de habilitação.

8 – Materiais necessários (fornecidos pelo TSE):

- 3 Urnas eletrônicas
- Mídias e suprimentos da UE.

9 – Possíveis resultados e impacto:

9.1 Resultados pretendido e provável.

Adulterar a destinação dos votos, com a substituição dos votos regulamente registrado pelos arbitrariamente inseridos em outra urna, sendo os votos espúrios encaminhados a continuidade de votação pelo processo de contingência.

Além disso, cumpre salientar que o presente plano de ataque, será executado por ***ethical hackers***, em ambiente controlado e com limitação de escopo, tendo seus resultados reduzidos em comparação ao cenário em que um ataque real seria executado, inclusive por atacantes internos.

9.2 Análise de risco e do impacto potencial.

Quanto a viabilidade: O ataque é viável, visto que conforme discorrido no item 2 e associado a outros ataques, como de engenharia social e outros, pode ser plenamente aplicado ao cenário real.

Quanto a extensão de ataque: O ataque se estende por quantas seções que tiver processo de contingência com continuidade da votação com votos espúrios.

10 – Rastreabilidade:

10.1 Detecção de ataques

Não se vislumbra a possibilidade de detecção preventiva do ataque. Além disso, eventual detecção preventiva dependeria de controle logístico,

10.2 Técnicas furtivas e Antiforense

Execução de alguns procedimentos com a UE desligada para frustrar registro de log. Além disso, não serão utilizadas técnicas furtivas ou antiforenses pois envolveriam sistemas, ambientes, procedimentos e elementos vedados pelo § 2 do art. 2 do edital de convocação do TPS (e.g. lacre físico, captura de dados biométricos para habilitação do eleitor, *et cetera*)

11 – Solução proposta:

- Manter os RDV da urna substituída segregado do RDV da urna de contingência e deixar substituir a assinatura do RDV da urna anterior pela assinatura da urna de contingência. Esta informação é

desnecessária para continuidade de votação apenas informação do processo de habilitação de eleitor e não os votos propriamente ditos são usados para continuidade da votação.

- Implementar software para possibilitar que o conteúdo dos relatórios emitidos pela UE, inclusive antes do início da votação, possa ser obtido e validado externamente. Assim, com a mecanismo da troca de chaves *Diffie-Hellman*, a UE e o softwares a ser implementados criptografariam o arquivo com a chave secreta partilhada e calculariam seu *hash.* Logo, esse *hash* dependeria da troca de chaves e consequentemente a chave privada do agente externo.
- Fazer referência e usar no *head* o *hash* do relatório anterior emitido de modo que todos os arquivos gerados por determinada urna sejam encadeados em blocos e para que seja possível acompanhar toda a cadeia de custódia dos arquivos gerados (trilha de auditoria em *blockchain* desde a lacração até a totalização)

6

Data
Resultado **( ) Aprovado** **( ) Aprovado com ressalvas** **( ) Reprovado**

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

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

Instituição proponente (se aplicável)

Proposta de Plano de Teste Não Vinculada à Instituição

Responsável

Prof. Dr. João Benedito dos Santos Junior & Prof. Dr. Luiz Alberto Ferreira Gomes

Resumo do plano (máximo de 120 caracteres)

Este Plano de Teste está inserido no contexto da verificação de integridade e autenticidade de sistemas eleitorais. Pretende-se, em tempo real, extrair, verificar e validar o conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis que estiverem embarcados na Urna Eletrônica, considerando um cenário em que seja necessário verificar a integridade e autenticidade após os procedimentos de certificação e liberação das Urnas Eletrônicas para o Pleito Eleitoral.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
(X) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
(X) Verificador Pré/Pós-Eleição (VPP)
(X) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
(X) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Pretende-se extrair, em tempo real, o resumo criptográfico, observando o padrão do algoritmo SHA 512 Radix 64, de cada código compilado e/ou executável que estiver embarcado no hardware da Urna Eletrônica, considerando a estrutura definida para o sistema de arquivos, suportado pelo Sistema Operacional Linux, conforme observado na Inspeção Preliminar dos Códigos-Fonte, realizada em 20 de outubro de 2023.

2 – Fundamentação teórica:

Um código criptográfico é gerado para garantir a integridade dos arquivos a serem investigados. Os códigos ou resumos criptográficos, também conhecidos como Algoritmos de HASH, permitem a verificação da integridade de arquivos digitais em quaisquer formatos e com quaisquer estruturas, tanto aqueles de natureza textual quanto aqueles binários (codificados). A partir de um arquivo de entrada, de qualquer tamanho em Bytes, os algoritmos de HASH geram uma sequência de caracteres de saída, de tamanho fixo (resumo criptográfico).

3 – Precondições para o teste:

Existência de um mecanismo e/ou módulo que exporte o conjunto completo dos arquivos compilados e/ou executáveis embarcados no hardware da Urna Eletrônica, em um modelo semelhante à estrutura publicada em https://www.justicaeleitoral.jus.br/tps/arquivos/2023/documentos/HashesPDF.zip, que apresenta, para download, os resumos digitais dos sistemas que compõem a plataforma eleitoral brasileira.

4 – Escopo – Superfície de ataque:

Este Plano de Testes está centrado na Urna Eletrônica, mais especificamente nos códigos compilados e embarcados na plataforma de hardware, considerando a existência de um sistema de arquivos suportado pelo Sistema Operacional Linux, conforme observado na Inspeção Preliminar dos Códigos-Fonte, realizada em 20 de outubro de 2023.

5 – Janela de atuação simulada do atacante:

Os proponentes implementaram, utilizando a linguagem Java, um módulo verificador e validador de HASH para conjuntos de arquivos. Este módulo, que poderá ser cedido ao TSE, gratuitamente, recebe como entrada um sistema de arquivos qualquer, composto por pastas, subpastas e arquivos, extrai o resumo criptográfico de cada arquivo e o compara com um padrão, que é dado como entrada na forma de um arquivo-texto.

6 – Pontos de intervenção:

Este Plano de Teste pretendo intervir no subsistema AVPART, no contexto do hardware da Urna Eletrônica, contribuindo com os procedimentos de Teste de Integridade, num cenário de pré-votação, e fortalecendo os aspectos de transparência do sistema eleitoral.

7 – Passos a serem realizados:

1. Conectar módulo extrator à Urna Eletrônica, utilizando uma interface USB;
2. Coletar o conjunto completo dos arquivos binários compilados e/ou executáveis existentes no sistema de arquivos do hardware da Urna Eletrônica;
3. Calcular o resumo criptográfico HASH SHA 512 Radix64 para cada arquivo coletado;
4. Verificar a integridade do resumo criptográfico em relação a um padrão estabelecido e conhecido;
5. Emitir o relatório de validação.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna Eletrônica;
2. Módulo exportador dos arquivos binários embarcados na Urna Eletrônica;
3. Listagem completa, em formato textual, dos resumos criptográficos HASH SHA 512 Radix64 de todos os arquivos binários embarcados na Urna Eletrônica.

9 – Possíveis resultados e impacto:

Ao longo dos mais de 25 anos de uso do Sistema Eletrônico de Votação nas Eleições Brasileiras, questionamentos sobre a integridade das Urnas Eletrônicas têm sido feitos por diferentes atores da sociedade e em diversos momentos da história recente do país. Este Plano de Teste, uma vez executado, poderá contribuir num cenário de pré-votação, em que seja possível oferecer à sociedade, nas seções eleitorais, um mecanismo de auditoria em tempo real, que garanta que os códigos binários existentes em todas as Urnas Eletrônicas são EXATAMENTE iguais, sem qualquer possibilidade de existência de software malicioso, de qualquer natureza, embarcado no hardware das mesmas.

10 – Rastreabilidade:

Para garantir a eficácia do Plano de Teste, pretende-se executar os passos, descritos no item 7, ao menos 5 (cinco) vezes, sendo que cada bateria de teste deve ser realizada em 1 (uma) hora e 30 minutos, desde o início da extração e geração dos resumos criptográficos até a emissão do relatório de validação. Ao final da bateria de testes, os 5 (cinco) relatórios de validação devem ser IDÊNTICOS.

11 – Solução proposta:

Um módulo de software, desenvolvido pelos autores desta proposta e utilizando a linguagem Java, que pode ser cedido, gratuitamente, ao TSE, que seja capaz de verificar, em tempo real e a qualquer tempo, a integridade dos códigos binários compilados e/ou executáveis embarcados nas Urnas Eletrônicas.

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Auditoria de Integridade e Segurança na Apuração Eletrônica de Votos
Instituição proponente (se aplicável)
Responsável João Vitor Santana Silva
Resumo do plano (máximo de 120 caracteres) Teste verifica integridade da apuração de votos para garantir resultados eleitorais confiáveis
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
(X) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

2 – Fundamentação teórica:

3 – Precondições para o teste:

4 – Escopo – Superfície de ataque:

5 – Janela de atuação simulada do atacante:

6 – Pontos de intervenção:

7 – Passos a serem realizados:

8 – Materiais necessários (fornecidos pelo TSE):

9 – Possíveis resultados e impacto:

10 – Rastreabilidade:

11 – Solução proposta:

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

Auditoria de Integridade e Segurança na Apuração Eletrônica de Votos

Resumo: "Teste verifica integridade da apuração de votos para garantir resultados eleitorais confiáveis."

1 - Descrição Geral do Plano: Este plano de teste de auditoria visa avaliar a integridade, confiabilidade e segurança do processo de apuração de votos em urnas eletrônicas usadas em eleições. O teste se concentra na detecção de vulnerabilidades que possam comprometer a precisão e a integridade da apuração.

2 - Fundamentação Teórica: Baseia-se em princípios de auditoria de sistemas eleitorais que enfatizam a necessidade de garantir que a apuração dos votos seja precisa, segura e resistente a ameaças. A integridade da apuração de votos é fundamental para a credibilidade do processo eleitoral, especialmente diante das contestações públicas frequentemente observadas. A apuração de votos é uma etapa crucial que determina os resultados eleitorais, e qualquer suspeita de manipulação ou falha na integridade dos dados pode minar a confiança pública no sistema democrático.

3 - Precondições para o Teste:

- Acesso à urna eletrônica de teste.
- Permissões de teste concedidas pelo órgão eleitoral (TSE).
- Recursos técnicos para simular ataques e manipulações nos dados da urna.

4 - Escopo - Superfície de Ataque:

- Integridade dos dados durante o processo de apuração.
- Detecção e prevenção de votos duplicados.
- Segurança da comunicação entre a urna e o sistema central.
- Resistência a falhas e recuperação de dados após interrupções.

5 - Janela de Atuação Simulada do Atacante:

- Durante o processo de apuração de votos.
- Durante a comunicação dos resultados para o sistema central.
- Em situações de falhas de energia ou interrupções.

6 - Pontos de Intervenção:

- Votos emitidos na urna.
- Dados durante a transmissão para o sistema central.
- Dados armazenados na urna eletrônica.
- Componentes físicos da urna eletrônica.

7 - Passos a Serem Realizados:

A. Emitir votos de teste na urna eletrônica.
B. Executar a apuração de votos.
C. Introduzir votos inválidos ou corrompidos na urna.
D. Simular votos duplicados.
E. Simular falha de energia durante a apuração.
F. Avaliar medidas de segurança, como criptografia.
G. Realizar testes de usabilidade.

8 - Materiais Necessários (Fornecidos pelo TSE):

- Urna eletrônica de teste.
- Acesso aos sistemas de teste.
- Recursos para simular cenários de teste.

9 - Possíveis Resultados e Impacto:

- Identificação de vulnerabilidades no processo de apuração.
- Detecção de votos duplicados.
- Evidências de integridade dos dados.
- Medidas de segurança eficazes.
- Recomendações para melhorias no sistema.

10 - Rastreabilidade:

- Documentação completa de todas as etapas de teste e resultados.
- Relatórios detalhados sobre as ações realizadas e resultados obtidos.

11 - Solução Proposta:

Auditorias Independentes:

1. Realizar auditorias independentes conduzidas por organizações de terceiros para verificar a integridade do processo de apuração.

Registro de Atividades:

1. Manter um registro detalhado das atividades durante a apuração, incluindo quem está envolvido, quando e quais ações são realizadas.

Relatórios de Transparência:

1. Preparar relatórios de transparência detalhados após a conclusão da apuração, destacando as etapas e os resultados.

Comissão de Observadores Eleitorais:

1. Permitir a presença de observadores eleitorais independentes que possam monitorar o processo de apuração e relatar suas observações.

A implementação dessas medidas não apenas tornará a apuração de votos mais transparente, mas também aumentará a confiança do público nas eleições e no sistema democrático como um todo.
Com base nos resultados do teste de auditoria, qualquer vulnerabilidade ou problema identificado deve ser relatado ao TSE. Uma solução proposta pode incluir melhorias no sistema de apuração, aprimoramento das medidas de segurança e garantia da integridade dos dados eleitorais. É fundamental que essas soluções sejam implementadas antes de eleições reais para garantir a integridade do processo de votação e apuração.

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

EXECUÇÃO DO JE-CONNECT UTILIZANDO COMPUTADOR COM SISTEMA OPERACIONAL INVÁLIDO

Instituição proponente (se aplicável)

Responsável

NICHOLAS BARROS DOS SANTOS

Resumo do plano (máximo de 120 caracteres)

ANALISAR A EFICÁCIA DA EXECUÇÃO DO JE-CONNECT EM COMPUTADORES QUE APRESENTAM FALHAS NA VALIDAÇÃO DO SISTEMA OPERACIONAL.

Sistemas a serem testados

Softwares

(X) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(X) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
(X) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
(X) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos

(X) Geração de mídias
(X) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
(X) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(X) Recuperação de dados na urna eletrônica
(X) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O PLANO DE ATAQUE CONSISTE EM 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, O QUE PODE OCASIONAR POSSÍVEIS RISCOS DA QUEBRA DE SIGILO E DO TRANSPORTE DOS DADOS OBTIDOS DURANTE O PLEITO.

2 – Fundamentação teórica:

O USO DE SISTEMAS OPERACIONAIS QUE NÃO ESTÃO ATUALIZADOS OU ESTÃO COM A SUA LICENÇA INVÁLIDA DEIXA O COMPUTADOR PASSÍVEL DE VÁRIAS POSSÍVEIS INTERCORRÊNCIAS, COMO ATAQUES DE FORÇA BRUTA, QUE PODEM PREJUDICAR E QUEBRAR O SIGILO DO VOTO E DO TRANSPORTE DOS ARQUIVOS QUE ESTÃO SENDO TRANSPORTADOS PARA O TSE, OCASIONANDO A POSSÍVEL AÇÃO DE AGENTES NOCIVOS AO PROCESSO, COMO A AÇÃO DE CYBERCRIMINOSOS OU A AÇÃO DE PROGRAMAS NOCIVOS A OPERAÇÃO.

ALÉM DISSO, FIREWALLS OU PROTOCOLOS CONFIGURADOS INCORRETAMENTE SERVEM COMO PONTOS DE ENTRADA PARA HACKERS, QUE PODEM APROVEITAR OS ERROS DE PROGRAMAÇÃO E IMPLEMENTAÇÃO EM APLICATIVOS DE TERCEIROS, S.O. E OUTROS SOFTWARES OU *FIRMWARES* PARA SE INFILTRAR EM REDES, OBTER ACESSO A DIRETÓRIOS DE USUÁRIOS OU INSERIR MALWARE. POR EXEMPLO, EM 2021, CYBERCRIMINOSOS APROVEITARAM UMA FALHA NA PLATAFORMA VSA (DISPOSITIVO DE ARMAZENAMENTO VIRTUAL) DA KASEYA (LINK EXTERNO À IBM.COM) PARA DISTRIBUIR RANSOMWARE, DISFARÇADO DE UMA ATUALIZAÇÃO DE SOFTWARE, PARA OS CLIENTES DA KASEYA.

O JE-CONNECT É UMA TECNOLOGIA DESENVOLVIDA E UTILIZADA PELA JUSTIÇA ELEITORAL BRASILEIRA NO ANO DE 2010 COM O OBJETIVO DE TRANSMITIR OS DADOS OBTIDOS, COMO O BOLETIM DE URNA DIRETAMENTE DE ALGUNS LOCAIS DE VOTAÇÃO, PRINCIPALMENTE AQUELES MAIS DISTANTES DOS CARTÓRIOS ELEITORAIS, COM A FINALIDADE DE DAR CELERIDADE A APURAÇÃO DOS VOTOS, SEM COMPROMETER A SEGURANÇA DO PLEITO.

QUANDO ENCERRADO OS TRÂMITES DE VOTAÇÃO, É INICIADA A TRANSMISSÃO DOS RESULTADOS DAQUELE LOCAL DE VOTAÇÃO DIRETAMENTE PARA O BANCO DE DADOS DO TRIBUNAL SUPERIOR ELEITORAL (TSE), LOCALIZADO EM BRASÍLIA, SEM A NECESSIDADE DE PASSAR PELO CARTÓRIO ELEITORAL OU TRIBUNAL REGIONAL ELEITORAL.

O PROCESSO É FEITO ATRAVÉS DE UM COMPUTADOR DA JUSTIÇA ELEITORAL, MAS QUANDO ISSO NÃO É POSSÍVEL POR DIVERSOS MOTIVOS, O PROCESSO É FEITO POR UM COMPUTADOR DO PRÓPRIO LOCAL DE VOTAÇÃO, UTILIZANDO UMA REDE PRIVADA VIRTUAL (VPN), GARANTINDO PLENA SEGURANÇA NO PROCESSO DE TRANSMISSÃO DE DADOS A INSTÂNCIA SUPERIOR

RESPONSÁVEL PELO PLEITO.

3 – Precondições para o teste:

PARA FAZER O TESTE APRESENTADO, NECESSITO DE UM COMPUTADOR OU NOTEBOOK COM ALGUM SISTEMA OPERACIONAL QUE NÃO ESTEJA COM A SUA CHAVE VALIDADA, ALÉM DOS ELEMENTOS DOS SISTEMAS MARCADOS ANTERIORMENTE.

4 – Escopo – Superfície de ataque:

POR TER SEU ACESSO E DISTRIBUIÇÃO DE ARQUIVOS FEITA PELA REDE MUNDIAL DE COMPUTADORES (INTERNET), O JE-CONNECT VINCULADO A UM S.O. INVÁLIDO PODE ESTAR VULNERÁVEL A ATAQUES, PODENDO SER ADICIONADO AO PROGRAMA OU NO MOMENTO DA TRANSMISSÃO DE DADOS ALGUM CÓDIGO MALICIOSO NAS INTERFACES DE PROGRAMAÇÃO DO PROGRAMA, FAZENDO COM QUE DIVULGUEM INDEVIDAMENTE OU ATÉ MESMO DESTRUAM INFORMAÇÕES CONFIDENCIAIS EM BANCOS DE DADOS QUE NÃO ESTÃO VINCULADOS AO TSE.

MESMO QUE O TSE APRESENTE VÁRIAS OUTRAS MODALIDADES DE OBTENÇÃO DOS DADOS DA URNA ELETRÔNICA, COMO A IMPRESSÃO E TRANSMISSÃO VIA MOBILE APP DO BOLETIM DE URNA (BU) APÓS O FINAL DO PLEITO, O POSSÍVEL USO DE COMPUTADORES COM S.O. INVÁLIDO PODE PREJUDICAR A SEGURANÇA E O SIGILO DOS VOTOS OBTIDOS.

ALÉM DO MAIS O USO INTENCIONAL DE AGENTES MALICIOSOS PODE EXTRAIR DADOS SENSÍVEIS, UTILIZANDO MALWARES, DESATIVANDO DISPOSITIVOS, E POR FIM, PREJUDICANDO A APURAÇÃO DO PLEITO.

ESSA SITUAÇÃO PODE FAZER COM QUE CRIMINOSOS PODEM ROUBAR DISPOSITIVOS DE TERMINAL OU OBTER ACESSO A ELES INVADINDO AS INSTALAÇÕES DE UMA ORGANIZAÇÃO. APÓS TOMAR POSSE DO HARDWARE, OS HACKERS PODEM ACESSAR DADOS E PROCESSOS ARMAZENADOS NESSES DISPOSITIVOS. ELES PODEM USAR TAMBÉM AS IDENTIDADES E AS PERMISSÕES DO DISPOSITIVO PARA ACESSAR OUTROS RECURSOS DE REDE. TERMINAIS USADOS POR TRABALHADORES REMOTOS, DISPOSITIVOS PESSOAIS DOS FUNCIONÁRIOS E DISPOSITIVOS DESCARTADOS DE MANEIRA INADEQUADA SÃO ALVOS TÍPICOS DE FURTO DE DADOS.

5 – Janela de atuação simulada do atacante:

O PLANO DE TESTE ATUARÁ SOB QUATRO PRINCÍPIOS:

1- **DISPONIBILIDADE:** A INFORMAÇÃO DA QUAL SE PROCURA DEVE ESTAR DISPONÍVEL SEMPRE QUE SE FIZER NECESSÁRIO, SEJA UTILIZANDO FIREWALLS OU BACKUPS;

2- **INTEGRIDADE:** A INFORMAÇÃO (VOTOS) DEVE CHEGAR AO DESTINO DE MANEIRA INTEGRA, COM O USO DE ASSINATURAS DIGITAIS, POR EXEMPLO;

3- **CONFIDENCIALIDADE:** ESSAS INFORMAÇÕES DEVEM MANTER A SUA CONFIDENCIALIDADE DO INÍCIO AO FIM DO PROCESSO (MANTENDO O SIGILO DO VOTO), ATRAVÉS DO USO DA CRIPTOGRAFIA;

4- AUTENTICIDADE: ESSAS INFORMAÇÕES (VOTOS) DEVEM GARANTIR A SUA VERACIDADE, MEDIANTE PROCEDIMENTOS DE AUDITORIA, ATRAVÉS DOUSO DA BIOMETRIA, ASSINATURAS DIGITAIS, DENTRE OUTROS MEIOS AUDITÁVEIS.

6 – Pontos de intervenção:

OS PRINCIPAIS PONTOS DE INTERVENÇÃO NESSE PLANO SÃO:

1- O JE-CONNECT, DO QUAL DEVE SER ANALISADO PARA O SEU USO EM POSSÍVEIS COMPUTADORES OU NOTEBOOKS COM VULNERABILIDADES NO SEU SISTEMA OPERACIONAL, FAZENDO COM QUE SE TRABALHE SOMENTE COM MÁQUINAS COM S.O. DEVIDAMENTE VALIDADAS;

2- O COMPUTADOR OU NOTEBOOK COM O SISTEMA OPERACIONAL UTILIZADO, DO QUAL ESPERA-SE PROVAR QUE ESSA VULNERABILIDADE NÃO INFLUENCIA NO SIGILO E NA TRANSMISSÃO DOS VOTOS;

3- A MÍDIA DE VOTAÇÃO, DA QUAL ESPERA-SE QUE SE MANTENHA ÍNTEGRA, SEM A PRESENÇA POSTERIOR DE AGENTES NOCIVOS PRESENTES NO COMPUTADOR UTILIZADO NA TRANSMISSÃO DE VOTOS VIA JE-CONNECT;

7 – Passos a serem realizados:

1ª SIMULAÇÃO DE ELEIÇÃO: ONDE SE ADOTARIA UMA PEQUENA QUANTIDADE DE VOTOS (ENTRE 10 E 20);

2ª APURAÇÃO DOS VOTOS: PARTINDO DESSA PREMISSA, RETIRA-SE A MÍDIA DE VOTAÇÃO DA URNA ELETRÔNICA E INSERE A MESMA NUM COMPUTADOR OU NOTEBOOK COM S.O. OPERANDO DE FORMA INCORRETA;

3ª EXECUÇÃO DO JE-CONNECT: COM A PRESENÇA DE UM COMPUTADOR OU NOTEBOOK OPERANDO COM O SISTEMA OPERACIONAL INVÁLIDO, FAZ-SE A SIMULAÇÃO DA EMISSÃO DESSES DADOS PARA UMA ESPÉCIE DE BANCO DE DADOS DO TSE, E SE VERIFICA SE EXISTE ALGUMA VULNERABILIDADE NO MOMENTO DA TRANSMISSÃO DOS VOTOS.

8 – Materiais necessários (fornecidos pelo TSE):

- GERENCIADOR DE DADOS, APLICATIVOS E INTERFACE COM A URNA ELETRÔNICA (GEDAI-UE);
- COMPUTADOR OU NOTEBOOK COM SISTEMA OPERACIONAL INVÁLIDO;
- SOFTWARE BÁSICO DA URNA ELETRÔNICA;
- SOFTWARE DE VOTAÇÃO (VOTA);
- GERAÇÃO DE MÍDIAS;
- CARGA DA URNA ELETRÔNICA;
- SISTEMAS TRANSPORTADOR, RECARQUIVOS;
- INFOARQUIVOS;
- SUBSISTEMA DE INSTALAÇÃO E SEGURANÇA (SIS);
- KIT JE-CONNECT;

- URNAS MODELOS 2020 E 2022, COM SEUS RESPECTIVOS *FIRMWARES* E MÍDIAS ELETRÔNICAS;
- SISTEMA DE APOIO ÀS AUDITORIAS DE AUTENTICIDADE E INTEGRIDADE - MÓDULO SORTEIO E MÓDULO VOTAÇÃO;
- VERIFICADOR PRÉ/PÓS-ELEIÇÃO (VPP);
- TRANSMISSÃO DE ARQUIVOS (KIT JE-CONNECT);
- TESTE DE INTEGRIDADE (VOTAÇÃO PARALELA);
- CONFERÊNCIA DE HASH OU VALIDAÇÃO DE ASSINATURAS NA URNA;
- RECUPERAÇÃO DE DADOS NA URNA ELETRÔNICA *FIRMWARES;*
- APURAÇÃO DE VOTOS NA URNA ELETRÔNICA

9 – Possíveis resultados e impacto:

SE PROCURA ENTENDER QUE O JE-CONNECT NÃO APRESENTE NENHUMA ALTERAÇÃO NO QUE SE TRATA DA VULNERABILIDADE DO SIGILO E DA TRANSMISSÃO DOS DADOS AO TSE NO FINAL DO PLEITO.

10 – Rastreabilidade:

VERIFICAR, ATRAVÉS DOS CÓDIGOS-FONTE, DO BOLETIM DE URNA IMPRESSO E DE OUTROS MEIOS DE VALIDAÇÃO SE OS VOTOS FORAM ENVIADOS VIA JE-CONNECT DE MANEIRA INTEGRA, CONFIDENCIAL E COM TODA SEGURANÇA E AUTENTICIDADE.

11- Solução proposta:

INDEPENDENTE DO RESULTADO APRESENTADO, DEIXO COMO MEDIDAS DE REFORÇO A SEGURANÇA CIBERNÉTICA AO SETOR RESPONSÁVEL DO TSE QUE SE ADOTE NOVOS MEIOS QUE DEIXEM O JE-CONNECT MAIS SEGURO, AO PERMITIR SOMENTE QUE COMPUTADORES COM SISTEMA OPERACIONAL DEVIDAMENTE VALIDADOS FAÇAM A EXECUÇÃO DO MESMO, FAZENDO COM QUE OS DADOS SEJAM TRANSMITIDOS COM O MÁXIMO DE SIGILO E SEGURANÇA PARA O BANCO DE DADOS DO ÓRGÃO MÁXIMO DA JUSTIÇA ELEITORAL.

Data	
Resultado	( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

1

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

COMPORTAMENTO DO JE-CONNECT NA EXECUÇÃO DE UM BOT DE MONITORAMENTO NO COMPUTADOR TRANSMISSOR DE DADOS

Instituição proponente (se aplicável)

Responsável

NICHOLAS BARROS DOS SANTOS

Resumo do plano (máximo de 120 caracteres)

ANALISAR O COMPORTAMENTO DO JE-CONNECT EM UM COMPUTADOR NA EXECUÇÃO DE UM BOT, PARA ATESTAR A SUA INTEGRALIDADE NA TRANSMISSÃO DOS DADOS.

Sistemas a serem testados

Softwares

(X) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(X) Software de Votação (VOTA)
(X) Recuperador de Dados (RED)
(X) Sistema de Apuração (SA)
(X)Sistemas Transportador, RecArquivos e InfoArquivos
(X) Subsistema de Instalação e Segurança (SIS) JEConnect
(X) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
(X) Sistema de apoio às auditorias de autenticidadee integridade - Módulo Sorteio e Módulo Votação
(X) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)(X)

Procedimentos

(X) Geração de mídias
(X) Carga da urna eletrônica
(X) Votação
( ) Transmissão de arquivos( )
( ) Sorteio de seções
(X) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas() Kit na urna
( ) Recuperação de dados na urna eletrônica
(X) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/3, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O PLANO DE ATAQUE CONSISTE EM DESENVOLVER E EXECUTAR UM BOT DE MONITORAMENTO NUM COMPUTADOR ONDE SERÁ UTILIZADO O JE-CONNECT, COM A FINALIDADE DE ANALISAR O COMPORTAMENTO DO PROGRAMA, 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, FUNÇÃO PRINCIPAL DO JE-CONNECT.

2 – Fundamentação teórica:

O JE-CONNECT É UMA TECNOLOGIA DESENVOLVIDA E UTILIZADA PELA JUSTIÇA ELEITORAL BRASILEIRA NO ANO DE 2010 COM O OBJETIVO DE TRANSMITIR OS DADOS OBTIDOS, COMO O BOLETIM DE URNA DIRETAMENTE DE ALGUNS LOCAIS DE VOTAÇÃO, PRINCIPALMENTE AQUELES MAIS DISTANTES DOS CARTÓRIOS ELEITORAIS, COM A FINALIDADE DE DAR CELERIDADE A APURAÇÃO DOS VOTOS, SEM COMPROMETER A SEGURANÇA DO PLEITO.

QUANDO ENCERRADO OS TRÂMITES DE VOTAÇÃO, É INICIADA A TRANSMISSÃO DOS RESULTADOS DAQUELE LOCAL DE VOTAÇÃO DIRETAMENTE PARA O BANCO DE DADOS DO TRIBUNAL SUPERIOR ELEITORAL (TSE), LOCALIZADO EM BRASÍLIA, SEM A NECESSIDADE DE PASSAR PELO CARTÓRIO ELEITORAL OU TRIBUNAL REGIONAL ELEITORAL.

O PROCESSO É FEITO ATRAVÉS DE UM COMPUTADOR DA JUSTIÇA ELEITORAL, MAS QUANDO ISSO NÃO É POSSÍVEL POR DIVERSOS MOTIVOS, O PROCESSO É FEITO POR UM COMPUTADOR DO PRÓPRIO LOCAL DE VOTAÇÃO, UTILIZANDO UMA REDE PRIVADA VIRTUAL (VPN), GARANTINDO PLENA SEGURANÇA NO PROCESSO DE TRANSMISSÃO DE DADOS A INSTÂNCIA SUPERIOR RESPONSÁVEL PELO PLEITO.

UM "BOT" – ABREAVIATURA DE ROBÔ - É UM PROGRAMA DE SOFTWARE QUE EXECUTA TAREFAS AUTOMATIZADAS, REPETITIVAS E PRÉ-DEFINIDAS, ONDE NORMALMENTE IMITAM OU SUBSTITUEM O COMPORTAMENTO HUMANO. POR SEREM AUTOMATIZADOS, PODEM EXECUTAR MÚLTIPLAS TAREFAS, COM MAIOR CELERIDADE COMPARADOS AOS USUÁRIOS HUMANOS. PODEM TRABALHAR COMO AGENTES BENEFÍCOS E ÚTEIS, PORÉM EXISTEM TAMBÉM OS BOTS NOCIVOS, CONHECIDOS COMO MALWARES.

OS BOTS DE MALWARE E OS BOTS DA INTERNET PODEM SER PROGRAMADOS/HACKEADOS PARA INVADIR CONTAS DE USUÁRIOS, PROCURAR INFORMAÇÕES DE CONTATO NA INTERNET, PARA ENVIAR SPAMS OU REALIZAR OUTROS ATOS PREJUDICIAIS.

PARA REALIZAR ESTES ATAQUES E DISFARÇAR A ORIGEM DO TRÁFEGO DE ATAQUE, OS ATACANTES PODEM DISTRIBUIR BOTS RUINS EM UMA REDE DE

BOT – OU SEJA, UMA REDE DE BOT. UMA BOTNET É UM NÚMERO DE DISPOSITIVOS CONECTADOS À INTERNET, CADA UM EM EXECUÇÃO UM OU MAIS BOTS, MUITAS VEZES SEM O CONHECIMENTO DOS PROPRIETÁRIOS DO DISPOSITIVO. COMO CADA DISPOSITIVO TEM SEU PRÓPRIO ENDEREÇO IP, O TRÁFEGO DE BOTNET VEM DE INÚMEROS ENDEREÇOS IP, TORNANDO MAIS DIFÍCIL IDENTIFICAR E BLOQUEAR A ORIGEM DO TRÁFEGO DE BOT MALICIOSO. OS BOTNETS PODEM MUITAS VEZES CRESCER USANDO DISPOSITIVOS PARA ENVIAR E-MAILS DE SPAM, O QUE PODE INFECTAR MAIS MÁQUINAS.

ENQUANTO OS BOTS MALWARE CRIAM PROBLEMAS E PROBLEMAS PARA AS ORGANIZAÇÕES, OS PERIGOS PARA OS CONSUMIDORES INCLUEM O SEU POTENCIAL PARA REALIZAR ROUBO DE DADOS E IDENTIDADE, KEYLOGGING DE INFORMAÇÕES SENSÍVEIS COMO SENHAS, DETALHES BANCÁRIOS E ENDEREÇOS; E PHISHING.

OS ROBÔS MALICIOSOS PODEM FACILMENTE PASSAR DESPERCEBIDOS. ELES SÃO FACILMENTE ESCONDIDOS DENTRO DE UM COMPUTADOR E MUITAS VEZES TÊM NOMES DE ARQUIVOS E PROCESSOS SIMILARES, SE NÃO IDÊNTICOS AOS ARQUIVOS OU PROCESSOS REGULARES DO SISTEMA.

EXEMPLOS DE BOTS MALICIOSOS INCLUEM OS SPAMBOTS, CHATBOTS MALICIOSOS, BOTS DE COMPARTILHAMENTO DE ARQUIVOS, CREDENTIAL STUFFING OU PREENCHIMENTO DE CREDENCIAIS, DOS OU DDOS BOTS.

OS CRIMINOSOS CIBERNÉTICOS USAM BOTS PARA COMETER UMA INFINIDADE DE DELITOS. ENTRE OS PRINCIPAIS, ESTÃO O ROUBO DE INFORMAÇÕES FINANCEIRAS E PESSOAIS, PARA ATACAR SERVIÇOS NA INTERNET LEGÍTIMOS, PARA EXTORQUIR DINHEIRO DAS VÍTIMAS, DENTRE VÁRIOS OUTROS DELITOS.

DENTRE OS VÁRIOS TIPOS DE BOTS, ESTÃO OS BOTS DE MONITORAMENTO, OS TRANSACIONAIS, OS DOWNLOAD BOTS, DENTRE OUTROS.

TIPICAMENTE, OS BOTS OPERAM ATRAVÉS DE UMA REDE. BOTS QUE PODEM SE COMUNICAR UNS COM OS OUTROS USARÃO SERVIÇOS BASEADOS NA INTERNET PARA FAZÊ-LO – COMO MENSAGENS INSTANTÂNEAS, INTERFACES COMO TWITTERBOTS OU ATRAVÉS DO INTERNET RELAY CHAT (IRC).

OS BOTS SÃO FEITOS A PARTIR DE CONJUNTOS DE ALGORITMOS QUE OS AJUDAM A REALIZAR AS SUAS TAREFAS. OS DIFERENTES TIPOS DE BOTS SÃO CONCEBIDOS DE FORMA DIFERENTE PARA REALIZAR UMA GRANDE VARIEDADE DE TAREFAS.

3 – Precondições para o teste:

PARA REALIZAR O TESTE APRESENTADO, NECESSITO DE UMA URNA ELETRÔNICA, TERMINAL DO MESÁRIO, COMPUTADOR OU NOTEBOOK, ALÉM DOS ELEMENTOS DE TRANSMISSÃO DE DADOS (KIT JE-CONNECT), SISTEMAS DE APURAÇÃO E INTEGRIDADE DOS DADOS, DENTRE OUTROS MARCADOS NA PARTE INICIAL DO DOCUMENTO.

4 – Escopo – Superfície de ataque:

O ESCOPO DO TRABALHO SERÁ O JE-CONNECT E A VALIDAÇÃO DA SUA SEGURANÇA EM RELAÇÃO A TRANSMISSÃO INTEGRAL E CONFIDENCIAL DOS DADOS PARA O TSE, INDEPENDENTE SE O COMPUTADOR DO QUAL ESTÁ SENDO UTILIZADO PARA ESSA FUNÇÃO ESTIVER COM O BOT EM EXECUÇÃO NO MOMENTO DA TRANSMISSÃO DE DADOS PARA O ORGÃO MÁXIMO DA JUSTIÇA ELEITORAL (TSE).

5 – Janela de atuação simulada do atacante:

O PLANO DE TESTE ATUARÁ SOB QUATRO PRINCÍPIOS:

1- INTEGRIDADE: A INFORMAÇÃO (VOTOS) DEVE CHEGAR AO DESTINO DE MANEIRA INTEGRA, COM O USO DE ASSINATURAS DIGITAIS, POR EXEMPLO;
2- AUTENTICIDADE: ESSAS INFORMAÇÕES (VOTOS) DEVEM GARANTIR A SUA VERACIDADE, MEDIANTE PROCEDIMENTOS DE AUDITORIA, ATRAVÉS DO USO DA BIOMETRIA, ASSINATURAS DIGITAIS, DENTRE OUTROS MEIOS AUDITÁVEIS.
3 - DISPONIBILIDADE: A INFORMAÇÃO DA QUAL SE PROCURA DEVE ESTAR DISPONÍVEL SEMPRE QUE SE FIZER NECESSÁRIO, SEJA UTILIZANDO FIREWALLS OU BACKUPS;
4- CONFIDENCIALIDADE: ESSAS INFORMAÇÕES DEVEM MANTER A SUA CONFIDENCIALIDADE DO INÍCIO AO FIM DO PROCESSO (MANTENDO O SIGILO DO VOTO), ATRAVÉS DO USO DA CRIPTOGRAFIA;

6 – Pontos de intervenção:

O PRINCIPAL PONTO DE INTERVENÇÃO NESSE PLANO É O USO DO JE-CONNECT, ONDE SERÁ COMPROVADA A SUA EFICÁCIA NA SEGURANÇA, CONFIDENCIALIDADE E INTEGRALIDADE NA TRANSMISSÃO E SIGILO DOS DADOS EM UM COMPUTADOR OU NOTEBOOK DO QUAL EXISTA UM BOT DE MONITORAMENTO EM EXECUÇÃO NO MOMENTO DO SEU FUNCIONAMENTO, QUE MONITORARÁ A EXECUÇÃO DO SISTEMA E TENTARÁ INVADIR E CONSQUENTEMENTE ATRAPALHAR O FUNCIONAMENTO DO SISTEMA, E POSTERIORMENTE, NA VALIDAÇÃO E NA PRESERVAÇÃO DO SIGILO DOS VOTOS.

7 – Passos a serem realizados:

1º DESENVOLVIMENTO E EXECUÇÃO DO BOT DE MONITORAMENTO: PRIMEIRAMENTE, SERIA FEITA A CRIAÇÃO E DESENVOLVIMENTO DO ROBÔ UTILIZANDO A LINGUAGEM PHYTON, PRESENTE EM VÁRIAS ETAPAS DO PROCESSO ELEITORAL;

2ª SIMULAÇÃO DE ELEIÇÃO: ONDE SE ADOTARIA UMA PEQUENA QUANTIDADE DE VOTOS (ENTRE 10 E 20);

3ª APURAÇÃO DOS VOTOS: PARTINDO DESSA PREMISSA, RETIRA-SE A MÍDIA DE VOTAÇÃO DA URNA ELETRÔNICA E INSERE A MESMA NUM COMPUTADOR OU NOTEBOOK COM A PRESENÇA DE UM BOT DE MONITORAMENTO;

4ª EXECUÇÃO DO JE-CONNECT: COM A PRESENÇA DE UM COMPUTADOR OU

NOTEBOOK OPERANDO COM UM BOT DE MONITORAMENTO, SERÁ EFETUADA UMA ANÁLISE, ONDE SE VERIFICARÁ ALGUMA POSSIBILIDADE DE OCORRER A QUEBRA DO SIGILO E DA INTEGRIDADE DOS VOTOS OBTIDOS E SE A EXECUÇÃO DO AGENTE PRESENTE NA MÁQUINA EXECUTORA DO SISTEMA PODE INFLUENCIAR DE ALGUMA FORMA O PROCESSO DE TRANSMISSÃO E SIGILO DOS VOTOS OBTIDOS DURANTE O PLEITO;

8 – Materiais necessários (fornecidos pelo TSE):

- SOFTWARE BÁSICO DA URNA ELETRÔNICA;
- SOFTWARE DE VOTAÇÃO (VOTA);
- URNAS MODELOS 2020 E 2022, COM SEUS RESPECTIVOS *FIRMWARES* E MÍDIAS ELETRÔNICAS;
- SISTEMA DE APOIO ÀS AUDITORIAS DE AUTENTICIDADE E INTEGRIDADE - MÓDULO SORTEIO E MÓDULO VOTAÇÃO;
- VERIFICADOR PRÉ/PÓS-ELEIÇÃO (VPP);
- COMPUTADOR OU NOTEBOOK

9 – Possíveis resultados e impacto:

SE PROCURA COMO RESULTADO QUE SE OBTENHA UMA MAIS UMA CONSTATAÇÃO DA INTEGRALIDADE, CONFIDENCIALIDADE E SEGURANÇA NECESSÁRIAS DURANTE TODO O PROCESSO ELEITORAL, PRINCIPALMENTE DA ETAPA QUE TRATA DA TRANSMISSÃO E VALIDAÇÃO DOS VOTOS OBTIDOS NO COMPUTADOR NA PRESENÇA DO BOT DE MONITORAMENTO DURANTE O PLEITO.

10 – Rastreabilidade:

TESTAR E RASTREAR SE, NA EXECUÇÃO DO BOT, EXISTE ALGUMA ALTERAÇÃO QUE POSSA ACARRETAR A QUEBRA DO SIGILO, DA CONFIDENCIALIDADE E DA INTEGRALIDADE DOS VOTOS DEPOSITADOS PELOS ELEITORES DURANTE TODO O PLEITO.

ESSE RASTREAMENTO SERÁ FEITO ATRAVÉS DA ANÁLISE COMPORTAMENTAL DO CÓDIGO-FONTE E DO PRÓPRIO BOT DE MONITORAMENTO NO MOMENTO DA EXECUÇÃO DO PROCESSO.

11 – Solução proposta:

RECOMENDO QUE O SISTEMA POSSA SER APERFEIÇOADO PARA QUE CERTAS VULNERABILIDADES E O AVANÇO DA TECNOLOGIA (NESSE CASO, PODENDO SER UTILIZADA PARA O LADO NEGATIVO – OS MALWARES), POSSA FAZER COM QUE O TSE POSSA APERFEIÇOAR ETAPAS DO PROCESSO DE VOTAÇÃO, VALIDAÇÃO, AUTENTICIDADE E SIGILO DO VOTO, UTILIZANDO DE MODO OBRIGATÓRIO EQUIPAMENTOS PRÓPRIOS E VALIDADOS DA JUSTIÇA ELEITORAL PARA REALIZAR A TRANSMISSÃO DOS VOTOS, FAZENDO COM QUE O PLEITO SEJA CADA VEZ MAIS SEGURO PARA OS ELEITORES E PARA A PRESERVAÇÃO DA NOSSA DEMOCRACIA.

6

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMACÕES GERAIS

Título do Plano de Teste
Investigação dos mecanismos de validação do Bootloader pela Bios para a proteção da carga segura do SO da UE.

Instituição proponente (se aplicável)

Responsável
Ricardo Antônio Pralon Santos

Investigação dos meios de proteção do bootloader da UE e a possibilidade de substituição por um bootloader "malicioso".

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
(X) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O plano se resume em 2 fases, na primeira fase de investigara os mecanismos de proteção contra a adulteração do bootloader e a possibilidade de substituição por um bootloader "malicioso" . Numa segunda fase , uma vez introduzido um bootloader malicioso, sera substituição da midia interna Flash Drive, por uma de maior capacidade contendo a copia da mídia original e uma segunda partição com um SO "hospedeiro" para qual o bootloader "malicioso' sera direcionado, neste SO hospedeiro rodara um programa Hypevisor que executara em VM o SO e aplicações contida na mídia original sem modificações. Esta imagem contendo o SO Hospedeiro e o programa Hypervisor sera desenvolvido previamente aos testes.

2 – Fundamentação teórica:

É de conhecimento publico que a urna eletrônica tem mecanismos de proteção embutidos que impedem a carga de programas não sejam os gerados pelo TSE. Estes mecanismos podem ser divididos em mecanismos de hardware e de software todos encadeados em uma sequência de validações. Em relação ao software o meio de mais baixo nível é proteção da carga do sistema operacional ou seja a validação do bootloader e sua iteração com a BIOS.

Nos parece que este é o ponto de mais vulnerável porque a BIOS ter um conjunto limitado de rotinas de iteração com o Modulo de Segurança , uma vez que facilidades como leitura de arquivos e partições são implementadas geralmente pelo Sistema Operacional(SO). Nas versões passadas uma das maneiras de protecao usadas para que a iteração BIOS /Bootloader se tornaram mais "especifica' da UE foi alterar o endereço de carga padrão das BIOS PC para outro valor, também existiam alguns HASHs no binario bootloader para permitir sua validação, mas não me parece ainda que o mesmo seja totalmente validado pela BIOS e Modulo de Segurança antes da carga do SO em si, acredito que isto se deve porque geralmente a BIOS é um código proprietário de terceiros , não obrigatoriamente do fabricante da placa mae e a complexidade de fazer uma validação completa talvez não fosse possível dadas limitações da arquitetura do PC ou de maneira custo efetiva. Assim mesmo podendo a validação do bootloader ser feita a posteriori pelo SO , poderia haver uma possibilidade de na hipótese de bootloader malicioso introduzido carregar um programa "Hypervisor" que rodaria o próprio software oficial da Urna incluído o SO original em modo de "máquina virtual". Como a Urna 2022 ao contrário das mais antigas, apresenta a mídia de SO/APLICAÇÃO interna, a Urna esta mídia poderia ser substituída em fase pre processo de votação e antes da lacração. Assim ela se comportaria como uma urna original ate que alguma rotina rodando neste software supervisor poderia por exemplo logar alterações de memoria por exemplo e capturar o sigilo ou a ordem de votação. Na verdade poderia ate trocar a votação alterando diretamente áreas de memoria.

Na teoria uma vez introduzido o bootloader malicioso todas estas possibilidades são abertas e todos as validações em seguir poderia passar porque seria o próprio SO e Aplicação do TSE que estaria executando, apanas sob supervisão de um programa hypervisor que "escutaria" tudo (que por si só é um ataque ao sigilo do voto) e numa segunda fase poderia atacar a votação uma vez se conseguisse identificar os endereços de memoria e disco usados pela aplicação de votação.

3 – Precondições para o teste:

Acesso a urna eletrônica , possibilidade de desmontagem/montagem, acesso a media interna (drive SSD M2).

4 – Escopo – Superfície de ataque:

Urna Eletrônica Completa , Flash de Carga.

5 – Janela de atuação simulada do atacante:

Acesso a Urna Eletrônica antes do Período Eleitoral.

6 – Pontos de intervenção:

Midia Interna da Urna (acesso ao Drive SSD M2) , Bios, extensão da Bios)

Ideal : acesso aos binários e extensões de Bios da Urna (arquivos .bin).

Pode ser necessário desabilitar Hardware de reset da URNA (numa condição no "mundo real" isto poderia ser feito com corte de trilhas dificilmente identificavel) mas não sera mandatório nestes testes.

7 – Passos a serem realizados:

1) O atacante tem acesso a uma urna eletrônica antes do período eleitoral, e se necessario faz a troca do drive SSD M2 por um de maior capacidade.

2) Neste novo Drive SSD M2 existem basicamente 2 partições, na primeira seria a copia da imagem disco original no formato binário sem alterações , na segunda ele instala o SO "hospedeiro" do programa Hypervisor.

3) O atacante substitui o bootloader original por um bootloader comprometido , que vai dar carga no SO "hospedeiro" na segunda partição que por sua vez carregara o software Hypervisor que por sua vez carrega o a imagem de disco contida na primeira partição, incluindo o bootloader original

4) A partir da ai o SO e Aplicação da UE rodam normalmente como tendo acesso transparente ao hardware da urna pelos mesmos endereços de IO mapeados normalmente pela máquina virtual incluído interface VGA, USBs e IOs. No caso mesmo a Bios original podem ser mapeados nos endereços virtuais fornecido pela VM.

8 – Materiais necessários (fornecidos pelo TSE):

Acesso a Urna Eletrônica, ferramentas de desmontagem,

PC com Linux ou Windows instalado

Conversor USB SSD M2 (no padrão do Flash Drive contido no hardware da urna) para acesso a midia interna da UE através do PC. (o investigador pretende levar uma mídia Drive SSD M2 de maior capacidade)

9 – Possíveis resultados e impacto:

Na teoria uma vez introduzido o bootloader malicioso e tendo sucesso na carga do SO "hospedeiro" e Programa "hypervisor" muitas possibilidades de ataque são abertas e todas as validações em seguir poderiam passar sem retornar erros , uma vez que seria o próprio SO e Aplicação do TSE que estaria executando na VM mas sob a supervisão de um programa hypervisor que "escutaria" e logaria tudo que fosse pertinente (que por si só é um ataque ao sigilo) e numa segunda fase poderia atacar a votação uma vez se conseguisse identificar os endereços de memoria e disco usados pela aplicação do TSE qualquer que seja.

10 – Rastreabilidade:

Um ataque bem-sucedido não poderia ser identificado de forma automática, porque em teoria seria o próprio software do TSE que rodaria na Urna "auto virtualizada". Na verdade como o o atacante se instala no Flash Drive interno , possibilidade seria o sacando e passando por um utilitário de disco para identificação da partição , ou se dando boot pelo cartão/disco usb externo e rodando um utilitário de validação de disco , todo outro teste realizado pelo aplicação do TSE embutido poderia ser enganado porque inspecionara o disco da maquina virtual (VM). Num ataque mais elaborado o próprio SO "hospedeiro" poderia se alto apagar após uma determinada data e restaurar o bootloader original.

11 – Solução proposta:

Uma solução poderia melhorar a forma como o bootloader é checado, ou seja checá-lo totalmente a priori, uma vez que o Modulo de segurança precisa do SO para se comunicar com o que esta efetivamente gravado no disco. Na verdade eu tenho conhecimento do Hardware da Urna 2012, no qual o processador do Modulo de segurança não tinha acesso ao espaço de endereços dos barramentos de memória e IO dos periféricos do PC. Se ele tivesse este acesso, ele poderia ler diretamente o bootloader do disco e fazer ele mesmo sua validação.

gov.br Documento assinado digitalmente
RICARDO ANTONIO PRALON SANTOS
Data: 27/10/2023 19:24:15-0300
Verifique em https://validar.iti.gov.br

5

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

USBExploit – acesso a dados da urna através da porta USB.

Instituição proponente (se aplicável)

ATITUS Educação – Faculdade Meridional

Responsável

Marcos Roberto dos Santos, Eduardo Bido, Rhayra Rodrigues Fiorentin, Leandro Caletti, Rafael Nollda Silva

Resumo do plano (máximo de 120 caracteres)

Captura de informações da urna através da conexão de um cabo console ou adaptador USB que possibilite acesso a dados.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(X) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Será conectado a urna eletrônica um cabo USB com conexão Ethernet ou Serial, com o intuito de gerar uma conexão, a fim de coletar dados da urna, bem como dos votos inseridos.

2 – Fundamentação teórica:

Na apresentação da urna eletrônica na fase de inspeção do código fonte foi nos passado a possibilidade de utilização das portas usb para acoplar uma impressora e nesta fazer a impressão do voto, gerando assim um comprovante. A partir desta informação temos a possibilidade de conectar um cabo adaptador usb/rs232 do computador do atacante a juma urna, utilizando softwares de emulação de porta console e com isso obter acesso ao sistema operacional da urna, capturando os dados tanto em memoria quando nas midias de armazenamento. Também a possibilidade de com esta técnica fazer a impressão dos votos em arquivos e assim lê-los posteriormente.

Outro ponto a ser explorado é a conexão de um adaptador de rede usb em uma das portas da urna criando assim uma conexão entre o computador do atacante e a urna, possibilitando o acesso ao sistema operacional e com isso a captura dos dados da urna, dados em memória, bem como as chaves armazenadas nas mídias.

3 – Precondições para o teste:

Acesso a urna eletrônica.

4 – Escopo – Superfície de ataque:

Será afetado apenas uma urna.

5 – Janela de atuação simulada do atacante:

Momento pré eleição, para testes de conexão de rede com a urna através dos conectores USB,e pós eleição para conferencia dos registros.

6 – Pontos de intervenção:

Momento de transporte da urna, por exemplo.

7 – Passos a serem realizados:

1: Atacante conectará um cabo console em uma das portas da urna
2: Execução de um software para obter acesso ao sistema operacional
3: Execução de um software para validar os dados em memória e/ou capturar os votos impressos no spool de impressão e captura das chaves de assinatura.
4: Se apropriar dos dados da urna bem como as chaves de assinatura

8 – Materiais necessários (fornecidos pelo TSE):

Urna Eletrônica 2020;

9 – Possíveis resultados e impacto:

Obtenção de dados da urna, tanto das chaves disponíveis no SO, quanto o arquivo com os votos de cada eleitor.

10 – Rastreabilidade:

Execução de uma checagem de conexão em um dispositivo nas portas usb.

11 – Solução proposta:

Não reconhecer dispositivos conectados a urna de maneira plug and play, sejam eles pendrives ou mesmo conectores de rede ou serial.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

COMISSÃO REGULADORA

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de shell a partir de um dispositivo USB

Instituição proponente (se aplicável)
ATITUS - Educacional

Responsável
Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili, André Izolani Rien, Brayan Vanz de Oliveira

Resumo do plano (máximo de 120 caracteres)
Abertura de um shell no sistema operacional responsável pela comunicação JE-Connect para obter acesso a rede do TSE.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
Connect) ( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
arquivos
(x) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
(x) Transmissão de arquivos (Kit JE

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(x) Transmissão de
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Será acessada a rede do TSE através de um shell executado por outro Pen drive conectado no computador que fará a transmissão dos dados.

2 – Fundamentação teórica:

Uma breve amostra foi apresentada na fase de inspeção, demonstrando a inicialização de um pen drive contendo o sistema operacional, gostaríamos de testar mais a fundo as possibilidades de execução de comandos e scripts através de outros dispositivos USBs para mitigar esta conexão entre o JE-Connect e o TSE e com isso obter acesso tanto rede do TSE, quanto as chaves de envio da mídia de carga. Este pode ser classificado no Mitre Att&CK nas técnicas: TA0008, T1134 e também T1037.

https://attack.mitre.org/tactics/TA0008/
https://attack.mitre.org/techniques/T1134/
https://attack.mitre.org/techniques/T1037/

3 – Precondições para o teste:

Acesso ao computador responsável pelo envio das informações ao TSE

4 – Escopo – Superfície de ataque:

Será afetado apenas o computador com o sistema JE-Connect rodando

5 – Janela de atuação simulada do atacante:

Momento do envio das informações ao TSE

6 – Pontos de intervenção:

Momento de envio dos arquivos para o TSE.

7 – Passos a serem realizados:

1: Atacante conecta o pendrive no computador responsável pelo envio dos dados;
2: Executa abertura do shell;
3: Executa a enumeração da rede;
4: Aplica exploits para permitir o acesso;

8 – Materiais necessários (fornecidos pelo TSE):

Computador com o sistema de envio dos arquivos;
Pen drives com sistema operacional e Token de acesso ao JE-Connect

9 – Possíveis resultados e impacto:

Obter acesso a rede do TSE o que possibilitaria a movimentação lateral e/ou escalada de privilégios.

10 – Rastreabilidade:

A identificação da movimentação lateral e do acesso aos computadores.

11 – Solução proposta:

Segundo o TSE a solução já é aplicada, porém como na inspeção dos códigos não foi possível testar, gostaríamos de ter a certeza de que o processo ocorre da maneira relatada.

•

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Captura do Video transmitido no display, com a alteração dos cabos trasnmissores
Instituição proponente (se aplicável) ATITUS - Educacional
Responsável Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili, André Izolani Rien, Brayan Vanz de Oliveira
Resumo do plano (máximo de 120 caracteres) Abrir a Urna e substituir o cabo HDMI para outro cabo que possua um dispositivo, o qual remeta a imagem para outro dispositivos conectados via Bluetooth
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
(X) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
(X) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Será aberta a Urna eletronica, para alterção do cabo o qual transmite as imagens para o display, para um cabo acoplado a um dispositivo, o qual permita a trasmissão de imagens para outros dispositivos, conectados via Wifi e ou Bluetooth

2 – Fundamentação teórica:

Com aplicação de tecnicas de Hardware hacking, será susbtituido o cabo HDMI, o qual é responsavel pela transmissão da imagem da placa, ate o terminal (display), para outro cabo, o qual ainda permitira a passagem da imagem, porem por este cabo estar conectado a outro dispositivo independete, permitira o envio destas imagens para outros dispositivos conectados a ele.

3 – Precondições para o teste:

Urna eletronica

4 – Escopo – Superfície de ataque:

Será afetado apenas uma urna em uma seção

5 – Janela de atuação simulada do atacante:

Como sabe-se que as urnas eletrônicas, são distribuidas antes do dia da eleição,o individuo mal intencionado, pode fazer a alteração das partes internas, para que assim o mesmo consiga capturar informações, sobre quais os candidatos, as pessoas estão vontando, assim podendo manipular uma possivel compra de votos. Tal situação acarreta na quebra do prncipio da Confidencialidade

6 – Pontos de intervenção:

Visto que para realizar a devida troca, é necessário um curto espaço de tempo, e sabendo onde as urnas são armazenadas, fica a critério do atacante onde realizar a substituição

7 – Passos a serem realizados:

1: Atacante descobre o local onde serão armazenadas as urnas, ou ate mesmo onde ja serão pre alacadas nas suas devidas sessões;
2: Executa a abertura da urna;
3: Substitui o cabo HDMI correto, para o cabo HDMI modificado;
4: Em um momento qualquer, o criminoso, desloca-se para o local de votação e de lá acessa o dispositovo alocado no interior da maquina e assim passa a verifica em quais candidatos as pessoas estão vontando, podendo ter um controle sobre uma possivel compra de votos

8 – Materiais necessários (fornecidos pelo TSE):

Urna Eletronica 2020;
Cabine de Votação;

9 – Possíveis resultados e impacto:

Quebra do sigilo do voto, o que de acordo com o edital é caracterizado como fraude. Como Impacto, a quebra de confiança no processo eleitoral.

3

10 – Rastreabilidade:

Como este procedimento depende de abrir urna pode ser que algum lacre seja danificado e visivelmente percebido, fazendo com que o presidente da secão eleitoral solicite a substituição da urna.

11 – Solução proposta:

Ao inves de a Urna usar de cabos HDMI, para a trasmissão da imagem da placa ate o display, poderia usar de cabos, comuns para passar dados criptografados, ate a uma placa acoplada diretamente ao display, a qual faria descriptografida dos dados e mostraria a imagem

•

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Adulteração no JE Connect

Instituição proponente (se aplicável)

Responsável
Vitor Aloisio do Nascimento Guia

Resumo do plano (máximo de 120 caracteres)
Garantir que não seja possível obter privilégios de usuário root na distro Linux do MSE de forma a adulterar o JEC.

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos

(X) Geração de mídias
(X) Carga da urna eletrônica
(X) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(X) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

DETALHAMENTO DO TESTE

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

1 – Descrição geral do plano:

Este plano tem como finalidade 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).

2 – Fundamentação teórica:

O Kit JE Connect é desenvolvido com softwares de código fonte aberto, o que possibilita a análise e contribuições de desenvolvedores de todo o mundo para aprimorá-lo. No entanto, essa abertura também implica que eventuais falhas em seu código fiquem visíveis e possam ser exploradas por indivíduos mal-intencionados.

3 – Precondições para o teste:

A – Acesso Memória de Resultados (MR).
B – Acesso ao Kit JE Connect.

4 – Escopo – Superfície de ataque:

A - Kernel Linux.
B - Pacotes do Debian.
C - Software JE Connect.
D - Mídia com Sistema Embarcado (MSE).
E - Memória de Resultados (MR).

5 – Janela de atuação simulada do atacante:

O teste será realizado em um período de um dia, abrangendo o dia da eleição, simulando as condições durante as eleições.

6 – Pontos de intervenção:

A - Tentativas de privilégio de usuário root não autorizado.
B - Tentativas de adulteração do software JE Connect.
C - Tentativas de adulteração no dados da Memória de Resultados (MR).
D - Tentativas de transmissão de dados adulterados.

7 – Passos a serem realizados:

A - Preparação da urna eletrônica.
B - Simulação de votação.
C - Obtenção de Memória de Resultados (MR).
D - Preparação do ambiente JE Connect.
E - Injeção de um pendrive bootavel com Kali Linux.
F - Análise do disco em busca de chaves de recuperação.
G - Obtenção de privilegio de usuário root.
H - Adulteração do software JE Connect.
I - Adulteração de dados do MR.
J - Transmissão de dados adulterados.

8 – Materiais necessários (fornecidos pelo TSE):

A - Um computador com pelo menos quatro portas USB disponíveis para boot.
B - Urna eletrônica para teste.
C - Pendrive de Memória de Resultado (MR).
D - Pendrives MSE e MC do Kit JE Connect.
E - Código PIN do JEC.

9 – Possíveis resultados e impacto:

A - Acesso de usuário root não autorizado.
B - Instalação de softwares maliciosos.
C - Acesso e modificação de dados sigilosos.
D - Adulteração do software JE Connect.
E - Adulteração de dados do MR.
F - Transmissão de dados adulterados.

10 – Rastreabilidade:

A - Relatórios detalhados de teste.
B - Documentação de vulnerabilidades identificadas.
C - Recomendações para correção de vulnerabilidades.

11 – Solução proposta:

Com base nos resultados do teste, será elaborada recomendações para que o TSE implemente as correções e melhorias necessárias no Kit JE Connnet para garantir sua segurança e integridade durante o processo eleitoral.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConect.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araujo Carvalho

Resumo do teste (máximo de 120 caracteres)
A linguagem de programação Python apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo Python usa a função *str.format* e *string-f* na formatação de string. essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-9930 – HORÁRIO DE FUNCIONAMENTO: DAS 13H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações no Python no software JEConect para a função *str.format()* e para funções *f-string()*.

2 – Fundamentação teórica:

Isso ocorre porque as funções de formatação de *string* podem acessar objetos de atributos, que podem vazar informações confidenciais, e/ou pode incluir um código executável nelas.

3 – Precondições para o teste:

O código fonte do JEConect em Python que utilizam as funções *str.format()* e/ou *f-string()*.

4 – Escopo – Superfície de ataque:

As funções *str.format()* e *f-string()* será utilizada para inserção de string de dados, e obter como resultado o acesso as informação confidenciais do JEConect.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar as funções *str.format()* e/ou *f-string()* no Python no software JEConect.

7 – Passos a serem realizados:

I. Identificar no código fonte as funções *str.format()* e/ou *f-string()*.
II. Testar para cada função identificada:
   a. Confidencialidade: o acesso as informações confidenciais por meio destas funções;
   b. Integridade: alterar informações confidenciais;
   c. Disponibilidade: interferir na transferência das informações confidenciais;
III. Repetir o passo II até testar todas as funções identificadas.
IV. Obtendo sucesso: registrar onde, como, e quais vulnerabilidades.

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto nos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) das informações da aplicação JEConect.

10 – Rastreabilidade:

O resultado final seria a rastreabilidade dos requisitos de segurança do código fonte em Python da aplicação JEConect para as funções *str.format()* e/ou *f-string()*.

11 – Solução proposta:

Esta solução proposta identificará:

- as vulnerabilidades no código fonte,
- como acontece,
- quais requisitos de segurança não atendidos,
- e permitirá a correção deste código fonte.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConect.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araujo Carvalho

Resumo do teste (máximo de 120 caracteres)
Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, onde um invasor pode abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas ou contornar firewalls.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-9830 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações nos módulos de processamento XML das interfaces do Python do pacote xml no software JEConect.

2 – Fundamentação teórica:

Isso ocorre porque os módulos do pacote xml exigem que haja pelo menos um analisador XML compatível com SAX-compliant, e o analisador Expat, que está incluso no Python, portanto o módulo xml.parsers.expat está sempre disponível, e podem acessar informações confidenciais.

3 – Precondições para o teste:

O código fonte do JEConect em Python que utilizam as funções do pacote *xml*.

4 – Escopo – Superfície de ataque:

O escopo/superfície de ataque é as funções do pacote *xml* no módulo xml.parsers.expat, que serão violadas para realizar acesso aos arquivos locais para acessar ou alterar informações confidenciais.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar as funções do pacote *xml* no módulo *xml.parsers.expat* do Python no software JEConect.

7 – Passos a serem realizados:

I. Identificar no código fonte as funções do módulo *xml.parsers.expat* utilizadas.
II. Testar para cada função identificada:
    a. Confidencialidade: o acesso as informações confidenciais por meio destas funções;
    b. Integridade: alterar informações confidenciais;
    c. Disponibilidade: interferir na transferência das informações confidenciais;
III. Repetir o passo II até testar todas as funções identificadas.
IV. Obtendo sucesso: registrar onde, como, e quais vulnerabilidades.

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto nos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) das informações do JEConect.

10 – Rastreabilidade:

O resultado final seria a rastreabilidade dos requisitos de segurança do código fonte em Python da aplicação JEConect para as funções funções do pacote *xml* no módulo *xml.parsers.expat*.

11 – Solução proposta:

Esta solução proposta identificará:

- as vulnerabilidades no código fonte,
- como acontece,
- quais requisitos de segurança não atendidos,
- e permitirá a correção deste código fonte.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações na função *urllib.parse* do Python no Software JEConect.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araujo Carvalho

Resumo do teste (máximo de 120 caracteres)
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.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-9830 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações na função *urllib.parse* da linguagem de programação 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.

2 – Fundamentação teórica:

Isso ocorre porque a função *urllib.parse* é uma função de análise amplamente usada, que torna possível dividir URLs em seus constituintes ou, alternativamente, combinar os componentes em uma string de URL. E tem como resultado da falta de validação de entrada, levando a um cenário em que é possível contornar os métodos de lista de bloqueio fornecendo um URL que começa com caracteres em branco (por exemplo, " https://youtube[.] com"). Essa vulnerabilidade ajudaria um invasor a ignorar as proteções definidas pelo desenvolvedor para esquema e host, e espera-se que essa vulnerabilidade apareça em uma ampla variedade de cenários."

3 – Precondições para o teste:

O código fonte do JEConect em Python que utilizam a função *urllib.parse* do Python.

4 – Escopo – Superfície de ataque:

O escopo/superfície de ataque é a função *urllib.parse*, que serão violadas para realizar acesso aos arquivos locais para acessar ou alterar informações confidenciais.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar as funções *urllib.parse* do Python no software JEConect.

7 – Passos a serem realizados:

I. Identificar a vulnerabilidade no código fonte da função *urllib.parse*.
II. Testar a função para:
   a. Confidencialidade: o acesso as informações confidenciais por meio destas funções;
   b. Integridade: alterar informações confidenciais;
   c. Disponibilidade: interferir na transferência das informações confidenciais;
III. Repetir o passo II até obter sucesso.
IV. Obtendo sucesso: registrar onde, como, e quais vulnerabilidades.

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto nos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) das informações do JEConect.

10 – Rastreabilidade:

O resultado final seria a rastreabilidade dos requisitos de segurança do código fonte em Python da aplicação JEConect para a função *urllib.parse*.

11 – Solução proposta:

Esta solução proposta identificará:

- as vulnerabilidades no código fonte,
- como acontece,
- quais requisitos de segurança não atendidos,
- e permitirá a correção deste código fonte.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConect.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araújo Carvalho

Resumo do teste (máximo de 120 caracteres)
Executar 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__*".

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9830 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações na execução de um *exploit* que permite usar código Python especialmente vinculado para iniciar uma chamada para a memoria já liberada em Python, e executar comandos *"/bin/sh"*.

2 – Fundamentação teórica:

O *exploit* pode ser utilizado para contornar mecanismos de isolamento em vários serviços e chamadas de ambientes, como ambientes de aprendizados, shells online, controladores embutidos, etc., e desabilitar métodos de acesso como *os.system*, explorando vulnerabilidade no CPython, e como os módulos de segurança PIE, RELRO e CET ativados.

3 – Precondições para o teste:

O código fonte do JEConect em Python.

4 – Escopo – Superfície de ataque:

O exploit se resume a obter informações sobre o endereço de uma das funções do código Python no código executável *CPython*, e realizar acesso aos arquivos locais ou alterar informações confidenciais.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar os endereços de memoria do Python por meio do CPython no software JEConect.

7 – Passos a serem realizados:

I. Com base no calculo do: endereço base da função binaria *CPython* na memória, e do endereço da função *system*(), ou seu stub PLT, na instância *libc*.
II. Uma transição direta para um determinado sistema de endereços é iniciada substituindo o ponteiro do primeiro argumento pela *string* "/bin/sh".
    a. Criar acesso ao buffer liberado em "*ob_item*", alocado no mesmo local que o buffer foi liberado.
    b. Criar duas "visões" diferentes no mesmo pedaço de memória.
        i. Uma visão, a visão de memória, como uma matriz de bytes, na qual podemos escrever ou ler arbitrariamente.
        ii. A segunda visão é uma lista, que criamos com falsos ponteiros do *PyObject*. Utilizando a implementação para PoC, e acessar os objetos contidos em *PyObject**, indexando a lista.
    c. Violar confidencialidade: o acesso as informações confidenciais por meio destas funções;
    d. Violar integridade: alterar informações confidenciais;
    e. Violar disponibilidade: interferir na transferência das informações confidenciais;

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto nos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) das informações do JEConect.

10 – Rastreabilidade:

O resultado final seria a rastreabilidade dos requisitos de segurança do código fonte em Python da aplicação JEConect.

11 – Solução proposta:

Esta solução proposta identificará:

- as vulnerabilidades no código fonte,
- como acontece,
- quais requisitos de segurança não atendidos,
- e permitirá a correção deste código fonte.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConect.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araújo Carvalho

Resumo do teste (máximo de 120 caracteres)
Executar vários *exploits* funcionais para permitir chamadas de: comandos e funções as bibliotecas nativas e externas do Python, e obter acesso as informações.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações na execução de vários *exploits* que permite executar código Python, como comandos *"/bin/sh"*.

2 – Fundamentação teórica:

O *exploit* pode ser utilizado para contornar mecanismos de isolamento em vários serviços e chamadas de ambientes, explorando tais vulnerabilidade do *Python*, e se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.

3 – Precondições para o teste:

O código fonte do JEConect em Python.

4 – Escopo – Superfície de ataque:

Os *exploits* se resumem a obter acesso não autorizado as informações e aos arquivos locais no *Python*.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar o código fonte e suas bibliotecas nativas e externas do Python por meio de *exploits* no software JEConect.

7 – Passos a serem realizados:

I. Com base em vários *exploits* que acessam endereços bases de objetos no Python.
II. Fazendo uma transição direta para um determinado sistema de endereços é possível modificar os ponteiros de tais objetos para argumento como *string* "/bin/sh".
    a. Criando o acesso as informações de objetos dos "*ob_item*" para objetos contidos no *PyObject*.
    b. Obter acesso ao certificado para conexão com a rede do TSE.
III. Se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.
    a. Violar confidencialidade: o acesso as informações por meio destes *exploits*;
    b. Violar integridade: transferir informações não certificadas;
    c. Violar disponibilidade: interferir na transferência das informações certificadas;

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto na quebra dos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) para informações do JEConect, e se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.

10 – Rastreabilidade:

O resultado final seria a rastreabilidade dos requisitos de segurança do código fonte em Python da aplicação JEConect.

11 – Solução proposta:

Esta solução proposta identificará:

- as vulnerabilidades no código fonte,
- como acontece,
- quais requisitos de segurança não atendidos,
- e permitirá a correção deste código fonte.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste
Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita.

Instituição proponente (se aplicável)
Faculdade de Computação
Universidade Federal do Mato Grosso do Sul

Responsável
Prof. Dr. Carlos Alberto da Silva
Ian Martinez Zimmermann
Matheus Vianna Silveira
Mario de Araújo Carvalho

Resumo do teste (máximo de 120 caracteres)
Executar vários *exploits* funcionais para permitir chamadas de: comandos e obter acesso as informações, com escalada de privilégio.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
(X) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
( ) Urna eletrônica
(X) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(X) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Este plano de teste pretende violar a confidencialidade, integridade e disponibilidade das informações na execução de vários *exploits* que permite executar código, como comandos *"/bin/sh"*.

2 – Fundamentação teórica:

O *exploit* pode ser utilizado para contornar mecanismos de isolamento em vários serviços e chamadas de ambientes, explorando tais vulnerabilidade da *OpenVPN*, e se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.

3 – Precondições para o teste:

O código fonte do JEConect e acesso a um kit JE Connect autorizado.

4 – Escopo – Superfície de ataque:

Os *exploits* se resumem a obter acesso não autorizado as informações e possível interceptação/alteração de informação.

5 – Janela de atuação simulada do atacante:

- Violar a confidencialidade dos dados com acesso a informações confidenciais.
- Violar a integridade dos dados com alteração de informações confidenciais.
- Violar a disponibilidade dos dados com interferência na transferência das informações confidenciais.

6 – Pontos de intervenção:

Violar as camadas de OpenVPN criadas pelo JEConnect que encapsulam a informação.

7 – Passos a serem realizados:

I. Explorar e observar *exploits* que exploram vulnerabilidades do OpenVPN.
II. Fazer uso do *exploits, sendo possível execução de comandos e extração de configurações e informações da VPN.*
III. Se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.
   a. Violar confidencialidade: o acesso as informações por meio destes *exploits*;
   b. Violar integridade: transferir informações não certificadas;
   c. Violar disponibilidade: interferir na transferência das informações certificadas;

8 – Materiais necessários (fornecidos pelo TSE):

- 1 desktop com Kali Linux, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 desktop com Black arch, versão 64, bootável por pen-drive, ou uma maquina virtual (VM).
- 1 pen-drive com JEConect habilitado para conexão e transmissão de arquivos.
- 1 VM que seja possível executar o KIT JE Connect.
- 2 pen-drive's de urnas eletrônicas com votação encerradas para transmissão no JEconect

9 – Possíveis resultados e impacto:

Impacto direto na quebra dos princípios de segurança (Confidencialidade, Integridade e Disponibilidade) para informações do JEConect, e se conectar diretamente ao TSE sem uma mídia segura e explorar os softwares interno do TSE.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-0830 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

10 – Rastreabilidade:

Seria possível verificar rastro de execução de códigos anormais, possíveis pacotes "não formatados" chegando ao destino.

11 – Solução proposta:

Explorando a(s) vulnerabilidade(s) seria possível adicionar pontos de controle e serialização de dados, além de um possível reforço no código para maior proteção da VPN, em possíveis novas vulnerabilidades.

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

COMISSÃO REGULADORA

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA Y 101, FAX: 3030-0830 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Executar código espúrio na Urna Eletrônica modelo 2020
Instituição proponente (se aplicável) Polícia Federal
Responsável Galileu Batista de Sousa
Resumo do plano (máximo de 120 caracteres) Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (Time Of Check to Time Of Use), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
(x) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
(x) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
(x) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O teste visa verificar a possibilidade de se trocar um arquivo, utilizado pela urna eletrônica, após a validação de sua assinatura.

2 – Fundamentação teórica:

Com o advento da utilização das assinaturas digitais para verificar a integridade dos arquivos tornou-se muito difícil executar ataques que simplesmente alteram o seu conteúdo, já que eles terão sua assinatura verificada. Entretanto, dependendo de como essa verificação é implementada, ela pode abrir espaço para os ataques do tipo TOCTOU, onde o conteúdo de um arquivo é alterado após a verificação de sua assinatura digital.

Hoje existem diversos equipamentos que podem auxiliar na execução desse tipo de ataque. O USBArmory MK II é um desses equipamentos. Trata-se de um computador inteiro rodando um dispositivo que aparenta ser um pen drive. Ele é capaz de simular diversos dispositivos USB, tais como teclados, placas de rede e dispositivos de armazenamento computacional. Mais informações sobre o USBArmory podem ser obtidas no site: https://inversepath.com/usbarmory.

3 – Precondições para o teste:

1. Uma Urna Eletrônica, modelo 2020;
2. Uma mídia de carga funcional;
3. USBArmory MK II (levado pelos Peritos);
4. Cabo extensor USB (levado pelos Peritos);
5. Computador com software de apoio capaz de gerar uma mídia de carga;
6. Estação de trabalho contendo:
    a. Ambiente para execução de máquina virtual;
    b. Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);
    c. Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos).

4 – Escopo – Superfície de ataque:

Urna eletrônica, modelo 2020, e respectiva mídia de carga.

5 – Janela de atuação simulada do atacante:

Acesso físico a uma Urna Eletrônica, modelo 2020, junto a uma respectiva mídia de carga.

6 – Pontos de intervenção:

Mídia de carga.

7 – Passos a serem realizados:

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 possa ser executado;
5. Realizar uma nova carga executando o ataque TOCTOU, onde um arquivo será substituído após a sua validação.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna modelo 2020;
2. Midia de carga da urna 2020;
3. Computador com software de apoio capaz de gerar uma mídia de carga;
4. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
5. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Execução de um código arbitrário na urna, possibilitando, no limite, execução de um software falso de votação.

10 – Rastreabilidade:

Não identificado.

11 – Solução proposta:

Carregar os artefatos críticos em memória, verificar sua assinatura e utilizar sempre a versão em memória, evitando recarregar o artefato do disco.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020
Instituição proponente (se aplicável) Polícia Federal
Responsável Galileu Batista de Sousa
Resumo do plano (máximo de 120 caracteres) Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(x) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O teste visa verificar a possibilidade de extrair a chave que cifra/decifra o kernel nas urnas modelo 2020.

2 – Fundamentação teórica:

A partir da análise do código fonte efetuada pelos Peritos, foi constatado que a chave que cifra/decifra o kernel encontra-se cifrada no disco. No momento do boot da urna, essa chave é decifrada pelo hardware de segurança e fica armazenada na memória RAM, sendo essa chave igual para todas as urnas. Caso seja executado um código malicioso na urna capaz de ler a memória RAM, essa chave pode ser capturada.

3 – Precondições para o teste:

1. Sucesso na execução de código arbitrário na urna;
2. Uma Urna Eletrônica, modelo 2020;
3. Uma mídia de carga funcional;
4. USBArmory MK II (levado pelos Peritos);
5. Cabo extensor USB (levado pelos Peritos);
6. Estação de trabalho contendo:
    a. Ambiente para execução de máquina virtual;
    b. Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);
    c. Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos).

4 – Escopo – Superfície de ataque:

Urna eletrônica, modelo 2020, e respectiva mídia de carga.

5 – Janela de atuação simulada do atacante:

Acesso a uma Urna Eletrônica, modelo 2020, junto a uma respectiva mídia de carga.

6 – Pontos de intervenção:

Urna Eletrônica e mídia de carga.

7 – Passos a serem realizados:

1. Rodar um código arbitrário a partir da mídia de carga simulada (USBArmory);
2. Executar um processo capaz de acessar a chave do kernel.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna modelo 2020;
2. Mídia de carga da urna 2020;
3. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
4. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Com a obtenção da chave que cifra/decifra o kernel, teoricamente seria possível mudar o kernel da urna e derivar outras chaves que são geradas a partir dessa chave.

10 – Rastreabilidade:

Não identificado.

11 – Solução proposta:

Não deixar a chave que cifra/decifra o kernel em memória o tempo todo. Utilizar o hardware de segurança toda vez que precisar acessar a chave.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto
Instituição proponente (se aplicável) Polícia Federal
Responsável Galileu Batista de Sousa
Resumo do plano (máximo de 120 caracteres) Caso seja possível extrair a chave que cifra/decifra o kernel da urna, uma chave derivada dessa poderá ser utilizada para cifrar um RDV falso. Posteriormente esse RDV falso poderia ser carregado em uma urna de contingência.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
(x) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
(x) Software de Votação (VOTA)
(x) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(x) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Caso a chave que cifra/decifra o kernel da urna seja obtida, teoricamente seria possível gerar um Registro Digital de Voto falso utilizando essa chave.

2 – Fundamentação teórica:

A partir da análise do código fonte efetuada pelos Peritos, foi constatado que o Registro Digital do Voto (RDV) é cifrado com uma chave derivada da chave que cifra/decifra o kernel da Urna. No caso de descoberta dessa chave, teoricamente seria possível alterar um RDV e depois utilizar uma urna de contingência para homologar, assinar e propagar o RDV falso.

3 – Precondições para o teste:

1. Chave que cifra/decifra o kernel da urna modelo 2020 (obtida em plano de teste anterior);
2. Adaptadores (SATA/m.2/NVME/USB) (levados pelos Peritos);
3. Uma Urna Eletrônica, modelo 2020;
4. Uma Urna Eletrônica de contingência, modelo 2020;
5. Estação de trabalho contendo:
    a. Ambiente para execução de máquina virtual;
    b. Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);
    c. Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos).

4 – Escopo – Superfície de ataque:

Urna eletrônica, modelo 2020, respectiva mídia de carga e flash externa.

5 – Janela de atuação simulada do atacante:

Acesso a uma Urna Eletrônica, modelo 2020, junto a uma respectiva mídia de carga.

6 – Pontos de intervenção:

Flash externa.

7 – Passos a serem realizados:

1. Executar um programa que utilize a chave do kernel como parâmetro e seja capaz de gerar um RDV válido.
2. Salvar esse RDV na flash externa e utilizar essa flash na urna de contenção.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna modelo 2020;
2. Urna de contingência, também modelo 2020;
3. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
4. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Adulteração do resultado de votação de uma Urna Eletrônica.

10 – Rastreabilidade:

Seria possível constatar divergências entre o RDV da memória interna da urna original e o RDV falso inserido (e aceito) na urna de contenção.

11 – Solução proposta:

Assinar o RDV temporário a cada registro de voto.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI
Instituição proponente (se aplicável) Polícia Federal
Responsável Galileu Batista de Sousa
Resumo do plano (máximo de 120 caracteres) Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo Bitlocker para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.
Sistemas a serem testados

Softwares

(x) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
(x) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo Bitlocker para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.

2 – Fundamentação teórica:

Existem algumas falhas documentadas na literatura que podem ser exploradas para obter a chave do Bitlocker que fica armazenada no TPM do computador, tais como BitLeaker, ataques de DMA e Hardware Debug.

3 – Precondições para o teste:

1. Estação Windows com SIS e GEDAI-UE instalado contendo uma porta PCIe/NVMe livre para uso;
2. Disco rígido adicional para efetuar cópia forense do disco instalado na estação SIS/GEDAI;
3. Placa PCILeech (levada pelos Peritos);
4. Adaptador m.2 para PCIe (levado pelos Peritos);
5. Leitor/gravador de BIOS (levado pelos Peritos);
6. Cabo USB modificado utilizado para depuração utilizando Intel DCI (levado pelos Peritos).
7. Estação de trabalho contendo

   a) Ambiente para execução de máquina virtual;

   b) Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging. (gerada pelos Peritos);

   c) Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging. (gerada pelos Peritos);

4 – Escopo – Superfície de ataque:

Estação desktop com SIS/GEDAI instalados.

5 – Janela de atuação simulada do atacante:

Acesso físico ao computador onde o SIS/GEDAI estão instalados.

6 – Pontos de intervenção:

Estação onde estão instalados o SIS/GEDAI.

7 – Passos a serem realizados:

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.

8 – Materiais necessários (fornecidos pelo TSE):

1. Estação desktop com SIS/GEDAI instalados contendo uma porta PCIe/NVMe livre para uso;
2. Disco rígido adicional para efetuar cópia forense do disco instalado na estação SIS/GEDAI;
3. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
4. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Possibilidade de engenharia reversa dos sistemas SIS/GEDAI.

10 – Rastreabilidade:

Não identificado.

11 – Solução proposta:

Utilizar máquinas que não permitam a alteração dos parâmetros de BIOS necessários para execução do ataque.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Alterar dados / programas nos sistemas SIS/GEDAI

Instituição proponente (se aplicável)

Polícia Federal

Responsável

Galileu Batista de Sousa

Resumo do plano (máximo de 120 caracteres)

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.

Sistemas a serem testados

Softwares

(x) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
(x) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
(x) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Utilizar técnicas avançadas para edição de memória, durante a execução do GEDAI, comprometendo o correto fluxo de informações entre os sistemas.

2 – Fundamentação teórica:

As técnicas que possibilitam edição de memória durante a execução de um programa podem ser empregadas para realizar modificações no comportamento dos programas de modo que realizem operações não previstas/esperadas. Essas modificações podem ser realizadas utilizando softwares de debugging ou hardwares especializados que possibilitam a modificação da memória durante a execução das aplicações.

Dentre essas ferramentas estão os debuggers (Xdbg, OllyDbg, IDA, Ghidra e WinDBG) e o hardware especializado PCILeech (https://github.com/ufrisk/pcileech).

3 – Precondições para o teste:

1. Chave do Bitlocker (obtida em outro plano de testes);
2. Estação Windows com SIS e GEDAI-UE instalado contendo uma porta PCIe/NVMe livre para uso;
3. Placa PCILeech (levada pelos Peritos);
4. Adaptador m.2 para PCIe (levado pelos Peritos);
5. Leitor/gravador de BIOS (levado pelos Peritos);
6. Estação de trabalho contendo:

   a) Ambiente para execução de máquina virtual;

   b) Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);

   c) Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);

   d) Imagem ISO do HIREN´s bootCD disponível (gerada pelos Peritos).

4 – Escopo – Superfície de ataque:

Estação desktop com SIS/GEDAI instalados.

5 – Janela de atuação simulada do atacante:

Acesso físico ao computador onde o SIS/GEDAI estão instalados.

6 – Pontos de intervenção:

Estação onde estão instalados o SIS/GEDAI.

7 – Passos a serem realizados:

1. Instalar a placa PCILeech no desktop onde 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:
    a. Desativar as proteções do Subsistema de Instalação e Segurança (SIS);
    b. Instalar um debugger na máquina;
    c. 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.

8 – Materiais necessários (fornecidos pelo TSE):

1. Estação desktop com SIS/GEDAI instalados contendo uma porta PCIe/NVMe livre para uso;
2. Disco rígido adicional para efetuar cópia forense do disco instalado na estação SIS/GEDAI;
3. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
4. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Possibilidade de criar interrupção do fluxo de dados gerados entre a urna e o seu ecossistema.

10 – Rastreabilidade:

Discrepância entre os dados na urna e nos sistemas do TSE.

11 – Solução proposta:

Fortalecer a segurança contra modificação dos aplicativos e estrutura de dados na máquina do GEDAI, utilizando por exemplo estratégias avançadas de proteção de códigos executáveis.

4

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Ataque de cold boot à Urna Eletrônica
Instituição proponente (se aplicável) Polícia Federal
Responsável Galileu Batista de Sousa
Resumo do plano (máximo de 120 caracteres) Congelamento da memória RAM da urna, objetivando extrair os dados em leitor externo para posterior decodificação.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(x) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
(x) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O ataque de congelamento físico conhecido como cold boot tentará manter os dados armazenados na memória volátil (RAM) para que seja possível extraí-los em um leitor externo. Caso a extração dos dados seja realizada com sucesso, a equipe tentará decodificar dados sensíveis e protegidos.

2 – Fundamentação teórica:

- Artigo de Referência: **https://github.com/DonnchaC/coldboot-attacks/blob/master/coldboot.pdf**

Lest We Remember: Cold Boot Attacks on Encryption Keys - J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten - February 21, 2008, USENIX Security Symposium - http://citp.princeton.edu/memory

Ao contrário da suposição popular, as DRAM[1]s usadas na maioria dos computadores modernos retêm seu conteúdo por vários segundos mesmo após a perda de energia, mesmo em temperatura ambiente e mesmo se removido de uma placa-mãe. Embora as DRAM tornam-se menos confiáveis quando não são atualizadas, seu conteúdo não é apagado imediatamente, persistindo suficientemente para aquisição maliciosa (ou forense) de imagens de memória de todo o sistema em que eram utilizadas. Este fenômeno limita a capacidade de um sistema operacional de proteger chaves criptográficas de um invasor com acesso físico. Reinicializações a frio (cold boot) podem ser utilizadas para executar com sucesso ataques a sistemas populares de criptografia de disco sem uso específico de dispositivos ou materiais especiais. Os tempos de remanência dos dados em memória podem ser aumentados dramaticamente com técnicas simples de resfriamento. É possível utilizar algoritmos para encontrar chaves criptográficas em imagens de memória e também corrigir erros causados pela queda de bits.

[1] Memória DRAM pode ser pensada como um arranjo de células, como uma tabela ou planilha. Estas células são feitas de capacitores e contém um ou mais bits de dados, a depender da configuração do chip. Esta tabela é endereçada através de decodificadores de linha e coluna, que por sua vez recebem seus sinais de geradores de clock, denominados geradores CAS (Column Address Strobe) e RAS (Row Address Strobe). De modo a minimizar o tamanho do pacote de dados, os endereços de linha e coluna são multiplexados em buffers. Por exemplo, se há 11 endereços, então haverá 11 linhas e 11 colunas de buffers. Transistores de acesso chamados "sense amps" ou amplificadores de sinal (numa tradução livre) são conectados a cada coluna de modo a possibilitar as operações de leitura e recuperação do chip. Uma vez que as células são capacitores que se descarregam para cada operação de leitura, o sense amp precisa recuperar ou restaurar o dado ali armazenado antes do fim do ciclo de acesso.
Referência: https://www.eecis.udel.edu/~portnoi/academic/academic-files/dram.html

3 – Precondições para o teste:

1. Urna eletrônica em funcionamento;
2. Acesso físico ao pente de memória RAM da urna para que possa ser possível retirá-lo;
3. Conhecimento do tipo de memória utilizada na urna;
4. Utilização de spray de gás congelante sobre a memória (levado pelos Peritos – certificado pela ANVISA, exemplo DermaFreeze®, Emdutos, registro ANVISA 80409950001);
5. Utilização de máquina de destino leitora, tipicamente um notebook (levado pelos Peritos), preparado e configurado previamente pela equipe, para onde o pente de memória RAM da urna será movido e lido após o congelamento;
6. Estação de trabalho contendo:
   - **a.** Ambiente para execução de máquina virtual;
   - **b.** Imagem de máquina virtual Linux com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos);
   - **c.** Imagem de máquina virtual Windows com diversas ferramentas forenses, desenvolvimento e debugging (gerada pelos Peritos).

4 – Escopo – Superfície de ataque:

O pente de memória RAM da urna.

5 – Janela de atuação simulada do atacante:

Após as urnas inseminadas, um atacante poderia abrir uma urna eletrônica furtada ou roubada para realização deste tipo de ataque. Os dados sensíveis obtidos, como por exemplo chaves de cifragem existentes na memória em tempo de execução, podem potencialmente serem utilizados na elaboração de ataques em maior escala.

6 – Pontos de intervenção:

Urna eletrônica, mais especificamente o pente de memória RAM utilizado pela urna;

7 – Passos a serem realizados:

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. Dar boot na máquina de destino capturando o conteúdo da memória.

8 – Materiais necessários (fornecidos pelo TSE):

1. Urna eletrônica funcional, permitindo acesso físico ao pente da memoria RAM;
2. Pentes adicionais de memória RAM para serem testados;

3. Uma máquina com sistema operacional Windows contendo o software de virtualização VirtualBox e o software forense FTK Imager, que pode ser obtido gratuitamente no sítio da Access Data (www.exterro.com);
4. Uma máquina com sistema operacional Linux distribuição Ubuntu Desktop 22.04 contendo o software de virtualização qEmu.

9 – Possíveis resultados e impacto:

Se efetivo, o ataque permitiria realizar o dump da memória e eventualmente extrair dados relevantes que são decifrados apenas em tempo de execução. Estes dados, a exemplo de chaves criptográficas protegidas, poderiam ser utilizados em ataques de maior escala objetivando por exemplo explorar o kernel protegido por cifragem, ou mesmo alterar os dados do RDV em tempo de execução na urna.

O ataque cold boot usualmente não é um procedimento destrutivo, contudo, não pode ser descartada a hipótese de avaria nos equipamentos envolvidos por envolver intervenções no hardware ligado e em pleno funcionamento.

10 – Rastreabilidade:

Atualmente o único indicativo da possibilidade de ocorrência deste tipo de ataque seria a verificação de rompimento dos lacres físicos existentes nas urnas.

11 – Solução proposta:

1. Impedimento físico da retirada do pente da memória RAM da urna. Algumas soluções sugeridas neste sentido: fixação física do pente da memória RAM da urna por meio de eventuais lacres; resinagem do pente de memória junto à placa-mãe;
2. Cifragem ou obfuscação em tempo de execução das chaves criptográficas e do conteúdo de toda a memória RAM.

5

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Tentativa de Man-in-the-Middle na Comunicação do Teclado com Arduíno.
Instituição proponente (se aplicável)
Responsável Luis Antonio Kowada e respectivo grupo
Resumo do plano (máximo de 120 caracteres) A avaliação tem como propósito testar vulnerabilidades na comunicação entre o teclado e a placa mãe das urnas.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1.– Descrição geral do plano:

O objetivo deste plano é 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.

Uma equipe de especialistas em segurança e eletrônica supervisionará o processo, com a documentação detalhada de todas as etapas. O teste ocorrerá em um ambiente controlado, assegurando que os procedimentos se assemelhem ao ambiente de uma eleição real. Durante o teste, todos os dados transmitidos entre o teclado e a placa-mãe serão registrados para posterior análise.

A análise dos dados capturados incluirá a descriptografia para avaliar a eficácia do protocolo criptográfico, bem como a identificação de qualquer padrão incomum ou comportamento suspeito.

Os resultados do teste serão compilados em um relatório detalhado, que será apresentado às autoridades eleitorais. Qualquer descoberta de vulnerabilidades será acompanhada de recomendações para aprimorar a segurança do sistema. A comunicação constante com as partes interessadas será mantida ao longo do processo, garantindo transparência e conformidade com todas as leis e regulamentos aplicáveis.

Este plano tem como objetivo contribuir para a segurança e integridade do processo eleitoral, mantendo o respeito à privacidade dos eleitores e aos requisitos legais vigentes.

2.– Fundamentação teórica:

Importância da Segurança em Sistemas Eleitorais:

- A integridade e a confiabilidade dos sistemas eleitorais são essenciais para garantir a legitimidade das eleições democráticas. As urnas eletrônicas desempenham um papel crítico na coleta de votos e na apuração dos resultados, tornando imperativo garantir sua segurança contra ameaças que possam comprometer o processo eleitoral.

Integridade da Comunicação Teclado-Placa Mãe:

- A comunicação entre o teclado e a placa-mãe das urnas eletrônicas é um dos elos mais cruciais na cadeia de segurança eleitoral. Qualquer falha na integridade dessa comunicação pode resultar na perda de votos, erros de contagem ou até mesmo manipulações maliciosas, comprometendo a confiabilidade do sistema.

Protocolos Criptográficos:

- Os protocolos criptográficos desempenham um papel vital na proteção da confidencialidade e integridade dos dados transmitidos entre o teclado e a placa-mãe. A análise desses protocolos é fundamental para avaliar se estão implementados de maneira segura e se podem resistir a tentativas de violação da segurança.

Análise de Padrões e Vulnerabilidades:

- A análise de padrões nos sinais transmitidos é necessária para identificar qualquer comportamento anormal ou repetitivo que possa sugerir a presença de um ataque MitM. Além disso, a avaliação de possíveis vulnerabilidades no hardware da urna eletrônica, incluindo o conector do teclado, é crucial para prevenir ataques físicos que possam comprometer a integridade do sistema.

Ataque "Man-in-the-Middle" (MitM):

- O ataque MitM representa uma ameaça significativa à segurança da comunicação entre o teclado e a placa-mãe. Nesse tipo de ataque, um invasor se posiciona entre os pontos de comunicação, interceptando e potencialmente alterando os dados transmitidos. Isso pode resultar na manipulação dos votos e comprometer a integridade do processo eleitoral. Portanto, a análise da comunicação teclado-placa-mãe visa identificar e mitigar possíveis vulnerabilidades que poderiam ser exploradas em um ataque MitM, mantendo a integridade do sistema eleitoral.

3.– Precondições para o teste:

Acesso às Urnas Eletrônicas:

- A equipe de teste deve ter acesso físico às urnas eletrônicas que serão examinadas, permitindo a conexão do Arduino e o monitoramento da comunicação entre o teclado e a placa-mãe.

Arduino Configurado:

- A equipe de teste precisará adentrar ao ambiente de teste com um Arduíno sem conexão com a internet que será implantado entre o teclado e a placa-mãe da urna eletrônica.
- Arduíno contendo duas portas USB devidamente configurado com software e hardware para atuar como intermediário na comunicação entre o teclado e a placa-mãe, permitindo a captura de dados.

4.– Escopo – Superfície de ataque:

- Comunicação entre o teclado e a placa-mãe.

5.– Janela de atuação simulada do atacante:

- A janela de atuação simulada do atacante será das 13h às 17h no primeiro dia e das 9h às 13h nos demais dias. Durante esse período, será realizado a configuração e instalação do dispositivo Arduíno, a coleta de informações, e as devidas análises do protocolo criptográfico e dos padrões nos sinais de comunicação dos dispositivos.
- Para o ataque real, o circuito precisa ser implementado idealmente antes da lacração da urna.

6.– Pontos de intervenção:

Comunicação Teclado-Placa Mãe:

- O ponto central da intervenção é a própria comunicação entre o teclado e a placa-mãe. A equipe de teste irá capturar e analisar os dados transmitidos nessa conexão para verificar a integridade e a segurança da comunicação.

Protocolo Criptográfico:

- A equipe de teste se concentra na análise do protocolo criptográfico usado para proteger os dados transmitidos entre o teclado e a placa-mãe. Isso incluirá a avaliação da robustez da criptografia e da autenticação utilizada.

Análise de Padrões de Dados:

- A identificação de possíveis padrões nos dados transmitidos será outro ponto de intervenção. Isso incluirá a busca de sequências repetitivas, tempos de resposta anormais ou qualquer comportamento suspeito que possa indicar uma tentativa de ataque.

7.– Passos a serem realizados:

Preparação:

- Revisão da documentação técnica relevante das urnas eletrônicas.
- Configuração de um ambiente de teste controlado, simulando um ambiente de eleição real.
- Preparação do hardware e software necessários, incluindo a instalação de ferramentas de análise de comunicação.

Coleta de Dados:

- Conexão do Arduíno entre o teclado e a placa-mãe para capturar os dados transmitidos.
- Registro de todas as interações entre o teclado e a placa-mãe durante a simulação de votação.

Análise de Dados:

- Descriptografia dos dados capturados para avaliar a eficácia do protocolo criptográfico.
- Identificação de possíveis padrões, como sequências repetitivas ou comportamentos anômalos.
- Análise dos resultados em busca de possíveis vulnerabilidades ou fraquezas.

Testes de Vulnerabilidade:

- Aplicação prática das vulnerabilidades encontradas nos protocolos de criptografia e nos padrões dos sinais, a fim de verificar a eficácia das medidas de segurança e identificar possíveis pontos de exploração.

Relatório e Recomendações:

- Preparação de um relatório detalhado dos resultados do teste, incluindo descobertas, análises e recomendações.
- Apresentação dos resultados às autoridades eleitorais e discussão de ações corretivas, se necessário.

8.– Materiais necessários (fornecidos pelo TSE):

- Além da urna, apenas chave de fenda para abrí-la, além de permitir a entrada do circuito e cabos a ser instalados.

9.– Possíveis resultados e impacto:

Resultados:

- **Vulnerabilidades Identificadas no Protocolo de Criptografia:** Compromete a confidencialidade dos dados transmitidos entre o teclado e a placa-mãe, podendo permitir a interceptação e leitura não autorizada dos votos.
- **Padronização dos Sinais de Comunicação:** Abre brechas para ataques do tipo "Man-in-the-Middle" (MitM), permitindo que um invasor intercepte e potencialmente manipule os dados transmitidos, comprometendo a integridade do processo eleitoral.

Impactos:

- **Confidencialidade dos Votos Comprometida:** Vulnerabilidades no protocolo de criptografia podem resultar na exposição não autorizada dos votos, comprometendo a confidencialidade do processo eleitoral.

- **Integridade do Processo Eleitoral em Risco:** Vulnerabilidades nos padrões dos sinais de comunicação podem representar uma ameaça significativa à integridade do processo eleitoral, com o potencial de manipular votos e afetar os resultados das eleições.

10.– Rastreabilidade:

Como o circuito permanece dentro da urna após a votação, ele pode ser visto ao se abrir a mesma. Mas isto não é feito antes do envio e apuração dos votos dela.

11.– Solução proposta:

Atualização do Protocolo de Criptografia:

A atualização do protocolo de criptografia é uma medida crítica para fortalecer a segurança da comunicação entre o teclado e a placa-mãe das urnas eletrônicas. O protocolo de criptografia desempenha um papel fundamental na proteção dos dados transmitidos, assegurando que eles permaneçam confidenciais e íntegros. Para aprimorar a resistência do protocolo a possíveis ataques, as seguintes ações detalhadas devem ser cuidadosamente consideradas:

Seleção de Algoritmos Criptográficos Fortes:

- A seleção de algoritmos criptográficos reconhecidos como seguros é imperativa. A implementação desses algoritmos deve ser rigorosamente verificada para garantir que não haja vulnerabilidades conhecidas em sua configuração.

Chaves de Criptografia Mais Longas:

- Aumentar o tamanho das chaves de criptografia é uma estratégia eficaz para tornar mais desafiadora a tentativa de quebra por meio de força bruta. O uso de chaves mais longas exige um esforço computacional significativamente maior para comprometer a criptografia. Recomenda-se a adoção de chaves com um comprimento consideravelmente maior, em conformidade com as melhores práticas de segurança.

Autenticação Mútua:

- A implementação da autenticação mútua é essencial para assegurar a integridade da comunicação. Isso requer que tanto o teclado quanto a placa-mãe se autentiquem mutuamente antes de permitir a transmissão de dados. Essa medida é particularmente eficaz na prevenção de tentativas de ataques "Man-in-the-Middle" (MitM), pois verifica a identidade e a integridade de ambas as partes envolvidas na comunicação.

6

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste Tentativa de reconhecimento das teclas digitadas usando IA
Instituição proponente (se aplicável)
Responsável Luis Antonio Kowada e respectivo grupo
Resumo do plano (máximo de 120 caracteres) O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identifica-usando um modelo de rede neural, quebrando o sigilo dos votos.
Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(X) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1.– Descrição geral do plano:

O teste proposto para as urnas eletrônicas visa 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.

O relatório final documenta de forma abrangente a metodologia, procedimentos, amostras de áudio coletadas e resultados obtidos, proporcionando uma visão clara das descobertas do teste. Recomendações são fornecidas para aprimorar a segurança das urnas eletrônicas com base nessas conclusões.

2.– Fundamentação teórica:

O Ataque de Canal Lateral Acústico (ASCA) baseia-se em conceitos fundamentais relacionados à coleta de informações por meio de emissões acústicas durante a operação de um dispositivo, neste caso, urnas eletrônicas. A fundamentação teórica abrange os seguintes aspectos:

Canal Lateral Acústico:

- Definição: O canal lateral acústico refere-se à emissão de sinais sonoros decorrentes das operações de um dispositivo.
- Princípio: Dispositivos eletrônicos, como teclados, emitem sinais sonoros distintos durante as interações do usuário, e esses sinais podem ser explorados para inferir informações sensíveis.

Transformada de Áudio em Imagens:

- Mel-Spectrogramas: Utilização de mel-spectrogramas como uma representação visual das características acústicas do áudio.
- Princípio: A conversão de áudio em imagens permite que características específicas, como padrões de pressionamento de teclas, sejam identificadas e utilizadas como entrada para modelos de aprendizado profundo.

Aprendizado Profundo (Deep Learning):

- Modelo CoAtNet: A escolha do modelo CoAtNet para o aprendizado profundo.
- Princípio: Modelos de aprendizado profundo, como CoAtNet, são capazes de aprender padrões complexos em dados, neste caso, imagens de mel-spectrogramas, para realizar tarefas específicas, como a identificação das teclas pressionadas.

Vulnerabilidades em Dispositivos Eletrônicos:

- Emanações Acústicas como Vetor de Ataque: Reconhecimento de que dispositivos eletrônicos podem inadvertidamente vazar informações através de sinais acústicos, tornando-os vulneráveis a ataques de canal lateral.

- Princípio: Exploração das vulnerabilidades inerentes às emissões acústicas para obter informações sensíveis, como teclas pressionadas durante o processo de votação.

3.– Precondições para o teste:

Disponibilidade das Urnas Eletrônicas:

- Garantir acesso físico e lógico às urnas eletrônicas a serem testadas.

Equipamento de Gravação:

- O grupo precisará ingressar no ambiente de teste com um gravador de áudio sem necessidade de acesso à internet. Este gravador (pode ser um celular) será essencial para registrar a frequência acústica das teclas durante o teste, garantindo a coleta dos dados sonoros.

Tempo Designado para Teste:

- Serão necessárias aproximadamente quatro horas diárias de contato com as urnas para coletar áudio das teclas, processar os dados coletados, treinar o modelo e realizar os testes finais de detecção das teclas pressionadas.

4.– Escopo – Superfície de ataque:

- Teclado das urnas.

5.– Janela de atuação simulada do atacante:

- A janela de atuação simulada do atacante será das 13h às 17h no primeiro dia e das 9h às 13h nos demais dias. Durante esse período, será realizada a coleta de áudio das teclas, o treinamento do modelo e os testes finais para detecção das teclas pressionadas.
- Num ataque real, a gravação do som seria feita em qualquer momento antes da eleição para treinar a rede neural. Durante a votação, dentro da seção, se possível próximo da urna seria feita a gravação do som das teclas digitadas. E posteriormente à eleição seria feita a extração das informações.

6.– Pontos de intervenção:

Coleta de Áudio:

- Verificação da qualidade da coleta de áudio das teclas, assegurando que o gravador sem acesso à internet esteja operando corretamente.

- Intervenção para ajustes técnicos, se necessário, visando otimizar a qualidade da captura da frequência acústica.

Treinamento do Modelo:

- Monitoramento do processo de treinamento do modelo de rede neural, intervindo para solucionar possíveis problemas e garantir uma adaptação eficiente aos áudios coletados.

- Ajustes nos parâmetros do modelo, se necessário, para aprimorar a capacidade de detecção das teclas pressionadas.

Testes Finais:

- Supervisão dos testes finais para avaliar a precisão da detecção das teclas pressionadas em situações simuladas.
- Intervenção para corrigir eventuais falhas e garantir a confiabilidade dos resultados obtidos.

7.– Passos a serem realizados:

Preparação do Equipamento:

- Verificar e configurar o equipamento de gravação de áudio, garantindo sua funcionalidade.

Acesso às Urnas Eletrônicas:

- Ingressar no ambiente de teste com um gravador e com um dispositivo de armazenamento sem acesso à internet para preservar a segurança do processo.

Coleta de Áudio:

- Registrar amostras de áudio das teclas pressionadas, replicando condições realistas de votação, levando em conta diferentes pressões sobre as teclas.

Processamento de Dados:

- Aplicar técnicas de processamento de sinal para isolar as teclas pressionadas nas amostras de áudio coletadas.
- Converter os dados de áudio em mel-spectrograms para realizar a o processamento de imagem.

Treinamento do Modelo:

- Iniciar o treinamento do modelo de rede neural usando os mel-spectrograms.
- Monitorar a convergência do modelo, ajustando parâmetros conforme necessário para otimizar o desempenho.

Testes Finais:

- Realizar testes finais em urnas eletrônicas sob condições simuladas, usando o modelo treinado para identificar teclas pressionadas.
- Documentar as detecções de teclas e comparar os resultados com o comportamento esperado das urnas.

Análise de Resultados:

- Avaliar cada detecção de tecla em relação ao funcionamento normal das urnas eletrônicas.
- Atribuir níveis de gravidade e risco às vulnerabilidades identificadas, fornecendo uma visão abrangente dos resultados.

Relatório Final:

- Desenvolvimento do relatório de testes contendo os resultados encontrados.

8.– Materiais necessários (fornecidos pelo TSE):

- Um computador com GPU para treinamento da rede neural ou ao menos um ambiente em que possamos usar um notebook com GPU para isso.

9.– Possíveis resultados e impacto:

- Os resultados esperados deste teste de Canal Lateral nas urnas eletrônicas incluem a identificação precisa das teclas pressionadas por meio da análise acústica. O impacto potencial desse cenário é significativo, uma vez que demonstraria a vulnerabilidade das urnas a ataques de canal lateral, destacando a possibilidade de extração de informações sensíveis (voto) por meio da captura e análise dos sons produzidos durante o processo de votação.

- O teste pode fornecer insights sobre a eficácia das medidas de segurança existentes e, consequentemente, orientar melhorias para fortalecer a resiliência das urnas contra potenciais ameaças acústicas.

10.– Rastreabilidade:

Considerando que qualquer um pode entrar com um celular na sala de votação, é praticamente impossível perceber o ataque, mesmo porque o celular pode estar num bolso ou cima de uma mesa, aparentemente desligado.

11.– Solução proposta:

A proposta de solução para fortalecer a segurança das urnas eletrônicas consiste na implementação de um algoritmo de ofuscação acústica. Este componente inovador tem como objetivo mitigar potenciais ataques de canal lateral baseados em análise acústica, preservando a confidencialidade do voto dos eleitores.

O que é Algoritmo de Ofuscação Acústica?

A ofuscação acústica refere-se à introdução controlada de ruído no sinal acústico gerado pelas interações, neste caso, pressionamento de teclas em urnas eletrônicas. O algoritmo de ofuscação acústica é projetado para tornar os padrões sonoros resultantes menos discerníveis, dificultando a identificação das teclas pressionadas.

Implementação de Ofuscação Acústica

Desenvolvimento do Algoritmo:

- Criação de um algoritmo de ofuscação acústica específico para a urna eletrônica, levando em consideração as características acústicas do teclado.

- O algoritmo deve introduzir ruído de forma controlada e dinâmica, utilizando técnicas de modulação, randomização e filtros adaptativos.

Ajuste Dinâmico:

- Implementação de ajuste dinâmico do ruído com base nas condições ambientais e variações no uso do teclado.

- A adaptação dinâmica deve equilibrar a ofuscação eficaz com a manutenção da usabilidade da urna.

Modulação e Randomização:

- Aplicação de modulação dinâmica para alterar características como amplitude, frequência ou fase do ruído ao longo do tempo.

- Introdução de randomização temporal e espectral para tornar o padrão sonoro mais imprevisível.

Filtros Adaptativos:

- Utilização de filtros adaptativos para ajustar continuamente a quantidade e as características do ruído em resposta às condições ambientais.
- Os filtros devem ser capazes de se adaptar a diferentes ambientes de votação.

Integração com o Sistema

Incorporação ao Firmware:

- Revisão e atualização do firmware da urna eletrônica para integrar o algoritmo de ofuscação acústica.
- Incorporação de medidas de segurança específicas para proteger os parâmetros do algoritmo.

Testes de Integração:

- Realização de testes extensivos para garantir a integridade e a eficácia da integração.
- Verificação da compatibilidade com o funcionamento normal da urna eletrônica e a manutenção da confidencialidade do voto.

Segurança Adicional

Criptografia de Parâmetros:

- Implementação de criptografia robusta para proteger os parâmetros do algoritmo de ofuscação.
- Garantia de que somente sistemas autorizados possam ajustar e atualizar os parâmetros.

Monitoramento Contínuo:

- Estabelecimento de um sistema de monitoramento contínuo para avaliar o desempenho do algoritmo em condições reais.
- A coleta de dados durante eleições simuladas e reais é essencial para ajustar e melhorar a ofuscação ao longo do tempo.

7

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
Instituição proponente (se aplicável):
Responsável: Diego Vergaças de Sousa Carvalho
Resumo do plano (máximo de 120 caracteres): Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.

Sistemas a serem testados

Softwares
( ) Gerenciador de Dados, Aplicativos e Interface com Eletrônica (GEDAI-UE)
( ) Transmissão de arquivos (Kit JE Connect)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e Inforquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
(**X**) Urnas modelos 2020 e 2022, com seus respectivos firmware e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
(**X**) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares
(**X**) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos
( ) Geração de mídias
( ) Carga da urna eletrônica
(**X**) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:
1. O teste a ser realizado deve, obrigatoriamente, ser reproduzível.
2. Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7808
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DIAS 11H ÀS 18H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

O teste visa testar o funcionamento do teclado da urna eletrônica. O intuito é garantir que o registro corresponda corretamente às teclas acionadas no teclado, mesmo sob condições não usuais de acionamento das teclas.

2 – Fundamentação teórica:

Controladores de teclados matriciais podem utilizar circuitos em formato de multiplexadores para ler uma grande quantidade de teclas utilizando poucas entradas digitais. Esta configuração de leitura do acionamento do teclado é conhecida por ser suscetível a erros quando múltiplas teclas são acionadas. Sabendo que a urna conta com teclas de acionamento independente ligados direto ao controlador, o teste irá verificar se estes erros de digitação simultânea ocorrem e, consequentemente, alteram o registro de voto. Para além da questão técnica, há uma dimensão da percepção pública da segurança das urnas acerca de alegações, feitas nos últimos anos, de que a urna não registra corretamente o voto de determinados eleitores. Embora este seja um teste superficial, o nosso intuito é demonstrar se a urna está ou não sujeita a um tipo de ataque que tente confundir o controlador do teclado sob condições não usuais de operação. O teste pode, inclusive, sob determinadas condições adversas, demonstrar que o teclado é resistente a falhas mecânicas ou de seus contatos elétricos.

3 – Precondições para o teste:

O teclado a ser testado precisa estar em um ambiente que permita reproduzir o cenário de votação, possibilitando o uso das teclas numéricas e de ações (teclas Corrige, Branco e Confirma) e a conferência do registro dos números digitados em tela.

4 – Escopo – Superfície de ataque:

Teclados físicos da urna eletrônica.

5 – Janela de atuação simulada do atacante:

O eleitor, em uma situação convencional de votação, irá pressionar aleatoriamente e simultaneamente várias teclas numéricas e de ação no teclado da urna. Por ser uma situação padrão e que não depende da atuação de atores externos e nem de situações adversas, este cenário pode acontecer em virtualmente qualquer caso de votação.

6 – Pontos de intervenção:

Caso o teclado não seja capaz de lidar corretamente com pressionamentos aleatórios e simultâneos de várias teclas, é possível que o registro correto do voto seja comprometido ou que a integridade da urna seja violada.

7 – Passos a serem realizados:

7.1 - 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.

7.2 - Reproduzir o teste do item 7.1 com mais uma tecla mantida pressionada

7.3 - Reproduzir o item 7.2, 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.

7.4 - Observar o comportamento do software ao manter um tecla ou um grupo de teclas pressionado por um período longo.

8 – Materiais necessários (fornecidos pelo TSE):

Urna eletrônica.

9 – Possíveis resultados e impacto:

9.1 - Independentemente dos valores pressionados no teclado, e da quantidade de teclas pressionadas simultaneamente, o registro do voto foi feito de acordo e a integridade da urna não foi violada.

9.2 - Ao pressionar uma determinada quantidade de teclas simultaneamente, é verificado que os dígitos exibidos na tela não correspondem às teclas que foram acionadas ou que as ações BRANCO,

CORRIGE e CONFIRMA não são executadas.

10 – Rastreabilidade:

10.1 - Caso o teclado do dispositivo testado possua um mecanismo similar a um keylogger, que registra em tempo real as teclas pressionadas, este tipo de ataque é possível de ser rastreado ao comparar o resultado registrado no voto versus os valores relatados no log de digitação.

10.2 - Caso o teclado do dispositivo testado não possua um mecanismo similar a um keylogger, que registra em tempo real as teclas pressionadas, este tipo de ataque não é rastreável.

11 – Solução proposta:

Caso a hipótese do teste acerca da incapacidade do teclado de registrar corretamente múltiplas teclas pressionadas simultaneamente se mostre verdadeira, é possível contornar este erro aprimorando o firmware do controlador do teclado para melhor realizar a lógica de varredura de entradas digitais.

Data:
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste: Inconsistência de Software

Instituição proponente (se aplicável):
Pontifícia Universidade Católica do Rio Grande Do Sul

Responsável: Avelino Francisco Zorzo

Resumo do plano (máximo de 120 caracteres):
Executar a avaliação de que o software que salvo na urna eletrônica é o mesmo software lacrado em cerimônia pública

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
( ) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
(X) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

( ) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

(X) Geração de mídias
(X) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
(X) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
( ) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

TRIBUNAL SUPERIOR ELEITORAL
SETOR DE ADMINISTRAÇÃO FEDERAL SUL (SAFS), QUADRA 7, LOTES 1/2, BRASÍLIA/DF – CEP: 70070-600 – TEL.: 3030-7000
PROTOCOLO ADMINISTRATIVO: SALA V 101, FAX: 3030-9850 – HORÁRIO DE FUNCIONAMENTO: DAS 11H ÀS 19H

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Durante a participação do processo de revisão de código foi aberto um questionamento para realizar a execução da validação dos arquivos que estavam sendo avaliados para garantir que os códigos avaliados são os mesmos códigos que foram lacrados. A solicitação foi recusada por entendimento que não seria um teste que fizesse parte do escopo do TPS. Porém, o intuito desse teste é realizar a verificação que os softwares avaliados durante o TPS são os mesmos softwares que serão embarcados na urna tendo como **hipótese** que o software AVPART está executando a verificação de forma incorreta.

Dessa forma, iniciaremos realizando o desenvolvimento de um script Python, utilizando bibliotecas comuns, que irá realizar a listagem e leitura de cada arquivo presente em uma mídia digital, finalizando com a computação do hash "sha512 Radix64" do conteúdo do arquivo. Posteriormente a execução do script Python será realizada a comparação dos dados disponibilizados de forma pública em: https://www.justicaeleitoral.jus.br/tps/arquivos/2023/documentos/HashesPDF.zip, os quais são os hashes dos arquivos disponibilizados para execução do processo de avaliação de código.

A finalidade deste Plano de Teste é garantir que os softwares avaliados durante o processo de revisão de código são os mesmos códigos usados durante as eleições, após as mudanças de software para correções de vulnerabilidades.

2 – Fundamentação teórica:

Para garantir a integridade de arquivos importantes em processos críticos, como o processo eleitoral brasileiro, é comum utilizar algoritmos de função resumo, as quais geram valores únicos para um conjunto de dados e sempre que for utilizado o mesmo conjunto de dados o resultado será igual. Dessa forma para um dado, por exemplo, "ABC" o resultado de uma função de resumo (SHA1) é "3c01bdbb26f358bab27f267924aa2c9a03fcfdb8" e sempre que executar com a mesma entrada de dados, "ABC", o resultado será sempre o mesmo independente da quantidade de execuções. Porém, ao modificar a entrada de dados para "ABc" a função resumo terá um resultado totalmente diferente, o resultado seria "39f10faee3f72d3f590daf63d9ac37c69db2791a". Este efeito é conhecido como efeito cascata, pois devido a mudança de um bit do valor de entrada o resultado muda por completo.

Durante o processo do TPS a avaliação de integridade dos arquivos sendo executados na Urna é realizado pelo software AVPART, o qual executa a verificação de assinatura dos arquivos dentro da urna, e também é possível imprimir a lista de hashes dos arquivos dentro da urna para uma conferência manual. Entretanto, essa conferência manual esta sujeita a muitos erros, pois se trata de um humano avaliando uma lista de caractéres que para o cérebro humano pode parecer aleatório.

Dessa forma, propõe-se a execução de verificação de integridade dos arquivos carregados na urna através de um software terceiro, não desenvolvido pelo TSE, de forma a garantir a transparência do processo eleitoral.

3 – Precondições para o teste:

- Python3
- Sistema de arquivos dos softwares que serão carregados na urna
- Acesso aos Hashes atualizados dos últimos softwares lacrados para execução dos planos de testes

4 – Escopo – Superfície de ataque:

Softwares que serão carregados na urna.

5 – Janela de atuação simulada do atacante:

Período após a lacração dos softwares até a configuração das urnas para as eleições.

6 – Pontos de intervenção:

1 - midia de urna

7 – Passos a serem realizados:

1. Desenvolver script Python3 que irá:
   1.1. Listar todos arquivos em um diretório
   1.2. Ler o conteúdo dos arquivos listados
   1.3. Computar o SHA512 de cada conteúdo lido
   1.4. Computar o valor Base64 de cada SHA512
   1.5. Comparar os resultados com os hashes públicos assinados

8 – Materiais necessários (fornecidos pelo TSE):

1. Computador
2. Softwares que foram lacrados em cerimônia pública, de preferência de dentro de uma mídia oficial
3. Mídia de carga da urna
4. Hashes dos arquivos lacrados em cerimônia pública

9 – Possíveis resultados e impacto:

Caso o plano de teste encontre algum resultado negativo então todo o processo de execução do TPS não terá validado, pois os softwares disponibilizados para realização do teste público são diferentes dos softwares carregados na urna.

10 – Rastreabilidade:

11 – Solução proposta:

Para solucionar esse problema sugerimos o desenvolvimento compartilhado de uma solução de verificação de conteúdo dos arquivos presente na urna e que tenha sido desenvolvido e mantido por uma insituição terceira, avaliando se os arquivos dentro da urna são os arquivos disponibilizados para avaliação pública.

3

Data
Resultado ( ) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

COMISSÃO REGULADORA

7.11 Anexo K – Lista definitiva de inscrições

TESTE PÚBLICO DE SEGURANÇA DA URNA — Tribunal Superior Eleitoral — #VOZ DA DEMOCRACIA ELEIÇÕES 2024

A Comissão Reguladora, instituída por meio da Portaria-TSE n° 672/2023, informa que, considerando a decisão do Excelentíssimo Ministro Presidente, que acatou as 16 inscrições previamente selecionadas pela Comissão supracitada, segue abaixo a lista definitiva das inscritas e inscritos no Teste Público de Segurança da Urna Eletrônica - 2023.

Nome da inscrita/inscrito	Tipo de Inscrição
Aline Barbosa da Silva	Individual
Diego Ferry Torrent	Individual
Érika Maria Rodrigues de Castro	Individual
Guilherme Henrique dos Santos	Individual
Joao Benedito dos Santos Junior	Individual
João Vitor Santana	Individual
Nicholas Barros dos Santos	Individual
Ricardo Antônio Pralon Santos	Individual
Marcos Roberto dos Santos	Grupo
Leandro Caletti	
Rafael Noll da Silva	
Eduardo Bido	
Rhayara Rodrigues Fiorentin	
Rafael Basso Reis	Grupo
Stefano Augusto Mossi	
Gabriel Viecili	
André Izolani Rien	
Brayan Vanz de Oliveira	
Vitor Aloisio do Nascimento Guia	Grupo
Hitatiana Maria Santiago Ferreira da Silva Guia	
Carlos Alberto da Silva	Grupo
Ian Martinez Zimmermann	
Matheus Vianna Silveira	
Mário de Araújo Carvalho	
Galileu Batista de Sousa	Grupo
Maria Isabel Vasconcelos Lima	
Breno Rangel Borges Marchetti	
João Paulo Vieira Almeida	
João Vitor de Sá Hauck	
Luis Antonio Brasil Kowada	Grupo
Gabriel Cardoso de Carvalho	
Caubi de Souza Loureiro Rosa	
Camila Ferreira Alves	
André Mário dos Reis dos Santos	Grupo
Alexandre Zago Boava	
Diego Vergaças de Sousa Carvalho	
Victor Antunes Ignácio de Medeiros Pereira da Silva	
Avelino Francisco Zorzo	Grupo
Ariel Rossetto Ril	
Daniel Dalalana Bertoglio	

7.12 Anexo L – Lista de presença – TPS

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 27/11		
	Nome do(a) Investigador(a)	Assinatura (Tarde)
1	Alexandre Zago Boava	NÃO VEIO
2	Aline Barbosa da Silva	Aline Barbosa da Silva
3	André Izolani Rien *	NÃO VEM
4	André Mário dos Reis dos Santos	NÃO VEIO
5	Ariel Rossetto Ril	
6	Avelino Francisco Zorzo	NÃO VEIO
7	Brayan Vanz de Oliveira	Brayan Vanz de Oliveira
8	Breno Rangel Borges Marchetti	Breno Rangel Borges Marchetti
9	Camila Ferreira Alves	
10	Carlos Alberto da Silva	
11	Caubi de Souza Loureiro Rosa	Caubi de Souza L Rosa
12	Daniel Dalalana Bertoglio	NÃO VEIO
13	Diego Vergaças de Sousa Carvalho	NÃO VEIO
14	Eduardo Bido	Eduardo Bido

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 27/11		
	Nome do(a) Investigador(a)	Assinatura (Tarde)
15	Érika Maria Rodrigues de Castro	
16	Gabriel Cardoso de Carvalho	
17	Gabriel Viecili	Gabriel Viecili
18	Galileu Batista de Sousa	
19	Guilherme Henrique dos Santos	Guilherme Henrique dos Santos
20	Hitatiana Maria Santiago Ferreira da Silva Guia	Hitatiana Maria Santiago Ferreira
21	Ian Martinez Zimmermann	Ian M Zimmermann
22	João Benedito dos Santos Junior	
23	João Paulo Vieira Almeida	
24	João Vitor de Sá Hauck	João Vitor de Sá Hauck
25	Leandro Caletti *	NÃO VEM
26	Luis Antonio Brasil Kowada	
27	Marcos Roberto dos Santos	
28	Maria Isabel Vasconcelos Lima	

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 27/11		
	Nome do(a) Investigador(a)	Assinatura (Tarde)
29	Mário de Araújo Carvalho	NÃO VEIO.
30	Matheus Vianna Silveira	Matheus
31	Nicholas Barros dos Santos	Nicholas Barros dos Santos
32	Rafael Basso Reis	Rafael
33	Rafael Noll da Silva	Rafael Noll da Silva
34	Rhayara Rodrigues Fiorentin	Rhayara R. Fiorentin
35	Stefano Augusto Mossi	Stefano Augusto Mossi
36	Vitor Aloisio do Nascimento Guia	VE [illegible]

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 28/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Alexandre Zago Boava	G-7	Alexandre Boava	Alexandre Boava
2	Aline Barbosa da Silva	I-1	Aline Barbosa	Aline Barbosa
3	André Izolani Rien	G-2	NÃO VEIO	
4	André Mário dos Reis dos Santos	G-7		
5	Ariel Rossetto Ril	G-8		
6	Avelino Francisco Zorzo	G-8	NÃO VEIO	não veio
7	Brayan Vanz de Oliveira	G-2	Brayan Vanz de Oliveira	Brayan Vanz de Oliveira
8	Breno Rangel Borges Marchetti	G-5		
9	Camila Ferreira Alves	G-6		
10	Carlos Alberto da Silva	G-4		
11	Caubi de Souza Loureiro Rosa	G-6	Caubi de S. S. Rosa	Caubi de S. L. Rosa
12	Daniel Dalalana Bertoglio	G-8	Não veio	
13	Diego Vergaças de Sousa Carvalho	G-7		
14	Eduardo Bido	G-1	Eduardo Bido	Eduardo Bido

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 28/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
15	Érika Maria Rodrigues de Castro	I-2		
16	Gabriel Cardoso de Carvalho	G-6		
17	Gabriel Viecili	G-2		
18	Galileu Batista de Sousa	G-5		
19	Guilherme Henrique dos Santos	I-3		
20	Hitatiana Maria Santiago Ferreira da Silva Guia	G-3		
21	Ian Martinez Zimmermann	G-4		
22	João Benedito dos Santos Junior	I-4		
23	João Paulo Vieira Almeida	G-5		
24	João Vitor de Sá Hauck	G-5		
25	Leandro Caletti	G-1	NÃO VEIO	
26	Luis Antonio Brasil Kowada	G-6		
27	Marcos Roberto dos Santos	G-1		
28	Maria Isabel Vasconcelos Lima	G-5		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 28/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
29	Mário de Araújo Carvalho	G-4	NÃO VEIO	
30	Matheus Vianna Silveira	G-4		
31	Nicholas Barros dos Santos	I-5		
32	Rafael Basso Reis	G-2		
33	Rafael Noll da Silva	G-1		
34	Rhayara Rodrigues Fiorentin	G-1		
35	Stefano Augusto Mossi	G-2		
36	Vitor Aloisio do Nascimento Guia	G-3		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 29/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Aline Barbosa da Silva	I-1	Aline Barbosa da Silva	Aline Barbosa da Silva
2	Érika Maria Rodrigues de Castro	I-2		
3	Guilherme Henrique dos Santos	I-3	Guilherme Henrique dos Santos	Guilherme Henrique dos Santos
4	João Benedito dos Santos Junior	I-4	ENCERROU TESTE	Encerrou o teste
5	Nicholas Barros dos Santos	I-5	Nicholas Barros dos Santos	Nicholas Barros dos Santos
6	Eduardo Bido	G-1	Eduardo Bido	Eduardo Bido
7	Leandro Caletti	G-1		
8	Marcos Roberto dos Santos	G-1	Marcos Roberto Dos Santos	Marcos Roberto Dos Santos
9	Rafael Noll da Silva	G-1	Rafael Noll da Silva	Rafael Noll da Silva
10	Rhayara Rodrigues Fiorentin	G-1	Rhayara R Fiorentin	Rhayara R Fiorentin
11	André Izolani Rien	G-2		
12	Brayan Vanz de Oliveira	G-2	Brayan Vanz de Oliveira	Brayan Vanz de Oliveira
13	Gabriel Viecili	G-2	Gabriel Viecili	Gabriel Viecili
14	Rafael Basso Reis	G-2	Rafael Basso	Rafael Basso

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 29/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
15	Stefano Augusto Mossi	G-2	Stefano Augusto M	Stefano A. Mossi
16	Hitatiana Maria Santiago Ferreira da Silva Guia	G-3	Hitatiana Maria Santiago Guia	Finalizou teste
17	Vitor Aloisio do Nascimento Guia	G-3	Vitor Aloisio do Nascimento Guia	Finalizou teste
18	Carlos Alberto da Silva	G-4		
19	Ian Martinez Zimmermann	G-4	Ian M Zimmermann	Ian M Zimmermann
20	Mário de Araújo Carvalho	G-4	Não veio	veio 30/11
21	Matheus Vianna Silveira	G-4	Matheus	Matheus
22	Breno Rangel Borges Marchetti	G-5		
23	Galileu Batista de Sousa	G-5		
24	João Paulo Vieira Almeida	G-5		
25	João Vitor de Sá Hauck	G-5		
26	Maria Isabel Vasconcelos Lima	G-5		
27	Camila Ferreira Alves	G-6	Camila Ferreira Alves	Camila Ferreira Alves
28	Caubi de Souza Loureiro Rosa	G-6	Caubi de Souza L. Rosa	Caubi de S. L. Rosa

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 29/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
29	Gabriel Cardoso de Carvalho	G-6		
30	Luis Antonio Brasil Kowada	G-6		
31	Alexandre Zago Boava	G-7		
32	André Mário dos Reis dos Santos	G-7		
33	Diego Vergaças de Sousa Carvalho	G-7		
34	Ariel Rossetto Ril	G-8		
35	Avelino Francisco Zorzo	G-8		—
36	Daniel Dalalana Bertoglio	G-8		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 30/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Aline Barbosa da Silva	I-1	Aline Barbosa	Aline Barbosa
2	Érika Maria Rodrigues de Castro	I-2		
3	Guilherme Henrique dos Santos	I-3	Guilherme Henrique dos Santos	Guilherme Henrique dos Santos
4	João Benedito dos Santos Junior	I-4	—	—
5	Nicholas Barros dos Santos	I-5	Nicholas Barros dos Santos	Nicholas Barros dos Santos
6	Eduardo Bido	G-1	Eduardo Bido	Eduardo Bido
7	Leandro Caletti	G-1	Não Vem	Não Vem
8	Marcos Roberto dos Santos	G-1		
9	Rafael Noll da Silva	G-1	Rafael Noll da Silva	Rafael Noll da Silva
10	Rhayara Rodrigues Fiorentin	G-1	Rhayara R Fiorentin	Rhayara R Fiorentin
11	André Izolani Rien	G-2	Não Vem	Não vem
12	Brayan Vanz de Oliveira	G-2	Brayan Vanz de Oliveira	Brayan Vanz de Oliveira
13	Gabriel Viecili	G-2	Gabriel Viecili	Gabriel Viecili
14	Rafael Basso Reis	G-2		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 30/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
15	Stefano Augusto Mossi	G-2	Stefano Mossi	Stefano Mossi
16	Hitatiana Maria Santiago Ferreira da Silva Guia	G-3	Concluiu teste em 29/11	Concluiu teste em 29/11
17	Vitor Aloisio do Nascimento Guia	G-3	Concluiu teste em 29/11	Concluiu o teste em 29/11
18	Carlos Alberto da Silva	G-4		
19	Ian Martinez Zimmermann	G-4		
20	Mário de Araújo Carvalho	G-4		x
21	Matheus Vianna Silveira	G-4		
22	Breno Rangel Borges Marchetti	G-5		
23	Galileu Batista de Sousa	G-5		
24	João Paulo Vieira Almeida	G-5		
25	João Vitor de Sá Hauck	G-5		
26	Maria Isabel Vasconcelos Lima	G-5		
27	Camila Ferreira Alves	G-6		
28	Caubi de Souza Loureiro Rosa	G-6	Caubi de Souza L. Rosa	Caubi de Souza L. Rosa

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 30/11				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
29	Gabriel Cardoso de Carvalho	G-6		
30	Luis Antonio Brasil Kowada	G-6		Retornou para o Rio
31	Alexandre Zago Boava	G-7		
32	André Mário dos Reis dos Santos	G-7		
33	Diego Vergaças de Sousa Carvalho	G-7		
34	Ariel Rossetto Ril	G-8		x Veio, mas saiu antes
35	Avelino Francisco Zorzo	G-8	Não veio	Não veio
36	Daniel Dalalana Bertoglio	G-8		x Veio, mas saiu antes

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 01/12				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Aline Barbosa da Silva	I-1	Aline Barbosa	Aline Barbosa
2	Érika Maria Rodrigues de Castro	I-2		
3	Guilherme Henrique dos Santos	I-3		
4	João Benedito dos Santos Junior	I-4	concluiu teste em 29/11	Concluiu teste em 29/11
5	Nicholas Barros dos Santos	I-5	Nicholas Barros	
6	Eduardo Bido	G-1		
7	Leandro Caletti	G-1	não veio	não veio
8	Marcos Roberto dos Santos	G-1		
9	Rafael Noll da Silva	G-1	Rafael Noll da Silva	Rafael Noll da Silva
10	Rhayara Rodrigues Fiorentin	G-1	Rhayara R. Fiorentin	Rhayara R. Fiorentin
11	André Izolani Rien	G-2	não veio	não veio
12	Brayan Vanz de Oliveira	G-2	Brayan Vanz de Oliveira	Brayan Vanz de Oliveira
13	Gabriel Viecili	G-2	Gabriel Viecili	Gabriel Viecili
14	Rafael Basso Reis	G-2	Rafael	29/11

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 01/12				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
15	Stefano Augusto Mossi	G-2	Stefano Mossi	Stefano Mossi
16	Hitatiana Maria Santiago Ferreira da Silva Guia	G-3	concluiu teste em 29/11	Concluiu teste em 29/11
17	Vitor Aloisio do Nascimento Guia	G-3	Concluiu teste em 29/11	Concluiu teste em 29/11
18	Carlos Alberto da Silva	G-4		
19	Ian Martinez Zimmermann	G-4		
20	Mário de Araújo Carvalho	G-4		
21	Matheus Vianna Silveira	G-4		
22	Breno Rangel Borges Marchetti	G-5		
23	Galileu Batista de Sousa	G-5		
24	João Paulo Vieira Almeida	G-5		
25	João Vitor de Sá Hauck	G-5		
26	Maria Isabel Vasconcelos Lima	G-5		
27	Camila Ferreira Alves	G-6		
28	Caubi de Souza Loureiro Rosa	G-6	Caubi de Souza L. Rosa	Caubi de S. L. Rosa

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

	Dia 01/12			
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
29	Gabriel Cardoso de Carvalho	G-6	[illegible] retorna	
30	Luis Antonio Brasil Kowada	G-6	Retornou Encerrou em 30/11	Encerrou em 30/11
31	Alexandre Zago Boava	G-7	Encerrou	encerrou
32	André Mário dos Reis dos Santos	G-7	Encerrou	encerrou
33	Diego Vergaças de Sousa Carvalho	G-7	Encerrou	encerrou
V 34	Ariel Rossetto Ril	G-8	[illegible]	[illegible]
35	Avelino Francisco Zorzo	G-8	Não veio	não veio
36	Daniel Dalalana Bertoglio	G-8	Não veio	não veio

DIA 02/12/23 _ G-5
1. João Paulo Pereira Abreu
2. Maria Isabel V Lima
3. Bruno Bergl Borges [illegible]
4. GALILEU BATISTA
5. João Vitor de Sá Paula

DIA 02/12/23 _ G-6
1. Caulki de Souza S. Rosa
2. [illegible]

7.13 Anexo M – Planos de testes apresentados na semana de execução

Nº 67

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

(I-3)

Título do Plano de Teste

Ab Inicio Validi Test Validi

Instituição proponente (se aplicável)

Responsável

Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)

Abrir a tela de correspondência.

Sistemas a serem testados

Softwares

(x) *Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)*
( ) *Software Básico da Urna Eletrônica*
( ) *Software de Carga (SCUE)*
( ) *Gerenciador de Aplicativos (GAP)*
( ) *Software de Votação (VOTA)*
( ) *Recuperador de Dados (RED)*
( ) *Sistema de Apuração (SA)*
( ) *Sistemas Transportador, RecArquivos e InfoArquivos*
( ) *Subsistema de Instalação e Segurança (SIS)*
( ) *Kit JEConnect*
( ) *Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas*
( ) *Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação*
( ) *Verificador Pré/Pós-Eleição (VPP)*
( ) *Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)*

Hardwares

( ) *Urna eletrônica*
( ) *Transmissão de arquivos (Kit JE Connect)*

Procedimentos

(x) *Geração de mídias*
(x) *Carga da urna eletrônica*
( ) *Votação*
( ) *Transmissão de arquivos*
( ) *Sorteio de seções*
( ) *Teste de integridade (votação paralela)*
(x) *Conferência de hash ou validação de assinaturas na urna*
( ) *Recuperação de dados na urna eletrônica*
( ) *Apuração de votos na urna eletrônica*

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Alterar a tabela de correspondência, de modo que modifique a carga esperada de uma determinada urna, para outra arbitrária com votos espúrios e com isso alterar a distribuição dos votos.

2 – Fundamentação teórica:

* Com base nas observações realizadas no plano Suficiência Limitada Substituição Votos Mutare Permanente

3 – Precondições para o teste:

* Corrupção de membros da Justiça Eleitoral
* Acesso ao SIS e ao GEDAI

4 – Escopo – Superfície de ataque:

* SIS
* GEDAI

5 – Janela de atuação simulada do atacante:

* Geração de Mídias
* Disponibilização dos Votos

6 – Pontos de intervenção:

* Blocos de Geração de Mídias
*

7 – Passos a serem realizados:

* Todos alterar as configurações e arquivos do ~~[illegible]~~ GEDAI para que o sistema de totalização receba votos provenientes de outra urna que não a esperada.

8 – Materiais necessários (fornecidos pelo TSE):

* Acesso a SIS e ao GEDAI

9 – Possíveis resultados e impacto:

* Alterações de resultado entre a carga gerada e a carga esperada.
* Potencial impacto sob toda eleição com a alteração da tabela de correspondência.

10 – Rastreabilidade:

* Pode ser detectado usando conferência de lista, conferência de arquivos alterados

11 – Solução proposta:

* Criar usando lógica de modo que redirecione outra urna que na ~~aplicação~~ preparação da urnas remeta a uma dirigida consiga decifrar os arquivos necessários a votação.

3

Data	
Resultado	(X) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

28/11/23
11:23

Nº 108 1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Urna inválida ess.

Instituição proponente (se aplicável)

Responsável

Guilherme Henrique dos Santos

Resumo do plano (máximo de 120 caracteres)

Usar o SA como validador de um BU com votos inválidos

Sistemas a serem testados

Softwares

( ) Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)
( ) Software Básico da Urna Eletrônica
( ) Software de Carga (SCUE)
( ) Gerenciador de Aplicativos (GAP)
( ) Software de Votação (VOTA)
( ) Recuperador de Dados (RED)
(x) Sistema de Apuração (SA)
( ) Sistemas Transportador, RecArquivos e InfoArquivos
( ) Subsistema de Instalação e Segurança (SIS)
( ) Kit JEConnect
( ) Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas
( ) Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação
( ) Verificador Pré/Pós-Eleição (VPP)
( ) Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)

Hardwares

(x) Urna eletrônica
( ) Transmissão de arquivos (Kit JE Connect)

Procedimentos

( ) Geração de mídias
( ) Carga da urna eletrônica
( ) Votação
( ) Transmissão de arquivos
( ) Sorteio de seções
( ) Teste de integridade (votação paralela)
( ) Conferência de hash ou validação de assinaturas na urna
( ) Recuperação de dados na urna eletrônica
(x) Apuração de votos na urna eletrônica

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Em continuidade ao plano Suffragium Simulata Substantiam Veritas Mutare Possumus pretende-se usar o SA para recognitar o BU com votos espúrios.

2 – Fundamentação teórica: ART 206, inciso II da resolução 23.669

~~Não há restrições em que um ator de ameaça use um ataque de DDoS para impedir o uso do sistema de totalização e forçar o uso do SA como totalizador de votos~~

3 – Precondições para o teste:

* Entrega do BU com votos espúrios com assinatura validada para serem reconhecidos no SA.

4 – Escopo – Superfície de ataque:

* SA.

5 – Janela de atuação simulada do atacante:

* Apuração do BU conforme previsto no Art. 206, inciso II

6 – Pontos de intervenção:

* uso do SA na situação prevista pelo art. 206, inciso II.

7 – Passos a serem realizados:

* Iniciar o SA como totalizador do BU
* Digitar o BU com votos espúrios
* Concluir o processo.

8 – Materiais necessários (fornecidos pelo TSE):

* VE com SA.

9 – Possíveis resultados e impacto:

* Demostrar que é possível validar um BU com votos inválidos.

10 – Rastreabilidade:

Não serão usadas técnicas furtivas e antiforense.

11 – Solução proposta:

Incluir mecanismo de conferência de correspondência antes disso processo

3

Data	29/11/2023
Resultado	(X) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

1

146

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Suffragium non est vulgarus.

Instituição proponente (se aplicável)

Responsável

Guilherme Henrique dos Santos -I-3

Resumo do plano (máximo de 120 caracteres)

Troca de votos, mediante substituição por um período de tempo da MV por uma MV clonada.

Sistemas a serem testados

Softwares

( ) *Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)*
( ) *Software Básico da Urna Eletrônica*
( ) *Software de Carga (SCUE)*
( ) *Gerenciador de Aplicativos (GAP)*
(X) *Software de Votação (VOTA)*
( ) *Recuperador de Dados (RED)*
( ) *Sistema de Apuração (SA)*
( ) *Sistemas Transportador, RecArquivos e InfoArquivos*
( ) *Subsistema de Instalação e Segurança (SIS)*
( ) *Kit JEConnect*
( ) *Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas*
( ) *Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação*
( ) *Verificador Pré/Pós-Eleição (VPP)*
( ) *Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)*

Hardwares

(X) *Urna eletrônica*
( ) *Transmissão de arquivos (Kit JE Connect)*

Procedimentos

( ) *Geração de mídias*
( ) *Carga da urna eletrônica*
(X) *Votação*
( ) *Transmissão de arquivos*
( ) *Sorteio de seções*
( ) *Teste de integridade (votação paralela)*
( ) *Conferência de hash ou validação de assinaturas na urna*
( ) *Recuperação de dados na urna eletrônica*
( ) *Apuração de votos na urna eletrônica*

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Interromper a votação retirando a MV original da UV, conectar a votação com MV clonada, posteriormente retirar a MV original.

2 – Fundamentação teórica:

O conteúdo da MV comparado com o conteúdo da Memória interna deverá retornar erro.

3 – Precondições para o teste:

* Acesso livre a UE

4 – Escopo – Superfície de ataque:

* Módulo de votação

5 – Janela de atuação simulada do atacante:

* Período de Votação.

6 – Pontos de intervenção:

* ~~Processo de~~
* Registro da MV.

7 – Passos a serem realizados:

* Retirar a MV após a votação encerrada
* Retirar clone da MV
* Inserir a MV clonada na UE
* Realizar nova 1 voto
* Substituir a MV clonada pela MV original

8 – Materiais necessários (fornecidos pelo TSE):

* UE
* Mídia de carga, mídia de votação, Mídia de Votação para Cloné

9 – Possíveis resultados e impacto:

* Rescante dos dados - registrados da MV clonada

10 – Rastreabilidade:

* Pode ser rastreado mediante comparação dos registros com a memória interna.

11 – Solução proposta:

* ~~Implantar~~ Parametrização do Rockup.

3

Data	
Resultado	(X) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

167

1

TESTE PÚBLICO DE SEGURANÇA DA URNA

PLANO DE TESTE DO SISTEMA ELETRÔNICO DE VOTAÇÃO E APURAÇÃO

INFORMAÇÕES GERAIS

Título do Plano de Teste

Escalação de Privilégio no Windows (SIS) G.4

Instituição proponente (se aplicável)

UFMS

Responsável

Carlos Alberto da Silva

Resumo do plano (máximo de 120 caracteres)

Utilizar ~~vulnerabilidade~~ do opt falha de permissionamento para escalar privilégio e acesso a arquivos críticos

Sistemas a serem testados

Softwares

( ) *Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE)*
( ) *Software Básico da Urna Eletrônica*
( ) *Software de Carga (SCUE)*
( ) *Gerenciador de Aplicativos (GAP)*
( ) *Software de Votação (VOTA)*
( ) *Recuperador de Dados (RED)*
( ) *Sistema de Apuração (SA)*
( ) *Sistemas Transportador, RecArquivos e InfoArquivos*
(✓) *Subsistema de Instalação e Segurança (SIS)*
( ) *Kit JEConnect*
( ) *Urnas modelos 2020 e 2022, com seus respectivos firmwares e mídias eletrônicas*
( ) *Sistema de apoio às auditorias de autenticidade e integridade - Módulo Sorteio e Módulo Votação*
( ) *Verificador Pré/Pós-Eleição (VPP)*
( ) *Verificador de integridade e autenticidade de sistemas eleitorais (AVPART)*

Hardwares

( ) *Urna eletrônica*
( ) *Transmissão de arquivos (Kit JE Connect)*

Procedimentos

( ) *Geração de mídias*
( ) *Carga da urna eletrônica*
( ) *Votação*
( ) *Transmissão de arquivos*
( ) *Sorteio de seções*
( ) *Teste de integridade (votação paralela)*
( ) *Conferência de hash ou validação de assinaturas na urna*
( ) *Recuperação de dados na urna eletrônica*
( ) *Apuração de votos na urna eletrônica*

Observações:

1. **O teste a ser realizado deve, obrigatoriamente, ser reproduzível.**
2. **Este plano deve conter, no máximo, 10 (dez) páginas em formato A4 ou carta.**

2

DETALHAMENTO DO TESTE

1 – Descrição geral do plano:

Utilizando escalação de privilégio para assumir controle administrativo

2 – Fundamentação teórica:

Falha de permissionamento

3 – Precondições para o teste:

Acesso ao computador SIS e variáveis de acesso.

4 – Escopo – Superfície de ataque:

Todos os softwares que rodam na plataforma SIS

5 – Janela de atuação simulada do atacante:

Durante a votação, geração de mídias, range de urna

6 – Pontos de intervenção:

Plataforma SIS e software

7 – Passos a serem realizados:

Acesso ao computador e acesso a app com possibilidade de escalar o acesso administrativo.

8 – Materiais necessários (fornecidos pelo TSE):

Computador SIS e credenciais de acesso

9 – Possíveis resultados e impacto:

Alteração dos sistemas de geração e votação

10 – Rastreabilidade:

11 – Solução proposta:

3

Data	1/12/2023
Resultado	(✓) Aprovado ( ) Aprovado com ressalvas ( ) Reprovado

Justificativa

COMISSÃO REGULADORA

7.14 Anexo N – Relatório técnico parcial do TSE

INTRODUÇÃO **4**

SUMÁRIO DOS PLANOS DE TESTES APROVADOS **5**

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 cidadão 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 a 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

NÚMEROS DO TESTE PÚBLICO DE SEGURANÇA – EDIÇÃO 2023 33

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

INTRODUÇÃO

O Teste Público de Segurança 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 Teste Público de Segurança é oportunizado aos participantes identificar eventuais vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato do voto, para que tais 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 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 cidadã ou cidadão brasileiros, maiores de 18 anos, que, individualmente ou em grupo, preencham os requisitos definidos em edital.

TESTE PÚBLICO DE SEGURANÇA DA URNA

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 cidadão 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	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	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

Tribunal Superior Eleitoral

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 teste apresentados e aprovados durante a realização do TPS 2023

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 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, via áudio, da urna eletrônica 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 cidadão 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, sem conhecer as proteções existentes, não conseguindo realizar qualquer alteração na mídia de carga.

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 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; 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 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 votos 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 *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) e Brayan Vanz de Oliveira
Apoio técnico:	Victor Takashi Hayashi (USP)
Objetivo:	Abrir a urna eletrônica e substituir o cabo HDMI por outro cabo 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) e Brayan Vanz de Oliveira
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. Este 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 técnicas:	O plano de teste foi bem-sucedido ao explorar vulnerabilidade documentada do sistema operacional Windows e o seu mecanismo de 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 eleitor, 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 eleitor, é preciso que todas as teclas digitadas pelo eleitor 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 eleitor, 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 mesmo eleitor 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 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

NÚMEROS DO TESTE PÚBLICO DE SEGURANÇA DA URNA – EDIÇÃO 2023

A fase de realização do Teste Público de Segurança de 2023 aconteceu no período de 27 de novembro a 1º de dezembro de 2023, na sede do Tribunal Superior Eleitoral, tendo sido prorrogado por mais 1 (um) dia, a pedido de 2 grupos de investigadores.

A 7ª edição alcançou um recorde de pré-inscrições, totalizando 85 pré-inscritos, 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 03 planos na semana do Teste Público de Segurança, tem-se, durante a semana do TPS, 33 participantes e 35 planos executados.

Quanto aos planos executados, foram apresentados 7 supostos achados, os quais foram analisados pela Comissão Avaliadora. Após a avaliação, a comissão recomendou o retorno de 5 desses planos para o Teste de Confirmação, com o objetivo de verificar, em versão ajustada do sistema eleitoral, a efetividade das correções a serem implementadas pela equipe do TSE.

Os achados aceitos pela Comissão Avaliadora serão avaliados pela equipe técnica da Secretaria de Tecnologia da Informação TSE, que buscará soluções efetivas e as implementará de acordo com os processos utilizados no desenvolvimento dos sistemas eleitorais.

E, para que as soluções sejam validadas, será realizado, no período de 15 a 17 de maio de 2024, o Teste de Confirmação. Conforme prevê o Edital nº 1/2023 do TPS, as investigadoras e os investigadores serão convocados para retornarem ao TSE e repetirem, em versão ajustada do sistema eleitoral, os testes que identificaram a falha, a vulnerabilidade explorada ou a fraude.

Uma vez realizados os novos testes e tendo sido comprovado o saneamento das falhas e/ou vulnerabilidades anteriormente encontradas, a investigadora, o investigador e/ou grupo de investigadores deverão assinar termo com a confirmação das correções feitas pelo TSE ou submeter nova manifestação, à qual o TSE responderá tecnicamente posteriormente.

Resumo dos números do Teste Público de Segurança - 2023	
Total de pré-inscritos	**85**
Total de planos apresentados durante a fase de pré-inscrição	**48**
Total de **inscrições aprovadas** pós 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**
Pedidos recebidos durante os testes	**178**
Pedidos deferidos ou deferidos com ressalva	**172**

Documento consolidado e revisado pelo
Núcleo Estratégico de Comunicação de Informática – Neci

Secretaria de Tecnologia da Informação – STI

7.15 Anexo O – Relatório parcial da USP

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

Laboratório de Arquitetura e Redes de Computadores

Relatório Técnico: RT-TPS2023-USP-LARC
Projeto: TPS 2023

Parceiro: Tribunal Superior Eleitoral - TSE
Referência: Convênio TSE nº 15/2023

Data: 18/12/2023

Título	Relatório Técnico RT-TPS2023-USP-LARC
Versão	1.1
Data	18/12/2023
Autores	Equipe LARC-USP TPS
Projeto	TPS 2023

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Sumário

Sumário 1
Lista de Acrônimos 3
Lista de Gráficos 4
Sumário Executivo 5
1 Introdução 6
2 Sumário dos Planos de Testes no TPS 2023 7
3 Detalhamento dos Planos de Teste 10
3.1 Quebra do sigilo do voto 10
3.2 Fragilizar do sigilo do voto 11
3.3 Invadir a mídia de carga da urna eletrônica 12
3.4 Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia 12
3.5 Fraus Omnia Corrumpit 13
3.6 Nihil Autem Absconditum Est, Quod Non Reveletur 14
3.7 Qui Duplicat, Videre Suffragio Potest 15
3.8 Suffragium Simulata Substantiam Veritas Mutare Possunt 16
3.9 Ab Initio In Validi, Post Validi 17
3.10 Omnia Invalidi Est 17
3.11 Suffragium Non Est Relatus 18
3.12 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 19
3.13 Execução do JE-Connect utilizando computador com sistema operacional inválido 20
3.14 Comportamento do JE-Connect na execução de um bot de monitoramento no computador transmissor de dados 21
3.15 USBExploit – acesso a dados da urna através da porta USB 21
3.16 Captura do vídeo transmitido na tela, com a alteração dos cabos transmissores 22
3.17 Acesso a rede do TSE por intermédio do software JE-Connect, realizando a execução de shell a partir de um dispositivo USB 23
3.18 Adulteração no JE Connect 24
3.19 Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect 25
3.20 Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConnect 27

3.21 Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JEConnect 28
3.22 Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConnect 29
3.23 Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConnect 30
3.24 Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita 31
3.25 Escalação de privilégio no Windows-SIS 32
3.26 Executar código espúrio na Urna Eletrônica modelo 2020 33
3.27 Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020 35
3.28 Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto 36
3.29 Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI 37
3.30 Alterar dados/programas nos sistemas SIS/GEDAI 39
3.31 Ataque de cold boot à Urna Eletrônica 40
3.32 Tentativa de Man-in-the-Middle na comunicação do teclado com Arduíno 41
3.33 Tentativa de reconhecimento das teclas digitadas usando IA 42
3.34 Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas 43
3.35 Inconsistência de Software 45
4 Análise do TPS 2023 47
4.1 Análise do perfil dos planos de teste 47
4.2 Análise do perfil das solicitações dos investigadores 49
5 Recomendações para o próximo TPS 53
5.1 Preparação para o evento 53
5.2 Softwares utilizados pelos investigadores no TPS 53
5.3 Infraestrutura sugerida para o TPS 54
5.4 Acesso ao código fonte 55
5.5 Atuação do apoio técnico 55
5.6 Divulgação e transparência 56
6 Considerações Finais 57

Lista de Acrônimos

ADH	Ajuste de Data e Hora
ATUE	Aplicativo de Teste da Urna Eletrônica
BU	Boletim de Urna
GAP	Gerenciador de Aplicativos
GEDAI-UE	Gerenciador de Dados, Aplicativos e Interface – Urna Eletrônica
JE	Justiça Eleitoral
LARC	Laboratório de Arquitetura e Redes de Computadores
MC	Mídia de Carga
ME	Mídia Externa
MI	Mídia Interna
MR	Mídia de Resultado
MV	Mídia de Votação
PCS	Departamento de Engenharia de Computação e Sistemas Digitais
RDV	Registro Digital do Voto
RED	Sistema de Recuperação de Dados
ROM	*Read-Only Memory*
SEINT	Seção de Integração, Garantia e Controle de Qualidade de Soluções
SETOT	Seção de Totalização e Divulgação de Resultados
SEVIN	Seção de Voto Informatizado
STE	Sistema de Teste Exaustivo
TE	Terminal do Eleitor
TM	Terminal do Mesário
TPS	Teste Público de Segurança
TRE	Tribunal Regional Eleitoral
TSE	Tribunal Superior Eleitoral
UE	Urna Eletrônica
USP	Universidade de São Paulo
VPP	Verificação Pré/Pós votação

Lista de Gráficos

Gráfico 1: Classificação dos Planos de Teste Propostos por Tipo de Ataque 47
Gráfico 2: Classificação dos Planos de Teste Propostos por Resultado Final ... 49
Gráfico 3: Classificação das Solicitações dos Investigadores durante o TPS 50
Gráfico 4: Solicitações dos Investigadores por Dia 52

Sumário Executivo

Este relatório foi elaborado para evidenciar as observações da equipe do LARC, registrando sua participação no Teste Público de Segurança – TPS 2023 – realizado nas dependências do TSE de 26 de novembro a 2 de dezembro de 2023.

Esta participação no TPS 2023 é uma atividade prevista no projeto que tem por objetivo avaliar a segurança do sistema de votação eletrônico, tanto nos aspectos de hardware, quanto de software e também de processo.

A execução do projeto contempla as etapas antes, durante e após a realização do TPS 2023. Tais atividades são previstas como objeto do Convênio-TSE nº15/2023 firmado entre o Tribunal Superior Eleitoral (TSE) e a Universidade de São Paulo (USP), cujo principal objetivo é avaliar e identificar vulnerabilidades, falhas ou potenciais pontos de melhoria em relação à integridade e ao anonimato dos votos em eleições brasileiras.

O presente relatório descreve os planos de teste alistados para o TPS 2023, considerando os executados e não executados, bem como os propostos antes e durante o TPS.

Para cada plano de teste foram identificados os investigadores proponentes, os apoios técnicos que acompanharam os investigadores, bem como descritos o objetivo do plano de teste, os passos propostos pelo investigador, o relaxamento dos mecanismos de segurança (se houve) para sua execução, o resultado e um breve comentário técnico.

Na última parte deste documento a equipe do LARC fez uma avaliação analítica do TPS, com estatísticas a partir dos números observados e coletados durante o evento, de forma a contribuir com o planejamento do próximo TPS.

Por fim, também foram feitas recomendações, sob o ponto de vista da preparação, do processo, da infraestrutura e da dinâmica de execução dos testes.

As considerações finais encerram este documento.

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

1 Introdução

Desde 2009 o Teste Público de Segurança (TPS) do sistema eletrônico de votação vem sendo aplicado com a finalidade de fortalecer a confiabilidade, transparência, segurança na captação e na apuração dos votos, além de propiciar melhorias no processo eleitoral. O principal objetivo do TPS é efetuar ações controladas com o objetivo de identificar e corrigir vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Neste contexto, o TSE e a USP, firmaram o Convênio-TSE nº15/2023, com a finalidade do Laboratório de Arquitetura e Redes de Computadores (LARC) do Departamento de Engenharia de Computação e Sistemas Digitais (PCS) da Escola Politécnica da USP, planejar, executar testes que antecederam o TPS, relatar pontos de melhoria ao TSE, além de acompanhar o TPS, emitir relatórios de acompanhamento com recomendações, bem como verificar a eficácia das soluções empregadas para correção de possíveis vulnerabilidades ou falhas.

Para acompanhamento dos trabalhos do TPS 2023, a equipe do LARC foi composta pelos seguintes pesquisadores:

- Wilson Vicente Ruggiero
- Marcos Antonio Simplicio Junior
- Yeda Regina Venturini
- Andrea Erina Komo
- Eduardo Seiti Teruiya
- Felipe Kenzo Shiraishi
- Fernando Frota Redígolo
- Firmiano Ramos Perlingeiro
- Gabriel Soares dos Santos Nunes
- Guilherme Fumagali Marques
- Matheus Santhiago Araujo Januario
- Matheus Tavares de Andrade
- Nelson Yamamoto
- Ryan Weege Achjian
- Victor Takashi Hayashi

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

2 Sumário dos Planos de Testes no TPS 2023

Plano de Teste		Situação Final	Data Término	Investigador(es)	
				ID	Nome(s)
1	Quebra do sigilo do voto	Executado s/ achado	30/11	I-1	Aline Barbosa da Silva Ferreira
2	Fragilizar sigilo do voto	Executado s/ achado	30/11		
3	Invadir a mídia de carga da urna eletrônica	Executado s/ achado	01/12		
4	Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia	Executado s/ achado	30/11	I-2	Érika Maria Rodrigues de Castro
5	Fraus Omnia Corrumpit	Executado s/ achado	30/11	I-3	Guilherme Henrique dos Santos
6	Nihil Autem Absconditum Est, Quod Non Reveletur	Executado s/ achado	30/11		
7	Qui Duplicat, Videre Suffragio Potest	Executado s/ achado	30/11		
8	Suffragium Simulata Substantiam Veritas Mutare Possunt	Executado s/ achado	30/11		
9	Ab Initio In Validi, Post Validi **(*)**	Executado s/ achado	01/12		
10	Omnia Invalidi Est **(*)**	Executado s/ achado	30/11		
11	Suffragium non est relatus **(*)**	Executado s/ achado	30/11		
12	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	Executado s/ achado	28/11	I-4	João Benedito dos Santos Junior
13	Execução do JE-Connect utilizando computador com sistema operacional inválido	Executado s/ achado	28/11	I-5	Nicholas Barros dos Santos
14	Comportamento do JE-Connect na execução de um bot de monitoramento no computador transmissor de dados	Executado s/ achado	30/11		
15	USBExploit – acesso a dados da urna através da porta USB	Executado s/ achado	01/12	G-1 (Atitus)	Marcos Roberto dos Santos, Leandro Caletti, Eduardo Bido e Rhayra Rodrigues Florentin
16	Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores	Executado s/ achado	01/12	G-2 (Atitus)	Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili e Brayan Vanz de Oiliveira
17	Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de shell a partir de um dispositivo USB	Executado s/ achado	01/12		

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Plano de Teste		Situação Final	Data Término	Investigador(es)	
				ID	Nome(s)
18	Adulteração no JE Connect	Executado s/ achado	29/11	G-3	Vitor Aloisio do Nascimento Guia e Hitatiana Maria Santiago Ferreira da Silva Guia
19	Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect	Executado c/ achado	30/11	G-4 (UFMS)	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
20	Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConnect	Executado s/ achado	30/11		
21	Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JEConnect	Executado s/ achado	30/11		
22	Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConnect	Executado s/ achado	30/11		
23	Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConnect	Executado s/ achado	30/11		
24	Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita	Executado s/ achado	30/11		
25	Escalação de privilégio no Windows-SIS **(*)**	Executado c/ achado	01/12		
26	Executar código espúrio na Urna Eletrônica modelo 2020	Executado c/ achado	30/11	G-5 (PF)	Galileo Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
27	Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020	Executado c/ achado	02/12		
28	Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto	Não executado	–		
29	Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI	Executado c/ achado	28/11		
30	Alterar dados / programas nos sistemas SIS/GEDAI	Não executado	–		
31	Ataque de cold boot à Urna Eletrônica	Não executado	–		
32	Tentativa de Man-in-the-Middle na comunicação do teclado com Arduíno	Executado s/ achado	29/11	G-6 (UFF)	Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Camila Ferreira Alves e Caubi de Souza Loureiro Rosa
33	Tentativa de reconhecimento das teclas digitadas usando IA	Executado c/ achado	02/12		

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Plano de Teste		Situação Final	Data Término	Investigador(es)	
				ID	Nome(s)
34	Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas	Executado c/ achado	30/11	G-7	André Mário dos Reis dos Santos, Alexandre Zago Boava e Diego Vergaças de Sousa Carvalho
35	Inconsistência de Software	Executado s/ achado	01/12	G-8	Ariel Rossetto Ril e Daniel Dalalana Bertoglio

(*) Planos de Teste propostos pelo(s) investigador(es) no decorrer do TPS 2023 a aprovados pela Comissão Reguladora.

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

3 Detalhamento dos Planos de Teste

3.1 Quebra do sigilo do voto

Investigadora: Aline Barbosa da Silva Ferreira

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.

Resultado: Executado sem achados.

Etapas Propostas:

1. Inicia-se votação na urna eletrônica;
2. Primeiro eleitor hipotético 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.

Relaxamento nos mecanismos e procedimentos 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 a seção 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. Conforme explicado à investigadora pelo TSE, a situação relatada já foi discutida e está registrada no Acórdão TSE, da

sessão de 2/9/2010, processo administrativo Nº 1089-06.2010.6.00.0000/DF, relator Ministro Marco Aurélio. No voto, o Ministro descreve que a situação retratada é de ocorrência improvável, mas, caso ocorra, há de se garantir o direito à cidadania (manifestação da vontade por meio do voto), ainda que haja o risco de identificação do voto do eleitor. Além disso, foi explicado para a investigadora que a recomendação do TSE é que o primeiro eleitor não seja liberado para ir embora até que o segundo eleitor da mesma seção conclua o voto.

3.2 Fragilizar do sigilo do voto

Investigadora: Aline Barbosa da Silva Ferreira

Apoio Técnico: Andrea Erina Komo (USP)

Objetivo: Testar se as teclas, ao serem acionadas pelo eleitor, são realmente criptografadas e não há qualquer vulnerabilidade no teclado da urna eletrônica.

Resultado: Executado sem achados.

Etapas Propostas:

1. Instalar, na saída de áudio da urna eletrônica (habilitada para deficientes visuais), um dispositivo com fio auxiliar conectado a uma caixa de som para testar as teclas;
2. Ao pressionar uma tecla, sua identificação será transmitida pela caixa de som.

Relaxamento nos mecanismos e procedimentos 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 caixa de som pelo TSE.

Considerações técnicas: Nesse teste, a investigadora propôs uma eventual quebra do sigilo do voto do eleitor por conta 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 via áudio da urna eletrônica funciona corretamente. Ao menos em princípio, só haveria um vazamento do áudio se o próprio eleitor quisesse quebrar seu sigilo, pedindo a

ativação do som e ligando o dispositivo de áudio correspondente, situação indevida que seria facilmente identificada pelo mesário ou outros presentes.

3.3 Invadir a mídia de carga da urna eletrônica

Investigadora: Aline Barbosa da Silva Ferreira

Apoio Técnico: Andrea Erina Komo (USP)

Objetivo: Invadir a mídia de carga da urna eletrônica fazendo a limitação de votos aos candidatos de uma seção.

Resultado: Executado sem achados.

Etapas Propostas:

1. Conectar a mídia de carga em um computador;
2. Tentar invadir a mídia de carga;
3. Limitar os votos aos candidatos da mídia de carga;
4. Testar a mídia de carga limitada instalando na urna.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS.

Considerações técnicas: O teste proposto visava limitar o número de votos de algum candidato alterando a mídia de carga. A investigadora tentou alterar a mídia de carga, sem conhecer as proteções existentes, não conseguindo realizar qualquer alteração pretendida.

3.4 Mídia de Resultado: a confiança do cidadão 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, 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.

Resultado: Executado sem achados.

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. Testar a 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.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento do usuário/senha do SIS.

Considerações técnicas: O teste proposto visava limitar o número de votos de algum candidato alterando a mídia de carga. A investigadora tentou alterar a mídia de carga, sem conhecer as proteções existentes, não conseguindo realizar qualquer alteração pretendida.

3.5 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 eleitor e, com isso, manipular o resultado da votação.

Resultado: Executado sem achados.

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 aparente teclas inversas ao realmente teclado.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

Considerações técnicas: O investigador não conseguiu realizar o seu teste por não possuir componentes apropriados para implementar a sua prova de conceito. Apesar da ausência de execução, uma discussão foi feita para falar sobre as suas preocupações ao ter proposto tal teste. O investigador sugeriu 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; enfatizou a sugestão de melhoria feita sobre cifrar o canal de comunicação da tela.

3.6 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 entre os arquivos e da ordem de eleitores habilitados, violar o sigilo do voto.

Resultado: Executado sem achados.

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 eleitor 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.

Relaxamento nos mecanismos e procedimentos 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 os eleitores da seção. Argumentou que é um cenário válido somente para o caso de violação do sigilo do voto do último eleitor. Há uma decisão do TSE (vide item "3.1. Quebra do sigilo do voto") sobre o significado da quebra de sigilo do voto do último eleitor, sendo uma possibilidade já conhecida pelo TSE e que é tomada como risco aceitável. O investigador sugeriu que fossem impedidas cópias binárias de mídias de aplicação, apesar de reconhecer o aumento do custo associado.

3.7 Qui Duplicat, Videre Suffragio Potest

Investigador: Guilherme Henrique dos Santos

Apoio Técnico: Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)

Objetivo: Violar 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.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

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, constatou incompatibilidade no conector físico entre seu dispositivo e o utilizado pela urna.

3.8 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 votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.

Resultado: Executado sem achados.

Etapas Propostas:

1. Iniciar a votação na urna oficial (UE-A);
2. Iniciar votação na urna de contingência 1 (UE-B);
3. Habilitar eleitores e inserir votos espúrios na UE-B conforme 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.

Relaxamento nos mecanismos e procedimentos 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.

3.9 Ab Initio In Validi, 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.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

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.

3.10 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.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.11 Suffragium Non Est Relatus

Investigador: Guilherme Henrique dos Santos

Apoio Técnico: Felipe Kenzo Shiraishi (USP) e Eduardo Gil Tivanello (TRE/RO)

Objetivo: Verificar se um eleitor já votou, após introduzir uma mídia de votação que não tenha sido clonada antes do voto na urna eletrônica.

Resultado: Executado sem achados.

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 mesmo eleitor que inseriu o primeiro voto.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

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.

3.12 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.

Resultado: Executado sem achados.

Etapas Propostas:

1. Preparar ambiente;
2. Extrair arquivos da urna;
3. Verificar assinatura dos arquivos.

Relaxamento nos mecanismos e procedimentos 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, onde a chave seria 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 que, para acessar os arquivos da forma pretendida, seria necessário extrair o hardware de armazenamento secundário da urna eletrônica. Então, ao invés de consultar todos os arquivos, foi verificada com sucesso a integridade apenas dos arquivos da mídia de aplicação.

3.13 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.

Resultado: Executado sem achados.

Etapas Propostas:

1. Simular eleição com 10 votos;
2. Apurar os votos;
3. Executar JE-Connect com o sistema operacional inválido.

Relaxamento nos mecanismos e procedimentos de segurança: Remoção da chave de ativação do MS-Windows; Fornecimento de usuário/senha do SIS e 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.

3.14 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 onde será executado o JE-Connect, analisando seu comportamento para avaliar a integridade e segurança da transmissão dos votos para o TSE.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.15 USBExploit – acesso a dados da urna através da porta USB

Investigadores: Grupo Atitus: Marcos Roberto dos Santos, Leandro Caletti, Eduardo Bido e Rhayra Rodrigues Florentin

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Apoio Técnico: Firmiano Ramos Perlingeiro e Guilherme Fumagali Marques (USP)

Objetivo: Capturar informações da urna através da conexão de um cabo console ou adaptador USB (com conexão Ethernet ou Serial), que possibilite acesso aos dados, bem como dos votos inseridos.

Resultado: Executado sem achados.

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 as chaves de assinatura.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de Usuário/senha do SIS e Kit/senha do JE-Connect; Concedida 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, observou-se que a urna não recebia um endereço IP de forma automática. Após os testes de conexão Ethernet, foi tentada a conexão por meio de um adaptador USB - USB-C para a urna, cenário este que não resultou em comunicação de dados e energia.

3.16 Captura do vídeo transmitido na tela, com a alteração dos cabos transmissores

Investigadores: Grupo Atitus: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili e Brayan Vanz de Oliveira

Apoio Técnico: Victor Takashi Hayashi (USP)

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Objetivo: Abrir a urna eletrônica e substituir o cabo HDMI por outro cabo que possua um dispositivo intermediário, enviando a imagem da tela para outro dispositivo conectado via Bluetooth.

Resultado: Executado sem achados.

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 pessoas estão votando.

Relaxamento nos mecanismos e procedimentos 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 não foi descoberta pelos investigadores.

3.17 Acesso a rede do TSE por intermédio do software JE-Connect, realizando a execução de shell a partir de um dispositivo USB

Investigadores: Grupo Atitus: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili e Brayan Vanz de Oliveira

Apoio Técnico: Victor Takashi Hayashi (USP)

Objetivo: Abrir um shell no sistema operacional responsável pela comunicação do JE-Connect, obtendo acesso a rede do TSE.

Resultado: Executado sem achados.

Etapas Propostas:

1. Conectar o pendrive (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.

Relaxamento nos mecanismos e procedimentos 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 pendrive.

Considerações técnicas: Foi executado o script "window.print" para abrir o assistente de impressão com impressora PDF. Essa janela, ao habilitar navegação entre diretórios, permitiu observar os arquivos presentes no JE-Connect.

3.18 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 no JE-Connect. O objetivo é avaliar o comportamento do Kit do JE-Connect quando um agente obtém privilégio não autorizado de usuário root e tenta adulterar o software JE-Connect, bem como transmitir dados adulterados da Mídia de Resultados (MR).

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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 tiveram êxito.

3.19 Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect

Investigadores: Grupo UFMS: 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 invasores tenham acesso a informações confidenciais e/ou possam inserir um código executável.

Resultado: **Executado COM achado**.

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.

Relaxamento nos mecanismos e procedimentos 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, situação na qual o sistema informa que o limite foi excedido, e que será reiniciado;
4. Teclar Ctrl+C, cancelando o processo de reinicio, o que tem efeito similar a zerar o número de tentativas de login inválidas.

O sistema JE-Connect foi planejado para, a cada três erros de credenciais, realizar o reboot do kit, de forma 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. Este parâmetro não foi implementado no JE-Connect disponibilizado no TPS, apesar de ser uma necessidade já mapeada pela equipe de desenvolvimento do JE-Connect. 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 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 um eleitor votou.

3.20 Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JEConnect

Investigadores: Grupo UFMS: 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 vulnerabilidade da linguagem de programação Python. Especificamente, os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, permitindo a um invasor abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas, ou contornar firewalls.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.21 Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JEConnect

Investigadores: Grupo UFMS: 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 vulnerabilidade da linguagem de programação Python. Especificamente, 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. Essa vulnerabilidade 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.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.22 Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JEConnect

Investigadores: Grupo UFMS: 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 invocar 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__”.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.23 Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita e nas bibliotecas Python no Software JEConnect

Investigadores: Grupo UFMS: 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 a informações potencialmente sigilosas.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.24 Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita

Investigadores: Grupo UFMS: 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 a informações confidenciais, com escalada de privilégio.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

3.25 Escalação de privilégio no Windows-SIS

Investigadores: Grupo UFMS: 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 através da impressão da lista de certificados no VAP do SIS-desktop.

Resultado: **Executado COM achado**.

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 icone 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.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS e Kit/senha do JE-Connect.

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. Foi identificado no código fonte que o fechamento de proteção é solicitado, mas, 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. O privilégio permitiu aos investigadores ler, alterar ou apagar arquivos. A eventual alteração do conteúdo de arquivos assinados provocaria inconsistência e bloqueio do equipamento pelo SIS. Alterações também seriam detectadas com o uso do VAD ou VAP. Apesar do achado, a visualização dos arquivos mantidos no SIS e assinados digitalmente não produz efeitos sobre a integridade ou o sigilo do voto. A eventual alteração dos arquivos ensejaria incoerência de assinatura digital, uma vez que os arquivos são verificados pelo Gedai no momento de sua execução.

3.26 Executar código espúrio na Urna Eletrônica modelo 2020

Investigadores: Grupo Polícia Federal: Galileo 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.

Resultado: **Executado COM achado**.

Etapas Propostas:

1. Clonar mídia de carga;
2. Carregar sua imagem no USBArmory;

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

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.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS/GEDAI-EU para geração de mídias de carga. Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI.

Considerações técnicas: A equipe de investigadores revelou um problema na cadeia de confiança da urna. Mais especificamente, ficou evidenciada a existência de um bug na forma como o BIOS/UEFI da urna lida com o bootloader contido na mídia de carga: o processo é feito em duas etapas, uma primeira responsável por ler o conteúdo da mídia e validar seu conteúdo (*Time of Check* – TOC), e uma segunda por entregar o controle ao bootloader ainda contido na mídia de carga (*Time of Use* – TOU). A falta de atomicidade desse processo permite o ataque de TOCTOU no qual, logo após o fim da primeira etapa, o bootloader validado é adulterado, dado que seu conteúdo se encontra em local controlado pelo atacante. Assim, os investigadores foram capazes de manipular de forma arbitrária o código do bootloader, concentrando-se em duas ações a título de prova de conceito: expor a chave de decifração do kernel (chave de sistema operacional) e exibição de mensagem na tela da urna por meio de ASCII art. Não foram feitas modificações no kernel do sistema operacional, bibliotecas ou aplicativos da urna – embora a equipe tenha tentado fazer esse tipo de modificação usando o mesmo método de TOCTOU, e ainda que isso seja tecnicamente possível em teoria. Como principal limitação do ataque, cabe observar que a via explorada envolve a interceptação do tráfego USB da mídia de aplicação (uma mídia externa), seguida de manipulações limitadas somente sobre a mídia de carga. Consequentemente, as modificações feitas sobre o bootloader não seriam replicáveis para a mídia

interna da urna. Mais precisamente, mesmo que o ataque de TOCTOU realizado levasse à gravação de algo indevido na mídia interna da urna (e.g., o próprio bootloader modificado), tal modificação seria prontamente identificada pela cadeia de confiança da urna, em particular pelo BIOS não modificada do equipamento. Em particular, nos testes realizados pelos investigadores, 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. Consequentemente, a estratégia de TOCTOU utilizada não seria capaz de afetar processos que dependem da mídia interna, o que inclui o processo de votação em si. Em conclusão, 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 durante uma eleição real.

3.27 Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020

Investigadores: Grupo Polícia Federal: Galileo 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.

Resultado: **Executado COM achado**.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS/GEDAI-EU para geração de mídias de carga. Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI.

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 descrito no item "3.26 Executar código espúrio na Urna Eletrônica modelo 2020". Com a capacidade de manipulação do bootloader, a equipe de investigadores identificou um ponto no código que, uma vez modificado, permitiria expor 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 seria derivada a chave de decifração do RDV. Portanto, a partir da chave do SO, não foi possível obter a chave de decifração do RDV, a despeito de possibilidade teórica de fazê-lo a partir da semente exposta.

3.28 Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto

Investigadores: Grupo Polícia Federal: Galileo 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)

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

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.

Resultado: **Não executado**.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

Considerações técnicas: Plano de teste não executado por opção dos investigadores. A despeito disso, considerando sucesso de etapas preliminares anteriores, cabe mencionar que a capacidade de decifrar e cifrar um RDV não seria condição suficiente para gerar um arquivo válido para a urna. Afinal, o arquivo de RDV é mantido cifrado e assinado digitalmente pelo hardware de segurança da urna: mesmo que ele seja decifrado, manipulações indevidas invalidariam a assinatura realizada pela urna. Em outras palavras, como não foi identificada qualquer vulnerabilidade envolvendo o mecanismo de verificação de integridade do RDV, a chave de decifração do RDV não permitiria sua manipulação pelos investigadores.

3.29 Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI

Investigadores: Grupo Polícia Federal: Galileo Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

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/decifrar o disco da máquina onde são executados os softwares SIS/GEDAI.

Resultado: **Executado COM achado**.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS/GEDAI-EU para geração de mídias de carga. Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI.

Considerações técnicas: Usando o PCILeech, os investigadores foram capazes de obter a chave do Bitlocker carregada na memória RAM do sistema, permitindo a abertura das partições Bitlocker nas quais residem o SIS e os sistemas eleitorais. Cabe notar, contudo, que fazê-lo não é condição suficiente para o comprometimento do Gedai-UE, uma vez que ele 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. Essa Nenhuma dessas barreiras de segurança foi exercitada pelo grupo de investigadores no TPS, embora tenham sido analisadas pela equipe de pesquisadores da USP em busca de vulnerabilidades (já assumindo, para fins investigativos, eventual superação da barreira imposta pelo Bitlocker). Ainda que essas proteções fossem hipoteticamente superadas, resultando no comprometimento do Gedai-UE (algo que não foi realizado), não se vislumbra uma forma pela qual tal ataque seria capaz de alterar o software da urna ou dados de votação. Afinal, o software e os dados são protegidos por assinaturas digitais geradas fora do Gedai-UE e validadas pela urna.

3.30 Alterar dados/programas nos sistemas SIS/GEDAI

Investigadores: Grupo Polícia Federal: Galileo 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.

Resultado: **Não executado**.

Etapas Propostas:

1. Instalar a placa PCILeech no desktop onde 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:
    a. Desativar as proteções do Subsistema de Instalação e Segurança (SIS);
    b. Instalar um debugger na máquina;
    c. Modificar programas/estrutura de dados que propagam informações entre a urna e seu ecossistema. Ex.: Modificar a tabela de correspondência ou não transmití-la, porém registrar em logs que ela foi transmitida.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

Considerações técnicas: Plano de teste não executado por opção dos investigadores.

3.31 Ataque de cold boot à Urna Eletrônica

Investigadores: Grupo Polícia Federal: Galileo 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 para extração dos dados em leitor externo para posterior decodificação.

Resultado: **Não executado**.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

Considerações técnicas: Plano de teste não executado por opção dos investigadores.

3.32 Tentativa de Man-in-the-Middle na comunicação do teclado com Arduíno

Investigadores: Grupo UFF: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Camila Ferreira Alves e Caubi de Souza Loureiro Rosa

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.

Resultado: Executado sem achados.

Etapas Propostas:

1. Interconectar um arduino entre o teclado e placa mãe;
2. Capturar os dados transitados entre teclado e placa mãe;
3. Analisar os dados coletados com o objetivo de violar o sigilo.

Relaxamento nos mecanismos e procedimentos 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. Com isso, todas as demais etapas do plano ficaram comprometidas.

3.33 Tentativa de reconhecimento das teclas digitadas usando IA

Investigadores: Grupo UFF: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Camila Ferreira Alves e Caubi de Souza Loureiro Rosa

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.

Resultado: **Executado COM achado**.

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);

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

3. Capturar outros sinais sonoros do teclado, não conhecidos, para reconhecimento pela IA, violando assim o sigilo.

Relaxamento nos mecanismos e procedimentos de segurança: Nenhum.

Considerações técnicas: Os investigadores obtiveram em testes preliminares rodados em GPU, com uso de uma placa de video RTX3060, uma acurácia de 70% no reconhecimento de teclas digitadas em uma única urna eletrônica. O percentual aleatório é de aproximadamente 7,7%. A média de acurácia de aproximadamente 50% foi obtida testando com dois modelos de urnas diferentes e posições variadas de microfone. Durante o TPS, entretanto, os resultados alcançados não foram suficientes para predizer a tecla pressionada com a mesma acurácia. De qualquer forma, entende-se que a estratégia de uso de um microfone é uma abordagem interessante para a tentativa de quebra de sigilo do voto, sem que seja capaz de adulterar sua destinação. Apesar disso, e ainda que haja uma maior capacidade de coleta de dados para aprendizado de máquina, aumentando o número de amostras e tempo de treinamento, a aplicabilidade no caso real ainda é um obstáculo relevante. Razões incluem a dificuldade de: capturar som em uma seção eleitoral, com microfones direcionais (que possibilitariam um menor ruído) ou de qualquer outro tipo; manter um microfone camuflado na cabine de votação, sujeitas a inspeções periódicas pelos mesários; identificar quem seria o eleitor votando, informação que não seria capturada por eventual microfone na cabine. Assim, na prática, a estratégia proposta não parece ter vantagens claras em relação a outras tecnologias de captura externas à urna (e que não constituem uma vulnerabilidade inerente a ela), como o uso de uma micro-câmera apontada para a cabine, capturando tanto o teclado do equipamento como a face do eleitor.

3.34 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

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

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 das teclas.

Resultado: **Executado COM achado**.

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 um tecla ou um grupo de teclas pressionado por um período longo.

Relaxamento nos mecanismos e procedimentos 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: Os investigadores perceberam que o acionamento de duas teclas ao mesmo tempo leva a urna a não registrar os comandos das teclas. Duas teclas pressionadas simultaneamente, entretanto, permitiram que uma terceira fosse reconhecida, como se não houvesse qualquer outra tecla pressionada. Já uma quarta tecla não é mais reconhecida. Os investigadores alegaram a hipótese de que, após a digitação do número de um cargo completo,

uma tecla poderia ser mantida pressionada, impedindo, por exemplo, o reconhecimento da tecla “CONFIRMA”. Esse fato permitiria a criação de um vídeo malicioso, ao não mostrar a tecla mantida pressionada, levando o espectador a ser enganado, crendo que a urna não estaria permitindo o voto num determinado candidato. Por outro lado, já foram observados no passado vídeos com conteúdo similarmente enganoso, em que acontece o pressionamento de teclas não mostradas no vídeo. Logo, não soa correto assumir que se trata de algo “novo”, ou sequer intensificado pelo suposto achado da equipe. De qualquer forma, foi explicado aos investigadores que o requisito do edital de licitação está sendo satisfeito, de que o acionamento concomitante de duas teclas deve impedir o acionamento de qualquer outra tecla, impedindo que o eleitor registre um voto equivocadamente.

3.35 Inconsistência de Software

Investigadores: 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.

Resultado: Executado sem achados.

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.

Relaxamento nos mecanismos e procedimentos 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.

4 Análise do TPS 2023

4.1 Análise do perfil dos planos de teste

Com base nos planos de teste propostos pelos investigadores e nos registros de acompanhamento de execução de testes elaborados pelo Apoio Técnico, a equipe do LARC elaborou análises que poderão contribuir com o planejamento e dinâmica dos próximos TPS.

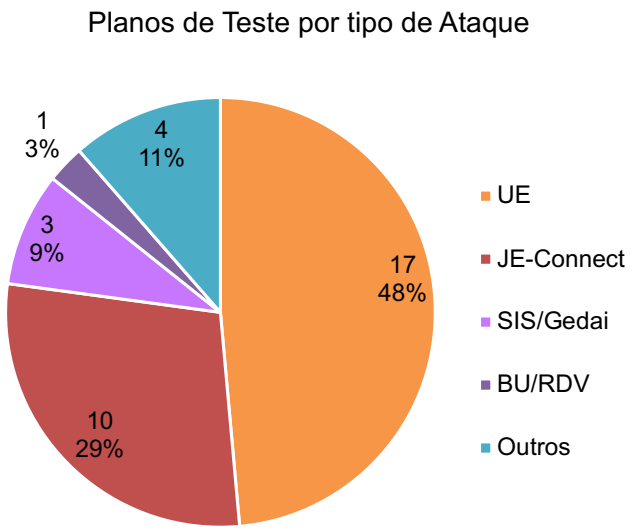


Gráfico 1: Classificação dos Planos de Teste Propostos por Tipo de Ataque

Os planos de teste propostos pelos investigadores foram classificados de acordo com o objetivo primário declarado, conforme mostrado no Gráfico 1.

É possível observar que os ataques diretos à urna eletrônica, sejam físicos (abrindo o gabinete e acessando o hardware) ou lógicos (por software) representaram quase a metade dos ataques propostos. Esse número é

ligeiramente superior ao observado no TPS 2021, onde 41% dos ataques foram direcionados à urna eletrônica. O JE-Connect representou quase 30% dos ataques no TPS 2023, indicando um aumento em relação aos 25% observados no TPS 2021.

A tabela a seguir apresenta a classificação dos planos de teste que serviram de base para a o gráfico 1.

Foco do Ataque	Total de Planos	Plano de Teste (Número no Sumário)
UE	17	1, 2, 5, 6, 7, 8, 9, 11, 15, 16, 26, 27, 28, 31, 32, 33, 34
JE-Connect	10	13, 14, 17, 18, 19, 20, 21, 22, 23, 24
SIS/Gedai	3	25, 29, 30
BU/RDV	1	10
Outros	4	3, 4, 12, 35

Dos 35 planos de teste propostos pelos investigadores, e aprovados pelo TSE, apenas 3 não foram executados, por opção dos investigadores. Dos 32 planos de teste executados, 7 terminaram com achados. Um achado não é necessariamente uma falha ou vulnerabilidade, mas uma oportunidade de melhoria ou aperfeiçoamento, sem implicar em um comprometimento na segurança dos sistemas de votação.

Com exceção da equipe da PF (Polícia Federal), observou-se (a exemplo do TPS 2021) que os demais investigadores não adotaram uma metodologia clara ou estruturada para execução dos planos de teste propostos, obtendo avanços principalmente por tentativa e erro. A execução por tentativas aleatórias, sem o devido registro dos passos executados e dos resultados parciais obtidos, dificultou a retomada dos testes entre um dia e outro, bem como as aferições de progresso

ao final de cada dia. Apesar disso, todos os investigadores consideraram seus planos de teste executados; a única exceção foi a própria equipe da PF, que optou por não executar 3 dos seus planos, conforme o gráfico 2.

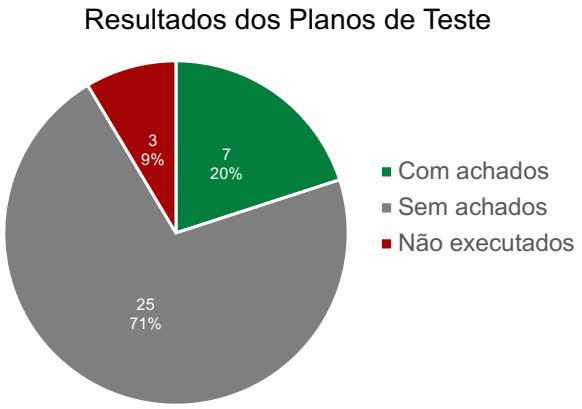


Gráfico 2: Classificação dos Planos de Teste Propostos por Resultado Final

4.2 Análise do perfil das solicitações dos investigadores

Com base nas solicitações feitas pelos investigadores durante o TPS, a equipe do LARC elaborou análises que poderão contribuir com o planejamento e dinâmica do próximo TPS.

Do total de 178 solicitações feitas pelos investigadores durante o TPS para auxiliar na execução dos planos de testes, apenas 6 foram indeferidas pela Comissão Reguladora. Esses indeferimentos ocorreram principalmente por estarem em desacordo com o edital do TPS 2023.

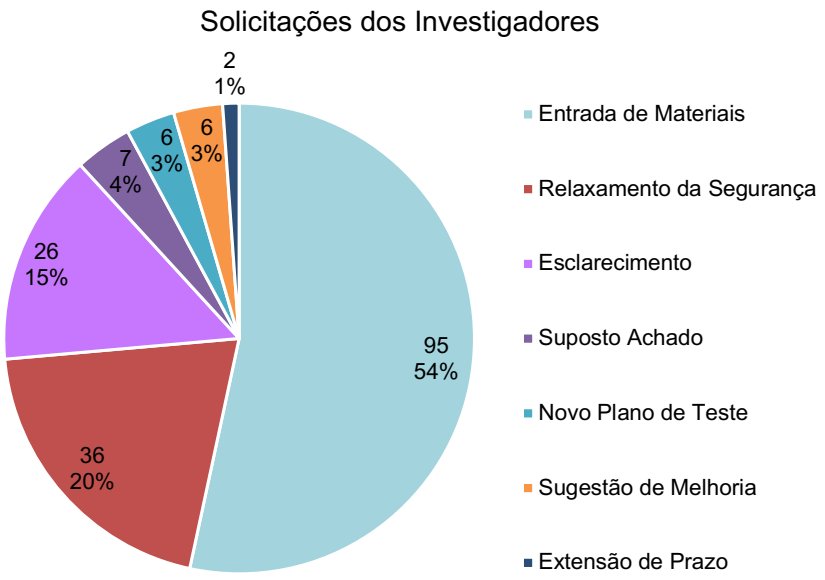


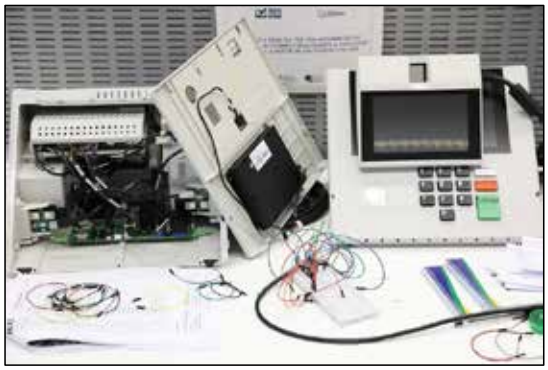
Gráfico 3: Classificação das Solicitações dos Investigadores durante o TPS

No gráfico 3, as solicitações para autorização de instalação e uso de softwares diversos foi agrupada nas solicitações de entrada de materiais, tornando o número bastante representativo.

De outro lado, o tempo gasto pelos investigadores no processo de download dos softwares autorizados (em estações específicas com acesso à Internet), cópia para pendrives (realizados somente pelo Apoio Técnico devido às restrições impostas pelas configurações das estações com acesso à Internet) e instalação em suas respectivas estações de trabalho, foi bastante significativa.

Ainda com base no gráfico 3, é possível afirmar que as requisições para entrada de materiais diversos (softwares, dispositivos e equipamentos) foi representativa e positiva para os investigadores, que puderam entrar com equipamentos como notebooks, placas, cabos, fones de ouvido etc.

Foi autorizado pela Comissão Reguladora que alguns investigadores abrissem o gabinete da urna eletrônica para medir sinais elétricos na tentativa de ataque, conforme foto a seguir.



Outros investigadores tiveram autorização para entrar com placas conforme foto a seguir.

O gráfico 4 indica que aproximadamente 58% das solicitações foram feitas nos dois primeiros dias do TPS, incluindo a maioria dos pedidos para relaxamento dos mecanismos e procedimentos de segurança e entrada de materiais.

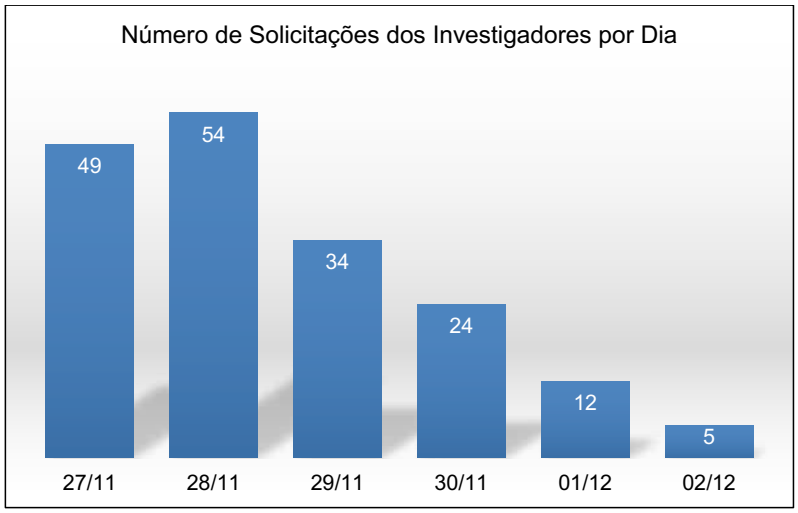


Gráfico 4: Solicitações dos Investigadores por Dia

A exemplo do TPS 2021, há destaque para o primeiro dia do TPS 2023 em que as atividades transcorreram das 14:00 às 18:00, com 49 solicitações. Isso corresponde a pouco menos que as 54 solicitações do segundo dia inteiro, que transcorreu das 09:00 às 18:00.

O último dia do TPS (02/12) contou apenas com os investigadores da Polícia Federal e da UFF, que permaneceram das 09:00 às 13:00.

5 Recomendações para o próximo TPS

5.1 Preparação para o evento

- Acolher demandas de softwares que os investigadores gostariam de ter no ambiente do TPS, pré-instalando os que forem aprovados pela Comissão Organizadora/Comissão Reguladora. Assim seria evitada a necessidade de avaliação sumária de um software/pacote, pela Comissão Reguladora durante o TPS, fazendo com que o investigador invista tempo na execução do plano de teste ao invés de gastar tempo com a instalação de pacotes.
- Disponibilizar no portal do TPS um "resumo amigável" (além do edital) em que sejam colocados exemplos do que o investigador poderá e não poderá fazer, preferencialmente com fotos de edições anteriores. Por exemplo, pode ser deixada clara a possiblidade de abertura do gabinete da urna eletrônica. Esse tipo de atitude proativa deve ajudar a evitar a desinformação de que no TPS “tudo é muito restrito";
- Disponibilizar no portal do TPS, além dos relatórios dos TPS anteriores, artigos relevantes (como os publicados no SBSeg). Assim, os investigadores teriam material de consulta com procedimentos e melhorias já realizadas na urna eletrônica e nos sistemas envolvidos, para evitar a repetição de proposição de planos de testes, além de sanar eventuais dúvidas.

5.2 Softwares utilizados pelos investigadores no TPS

- Disponibilizar um conjunto de softwares básicos pré-instalados, solicitados pela grande maioria dos investigadores, em particular os que foram usados nos TPS 2021 e 2023. Observa-se que a tendência é que haja um crescimento das necessidades de pacotes de software a cada edição;
- Disponibilizar repositório Python (PiP);

- Substituir Linux dos investigadores por uma distro voltada a testes de segurança, como o Kali Linux (quase todos os grupos solicitaram e efetivamente o utilizaram neste TPS);
- Facilitar a instalação de pacotes no Linux, de maneira que o investigador possa instalar diretamente da máquina, sem precisar de autorização ou downloads manuais. O fato de alguns pacotes demandarem dependências tornou a instalação mais complexa e lenta, com múltiplas interações. Algumas sugestões neste sentido:
    a) Disponibilizar mirror local do repositório Linux, que possa ser invocado com apt-get em uma rede local isolada, facilitando instalação após autorização (evita perda de tempo com instalação de dependências);
    b) Disponibilizar repositório-cache com pacotes já pré-autorizados e baixados. Se um investigador obtiver autorização, outros poderiam se beneficiar obtendo acesso também, mediante simples aprovação de solicitação, sem a necessidade da equipe técnica ter que executar o mesmo procedimento várias vezes durante o TPS;
    c) Possivelmente, controlar acesso à Internet via navegação Proxy.

5.3 Infraestrutura sugerida para o TPS

- Disponibilizar aos investigadores, em um servidor interno, os instaladores de alguns softwares open-source pré-autorizados como, por exemplo: virtualizadores (e.g. VirtualBox e VMWare Player) e Disassemblers (e.g. IDA Pro, Cutter, Ghydra);
- Disponibilizar para os investigadores, em um servidor interno, imagens bootáveis ou VMs de algumas distros open-source pré-autorizadas como, por exemplo: Kali Linux, REMnux, CAINE e Hiren's Boot PE.

5.4 Acesso ao código fonte

- Orientar o Apoio Técnico de forma que um investigador e principalmente grupos de investigadores, nunca fiquem sem supervisão no momento do acesso ao código fonte;
- Zelar pelos controles de acesso ao código fonte com registro de solicitação de acesso em formulários, com termo de responsabilidade.

5.5 Atuação do apoio técnico

- Adoção de formulários eletrônicos, eliminando, por exemplo, a necessidade de transcrição das notas de Acompanhamento dos Testes Públicos em papel para o digital;
- Disponibilização de tablets para a equipe de apoio técnico, de maneira a agilizar o preenchimento de formulários eletrônicos de requisição dos investigadores, sem a necessidade de se ausentar da bancada de testes;
- Adoção de uma ferramenta open source do tipo issue tracking (e.g.: Jira) para controlar as solicitações e autorizações;
- Eliminação da lista “Protocolo de Solicitações” por meio da implementação de workflow eletrônico de tratamento da solicitação;
- Aprovação eletrônica das solicitações pela Comissão Reguladora, por meio de workflow automatizado, dando mais celeridade ao processo e visibilidade à Comissão Avaliadora, que poderia acompanhar as solicitações dos investigadores em tempo real;
- Disponibilizar apoios técnicos dos TREs, em esquema de rodízio, nas próximas edições do TPS, para elucidar dúvidas e acolher de sugestões dos investigadores. Nos TPS 2021 e 2023, observou-se que muitas dúvidas e sugestões dos investigadores eram relacionadas ao processo eleitoral (por exemplo, logística das urnas eletrônicas, registro de candidatos e legislação

eleitoral) melhor conhecidas pelos servidores dos TREs, fugindo em alguns momentos da alçada técnica por parte dos apoios da USP;

- Manter sempre dois apoios técnicos por bancada, no caso de grupos de investigadores, pois houve situações em que o grupo se dividiu para executar paralelamente dois planos distintos ou mesmo para consultar o código fonte enquanto continuava os testes na bancada;
- Divulgar e explicar antecipadamente todos os formulários para que os apoios técnicos se familiarizem com o processo e os procedimentos antes do TPS;
- Caso os formulários permaneçam em papel, disponibilizá-los previamente em uma pasta para cada apoio técnico, evitando a seguinte situação paradoxal: sempre deve haver um apoio técnico acompanhando os investigadores, porém o apoio técnico também precisa se retirar para área reservada para obter os formulários e fazer o registro da solicitação.

5.6 Divulgação e transparência

- Publicar no site do TSE sugestões de investigadores que levaram a ações do TSE para o próximo TPS;
- Promover eventos em universidades do tipo Hackaton ou “mini-TPS” para aproximar alunos das tecnologias de votação desenvolvidas pelo TSE, promovendo disseminação de informações fidedignas, aumentando a confiança e a transparência, além de influenciar positivamente futuros formadores de opinião.

6 Considerações Finais

Os trabalhos realizados envolveram os melhores esforços colaborativos entre as equipes do TSE e do LARC para atuar em três frentes principais no TPS:

- Acompanhamento dos investigadores na execução da maioria dos planos de testes propostos (compondo com representantes dos TREs);
- Gestão das solicitações, conjuntamente com a Comissão Organizadora, feitas pelos investigadores durante o TPS para avaliação da Comissão Reguladora, de forma a obter autorizações para: entrada de materiais no ambiente do TPS, uso de softwares (não previstos inicialmente nos planos de testes), procedimentos envolvendo os equipamentos disponibilizados na bancada (como abertura dos gabinetes das urnas eletrônicas) e informações técnicas sobre os sistemas;
- Observação geral do TPS, acompanhando a execução dos planos de teste, interagindo com investigadores, Apoio Técnico, Comissão Organizadora, Comissão Reguladora e Comissão Avaliadora.

Além disso, a equipe do LARC esteve envolvida na etapa que antecedeu o TPS (denominada Pré-TPS), onde interagiu com os técnicos do TSE e TRE para elaborar e executar testes que ajudaram a identificar oportunidades de melhoria na segurança da urna eletrônica e demais sistemas eleitorais. Todas as contribuições foram registradas em relatórios e discutidas em reuniões com as equipes da Sevin, Setot, Seint, Módulo e JE-Connect.

Com a experiência adquirida pela equipe do LARC ao participar dos TPS 2021 e TPS 2023, espera-se uma integração cada vez maior com a equipe do TSE, com o intuito de aumentar as contribuições para aperfeiçoamento do evento e do sistema de votação eletrônica. De fato, diversas atividades de teste continuam em andamento dentro das dependências da USP, algumas das quais envolvendo conceitos e estratégias similares àquelas observadas no TPS 2021 e TPS 2023.

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Exemplos incluem: exploração de TOCTOU como forma de evadir a cadeia de verificação da urna; exploração de vulnerabilidades conhecidas no Bitlocker; uso de dispositivos externos para captura e eventual manipulação de dados nos canais de comunicação utilizados entre diferentes módulos da urna e do SIS. Desta forma, espera-se que novos achados sejam trazidos ao conhecimento do TSE antes mesmo da próxima edição do TPS. A adoção de mecanismos de segurança adicionais propostos no escopo dos projetos "Teste Público de Segurança – TPS 2023" e "Eleições do Futuro Fase II", em parceria entre USP e TSE, devem ajudar a construir um sistema eleitoral cada vez mais maduro, seguro e transparente.

7.16 Anexo P – Relatório parcial da Comissão Avaliadora

Relatório da Comissão Avaliadora

Primeira Etapa do TPS 2023

Realização: 27 de novembro a 02 de dezembro de 2023

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 701, de 20 de setembro de 2023, tem como atribuição validar a metodologia e os critérios de julgamento definidos no Edital do TPS e avaliar e homologar os resultados obtidos durante o teste. Cabe a ela, ao final, produzir relatório conclusivo contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes porventura identificadas.

A Comissão, composta por 13 membros, contou nesta segunda etapa com a presença dos representantes dos seguintes órgãos:

- TSE - Rogério Marrone de Castro Sampaio - Juiz Auxiliar da Presidência;
- TSE - Paulo Rogério Bonini - Juiz Auxiliar da Presidência;
- Membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:
  - Jamil Salem Barbar - Professor Doutor;
  - Mamede Lima-Marques - Professor Doutor;
  - Osvaldo Catsumi Imamura - Professor Doutor;
  - Antônio Esio Marcondes Salgado - Professor Mestre;
- MPF - Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas;
- CFOAB - Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico;
- CN - Veneziano Vital do Rêgo - Senador da República;
- PF - Paulo César Herrmann Wanner - Perito Criminal Federal e Coordenador da CCAT/CGCIBER/DCIBER/PF;
- TCU - André Luiz Furtado Pacheco - Auditor Federal de Controle Externo;

1

- CONFEA - Rodrigo de Souza Borges - Engenheiro de Computação e Gerente de Tecnologia da Informação;
- SBC - Roberto Samarone dos Santos Araújo - Professor Doutor.

O propósito deste relatório é apresentar os resultados dos testes propostos pelos investigadores e grupos de investigadores.

2 Metodologia de Avaliação dos Testes

Foi mantida a classificação dos resultados dos Planos de Teste como:

- 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 34 planos e os objetos das propostas foram os seguintes:

1. Plano de Teste 01:
   - **Título**: Quebra do sigilo do voto
   - **Investigador(es)**: Aline Barbosa da Silva Ferreira
   - **Resumo do teste**: No dia da Eleição, a votação se inicia normalmente. O primeiro eleitor vota, assim sucessivamente irei retirar da urna eletrônica a mídia de resultados. Ela será lida no Notebook com o kit JE-Connect, assim quebrando o sigilo do voto do eleitor.
2. Plano de Teste 02:
   - **Título**: Fragilizar sigilo do voto
   - **Investigador(es)**: Aline Barbosa da Silva Ferreira
   - **Resumo do teste**: No dia da Eleição na seção de votação, irei instalar um dispositivo na urna eletrônica em que ao eleitor pressionar as teclas do seu voto, o dispositivo emitira o som de qual tecla foi acionada.
3. Plano de Teste 03:
   - **Título**: Invadir a mídia de carga da urna eletrônica
   - **Investigador(es)**: Aline Barbosa da Silva Ferreira

- **Resumo do teste**: Invadir a mídia de carga da Urna Eletrônica, fazendo a limitação de votos aos candidatos daquela seção.

4. Plano de Teste 04:
   - **Título**: Inconsistência de Software
   - **Investigador(es)**: Ariel Rossetto Ril, Daniel Dalalana Bertoglio
   - **Resumo do teste**: Executar a avaliação de que o software que foi salvo na urna eletrônica é o mesmo software lacrado em cerimônia pública.
5. Plano de Teste 05:
   - **Título**: Sigilo e proteção do voto: Fortaleza magnética e defesa eletroacústica para a democracia
   - **Investigador(es)**: Diego Ferry Torrent
   - **Resumo do teste**: Resiliência cibernética abordando magnetismo, acústica, ultrassom e escudo faraday saltando a segurança Air-Gapped.
6. Plano de Teste 06:
   - **Título**: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
   - **Investigador(es)**: André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho
   - **Resumo do teste**: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.
7. Plano de Teste 07:
   - **Título**: Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia
   - **Investigador(es)**: Érika Maria Rodrigues de Castro
   - **Resumo do teste**: Trata-se de análise do comportamento da Mídia de Resultado "pen drive" da Urna Eletrônica em algumas etapas.
8. Plano de Teste 08:
   - **Título**: *Fraus omnia corrumpit*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**: Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do eleitor e com isso alterar a disposição dos votos.

9. Plano de Teste 09:
   - **Título**: *Nihil autem absconditum est, quod non reveletur*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**: 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 habilitados violar o sigilo do voto.
10. Plano de Teste 10:
   - **Título**: *Qui duplicat, videre suffragio potest*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**: Violar sigilo do voto, a partir da sequência de votantes e do conteúdo obtido do *display* do terminal de eleitor com acoplamento de um *Splitter* na saída de vídeo e outro display.
11. Plano de Teste 11:
   - **Título**: *Suffragium simulata substantiam veritas mutare possunt*
   - **Investigador(es)**: Guilherme Henrique dos Santos
   - **Resumo do teste**: Alterar a destinação dos votos, substituindo a votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.
12. Plano de Teste 12:
   - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações no *Python* do Software JE-Connect
   - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
   - **Resumo do teste**: A linguagem de programação *Python* apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo *Python* usa a função str.format e string-f na formatação de *string*. Essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.
13. Plano de Teste 13:
   - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do *Python* para geração de arquivos XML no Software JE-Connect
   - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva; Ian Martinez Zimmermann; Matheus Vianna Silveira; Mario de Araújo Carvalho

- **Resumo do teste**: Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, onde um invasor pode abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas ou contornar firewalls.

14. Plano de Teste 14:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JE-Connect
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: 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.
15. Plano de Teste 15:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JE-Connect
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Executar 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__".
16. Plano de Teste 16:
    - **Título**: 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
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Executar vários *exploits* funcionais para permitir chamadas de: comandos e funções as bibliotecas nativas e externas do Python, e obter acesso as informações.
17. Plano de Teste 17:
    - **Título**: Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita

- **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araujo Carvalho
- **Resumo do teste**: Executar vários *exploits* funcionais para permitir chamadas de: comandos e obter acesso às informações, com escalada de privilégio.

18. Plano de Teste 18:
    - **Título**: 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(es)**: Prof. Dr. João Benedito dos Santos Junior
    - **Resumo do teste**: Este Plano de Teste está inserido no contexto da verificação de integridade e autenticidade de sistemas eleitorais. Pretende-se, em tempo real, extrair, verificar e validar o conjunto completo dos resumos criptográficos HASH SHA-512 *Radix* 64 dos códigos compilados e/ou executáveis que estiverem embarcados na Urna Eletrônica, considerando um cenário em que seja necessário verificar a integridade e autenticidade após os procedimentos de certificação e liberação das Urnas Eletrônicas para o Pleito Eleitoral.
19. Plano de Teste 19:
    - **Título**: Auditoria de Integridade e Segurança na Apuração Eletrônica de Votos
    - **Investigador(es)**: João Vitor Santana Silva
    - **Resumo do teste**: Teste verifica integridade da apuração de votos para garantir resultados eleitorais confiáveis.
20. Plano de Teste 20:
    - **Título**: Tentativa de *Man-in-the-Middle* na Comunicação do Teclado com Arduíno
    - **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
    - **Resumo do teste**: A avaliação tem como propósito testar vulnerabilidades na comunicação entre o teclado e a placa mãe das urnas.
21. Plano de Teste 21:
    - **Título**: Tentativa de reconhecimento das teclas digitadas usando IA
    - **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves

- **Resumo do teste**: O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identificar as teclas usando um modelo de rede neural, quebrando o sigilo dos votos.

22. Plano de Teste 22:
    - **Título**: USBExploit – acesso a dados da urna através da porta USB
    - **Investigador(es)**: Marcos Roberto dos Santos, Rafael Noll da Silva Eduardo Bido, Rhayara Rodrigues Fiorentin
    - **Resumo do teste**: Captura de informações da urna através da conexão de um cabo console ou adaptador USB que possibilite acesso a dados.
23. Plano de Teste 23:
    - **Título**: Executar código espúrio na Urna Eletrônica modelo 2020
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
24. Plano de Teste 24:
    - **Título**: Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020
    - **Investigador(es)**: Galileu Batista de Sousa
    - **Resumo do teste**: Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
25. Plano de Teste 25:
    - **Título**: Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Caso seja possível extrair a chave que cifra/decifra o kernel da urna, uma chave derivada dessa poderá ser utilizada para cifrar um RDV falso. Posteriormente esse RDV falso poderia ser carregado em uma urna de contingência.
26. Plano de Teste 26:
    - **Título**: Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI

- **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- **Resumo do teste**: Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.

27. Plano de Teste 27:
    - **Título**: Alterar dados / programas nos sistemas SIS/GEDAI
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: 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.
28. Plano de Teste 28:
    - **Título**: Ataque de *cold boot* à Urna Eletrônica
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**: Congelamento da memória RAM da urna, objetivando extrair os dados em leitor externo para posterior decodificação.
29. Plano de Teste 29:
    - **Título**: Execução do JE-Connect utilizando computador com sistema operacional inválido
    - **Investigador(es)**: Nicholas Barros dos Santos
    - **Resumo do teste**: Analisar a eficácia da execução do JE-Connect em computadores que apresentam falhas na validação do sistema operacional.
30. Plano de Teste 30:
    - **Título**: Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados
    - **Investigador(es)**: Nicholas Barros dos Santos
    - **Resumo do teste**: Analisar o comportamento do JE-Connect em um computador na execução de um *bot*, para atestar a sua integralidade na transmissão de dados.
31. Plano de Teste 31:
    - **Título**: Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de *shell* a partir de um dispositivo USB

- **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili; Brayan Vanz de Oliveira
- **Resumo do teste**: Abertura de um *shell* no sistema operacional responsável pela comunicação JE-Connect para obter acesso a rede do TSE.

32. Plano de Teste 32:
    - **Título**: Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores
    - **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili; Brayan Vanz de Oliveira
    - **Resumo do teste**: Abrir a Urna e substituir o cabo HDMI para outro cabo que possua um dispositivo, o qual remeta a imagem para outro dispositivos conectados via Bluetooth.
33. Plano de Teste 33:
    - **Título**: Investigação dos mecanismos de validação do *bootloader* pela BIOS para a proteção da carga segura do SO da UE
    - **Investigador(es)**: Ricardo Antônio Pralon Santos
    - **Resumo do teste**: Investigação dos meios de proteção do *bootloader* da UE e a possibilidade de substituição por um *bootloader* "malicioso".
34. Plano de Teste 34:
    - **Título**: Adulteração no JE-Connect
    - **Investigador(es)**: Vitor Aloisio do Nascimento Guia, Hitatiana Maria Santiago Ferreira da Silva Guia
    - **Resumo do teste**: Garantir que não seja possível obter privilégios de usuário root na *distro* Linux do MSE de forma a adulterar o JEC.
35. Plano de Teste 35*[1]:
    - **Título**: Teste de escalação de privilégios no Windows (SIS)
    - **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
    - **Resumo do teste**: Utilizar falha de permissão para escalar privilégio e acesso a arquivos críticos.

[1] *Planos de Teste Adicionais solicitados no transcorrer do TPS (35 a 38)

36. Plano de Teste 36*:
    - **Título**: *Ab initio in valid post valid*
    - **Investigador(es)**: Guilherme Henrique dos Santos
    - **Resumo do teste**: Alterar a tabela de correspondência.
37. Plano de Teste 37*:
    - **Título**: *Omnia invalid est*
    - **Investigador(es)**: Guilherme Henrique dos Santos
    - **Resumo do teste**: Usar o SA como validador de um BU com votos inválidos.
38. Plano de Teste 38*:
    - **Título**: *Suffragium non est relatus*
    - **Investigador(es)**: Guilherme Henrique dos Santos
    - **Resumo do teste**: Descarte de votos mediante substituição por um período de tempo da MV (Mídia de Votação) por uma MV clonada.

4 Planos de Teste Executados

Para tornar os trabalhos de avaliação consistentes com o andamento das investigações e com os registros efetuados pela Equipe de Apoio Técnico do TPS 2023, constituída para acompanhar as atividades, registra-se a seguir os planos efetivamente executados pelos 16 grupos formados durante os testes.

1. Grupo 1:
    - **Título(s)**: Quebra do sigilo do voto; fragilizar sigilo do voto; invadir a mídia de carga da urna eletrônica
    - **Investigador(es)**: Aline Barbosa da Silva Ferreira
    - **Resumo do teste**:
        1. No dia da Eleição, a votação se inicia normalmente. O primeiro eleitor vota, assim sucessivamente irei retirar da urna eletrônica a mídia de resultados. Ela será lida no Notebook com o kit JE-Connect, assim quebrando o sigilo do voto do eleitor.
        2. No dia da Eleição na seção de votação, irei instalar um dispositivo na urna eletrônica em que ao eleitor pressionar as teclas do seu voto, o dispositivo emitira o som de qual tecla foi acionada.

3. Invadir a mídia de carga da Urna Eletrônica, fazendo a limitação de votos aos candidatos daquela seção.

– **Plano de Teste Proposto**: 1, 2 e 3.

2. Grupo 2:

– **Título(s)**: Inconsistência de Software

– **Investigador(es)**: Ariel Rossetto Ril, Daniel Dalalana Bertoglio

– **Resumo do teste**: Executar a avaliação de que o software que salvo na urna eletrônica é o mesmo software lacrado em cerimônia pública.

– **Plano de Teste Proposto**: 4

3. Grupo 3:

– **Título(s)**: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas

– **Investigador(es)**: André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho

– **Resumo do teste**: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.

– **Plano de Teste Proposto**: 6

4. Grupo 4:

– **Título(s)**: Mídia de Resultado: a confiança do cidadão na urna eletrônica e o coração da democracia

– **Investigador(es)**: Érika Maria Rodrigues de Castro

– **Resumo do teste**: Em resumo: trata-se de Trata-se de análise do comportamento da Mídia de Resultado "pen drive" da Urna Eletrônica em algumas etapas

– **Plano de Teste Proposto**: 7

5. Grupo 5:

– **Título(s)**: *Fraus omnia corrumpit; nihil autem absconditum est, quod non reveletur; qui duplicat, videre suffragio potest; suffragium simulata substantiam veritas mutare possunt, Ab initio in valid post valid, Omnia invalid est, Suffragium non est relatus*

– **Investigador(es)**: Guilherme Henrique dos Santos

– **Resumo do teste**:

1. Alterar a disposição indicativa do teclado e emular comportamento da tela, para que os votos não sejam registrados conforme vontade do eleitor e com isso alterar a disposição dos votos.
2. 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 habilitados violar o sigilo do voto.
3. Violar 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.
4. Alterar a destinação dos votos, substituindo a votos oficiais por votos espúrios depositados em urna de contingência, seguindo a votação em outra urna.
5. Alterar a tabela de correspondência.
6. Usar o SA como validador de um BU com votos inválidos.
7. Descarte de votos mediante substituição por um período de tempo da MV (Mídia de Votação) por uma MV clonada.

– **Plano de Teste Proposto**: 8. 9. 10, 11, 36, 37 e 38

6. Grupo 6:

– **Título(s)**: Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações nas bibliotecas do Python para geração de arquivos XML no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações na função urllib.parse do Python no Software JE-Connect; Violar a confidencialidade, integridade e disponibilidade das informações ao executar comandos a partir de scripts em área restrita do Python no Software JE-Connect; 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; Violar a confidencialidade, integridade e disponibilidade das informações do OpenVPN criada pelo KIT JE, possibilitando comandos a partir de scripts em área restrita.

– **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva; Ian Martinez Zimmermann; Matheus Vianna Silveira; Mario de Araujo Carvalho

– **Resumo do teste**:

1. A linguagem de programação Python apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo Python usa a função str.format e string-f na formatação de string. essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.

12

2. Os módulos de processamento XML na linguagem de programação Python não são seguros contra dados construídos de forma maliciosa, onde um invasor pode abusar dos recursos XML para realizar acesso aos arquivos locais, gerar conexões de rede para outras máquinas ou contornar firewalls.
3. 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.
4. Executar 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__".
5. Executar vários *exploits* funcionais para permitir chamadas de: comandos e funções as bibliotecas nativas e externas do Python, e obter acesso as informações.
6. Executar vários *exploits* funcionais para permitir chamadas de: comandos e obter acesso às informações, com escalada de privilégio.

– **Plano de Teste Proposto**: 12, 13, 14, 15, 16, 17 e 35

7. Grupo 7:

– **Título(s)**: 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(es)**: Prof. Dr. João Benedito dos Santos Junior

– **Resumo do teste**: Este Plano de Teste está inserido no contexto da verificação de integridade e autenticidade de sistemas eleitorais. Pretende-se, em tempo real, extrair, verificar e validar o conjunto completo dos resumos criptográficos HASH SHA-512 Radix 64 dos códigos compilados e/ou executáveis que estiverem embarcados na Urna Eletrônica, considerando um cenário em que seja necessário verificar a integridade e autenticidade após os procedimentos de certificação e liberação das Urnas Eletrônicas para o Pleito Eleitoral.

– **Plano de Teste Proposto**: 18

8. Grupo 8:

– **Título(s)**: Tentativa de *Man-in-the-Middle* na Comunicação do Teclado com Arduíno; Tentativa de reconhecimento das teclas digitadas usando IA

13

- **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
- **Resumo do teste**:
  1. A avaliação tem como propósito testar vulnerabilidades na comunicação entre o teclado e a placa mãe das urnas.
  2. O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identifica usando um modelo de rede neural, quebrando o sigilo dos votos.
- **Plano de Teste Proposto**: 20 e 21

9. Grupo 9:
   - **Título(s)**: USBExploit – acesso a dados da urna através da porta USB
   - **Investigador(es)**: Marcos Roberto dos Santos; Eduardo Bido; Rhayra Rodrigues Fiorentin; Rafael Nollda Silva
   - **Resumo do teste**:

     Captura de informações da urna através da conexão de um cabo console ou adaptador USB que possibilite acesso a dados
   - **Plano de Teste Proposto**: 22
10. Grupo 10:
    - **Título(s)**: Executar código espúrio na Urna Eletrônica modelo 2020; Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020; Utilizar a chave que cifra/decifra o kernel da urna para alterar o Registro Digital de Voto; Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI; Alterar dados / programas nos sistemas SIS/GEDAI; Ataque de cold boot à Urna Eletrônica
    - **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
    - **Resumo do teste**:
      1. Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
      2. Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.

3. Caso seja possível extrair a chave que cifra/decifra o kernel da urna, uma chave derivada dessa poderá ser utilizada para cifrar um RDV falso. Posteriormente esse RDV falso poderia ser carregado em uma urna de contingência.
4. Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.
5. 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.
6. Congelamento da memória RAM da urna, objetivando extrair os dados em leitor externo para posterior decodificação.

– **Plano de Teste Proposto**: 23, 24, 25, 26, 27 e 28

11. Grupo 11:
    – **Título(s)**: Execução do JE-Connect utilizando computador com sistema operacional inválido; Comportamento do JE-Connect na execução de um *bot* de monitoramento no computador transmissor de dados
    – **Investigador(es)**: Nicholas Barros dos Santos
    – **Resumo do teste**:
        1. Analisar a eficácia da execução do JE-Connect em computadores que apresentam falhas na validação do sistema operacional.
        2. Analisar o comportamento do JE-Connect em um computador na execução de um *bot*, para atestar a sua integralidade na transmissão de dados.
    – **Plano de Teste Proposto**: 29 e 30
12. Grupo 12:
    – **Título(s)**: Acesso a rede do TSE por intermédio do software JE-Connect realizando a execução de *shell* a partir de um dispositivo USB; Captura do Vídeo transmitido no display, com a alteração dos cabos transmissores
    – **Investigador(es)**: Rafael Basso Reis, Stefano Augusto Mossi, Gabriel Viecili, Brayan Vanz de Oliveira
    – **Resumo do teste**: 1) Abertura de um *shell* no sistema operacional responsável pela comunicação JE-Connect para obter acesso a rede do TSE. 2) Abrir a Urna e substituir o cabo HDMI para outro cabo que possua um dispositivo, o qual remeta a imagem para outro dispositivos conectados via Bluetooth.
    – **Plano de Teste Proposto**: 31 e 32

13. Grupo 13:
    - **Título(s)**: Adulteração no JE-Connect
    - **Investigador(es)**: Vitor Aloisio do Nascimento Guia, Hitatiana Maria Santiago Ferreira da Silva Guia
    - **Resumo do teste**: Garantir que não seja possível obter privilégios de usuário root na *distro* Linux do MSE de forma a adulterar o JEC
    - **Plano de Teste Proposto**: 34
    - Os investigadores proponentes dos testes 05, 19 e 33 não compareceram 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 não executados

Os planos de testes não executados foram: 25, 27 e 28.

5.2 Planos de teste executados sem contribuições

Os planos de teste executados que não obtiveram sucesso no alcance dos objetivos propostos foram: 01, 02, 03, 07, 08, 09, 10, 11, 13, 14, 15, 16, 17, 18, 20, 22, 29, 30, 31, 32, 34, 36, 37 e 38. O plano de teste 04 foi executado e confirmou que o software instalado na urna é o mesmo que foi assinado e lacrado.

Avaliação: As propostas de testes apresentadas encontraram barreiras e proteções que dificultaram o alcance dos objetivos planejados. Todavia, muitos investigadores compareceram com conhecimento e informações insuficientes, necessitando de muito tempo para conseguirem reanalisar os planos de testes e validar os procedimentos planejados, ou buscar alternativas.

5.3 Planos de teste executados com contribuição

Os planos de teste que apresentaram resultados de avanço nos objetivos propostos foram: 06, 12, 21, 23, 24, 26 e 35.

Plano de Teste 06:

- **Título**: Teste de capacidade do teclado da Urna Eletrônica em receber múltiplas entradas simultâneas
- **Investigador(es)**: André Mário dos Reis dos Santos, Alexandre Zago Boava, Diego Vergaças de Sousa Carvalho
- **Resumo do teste**: Teste no teclado da urna para averiguar se a tela e o voto computado estão de acordo com o que é digitado pelo eleitor.
- **Resultado obtido**: O MSTE, Módulo de Segurança do Teclado do Eleitor, não registra os comandos das teclas quando duas teclas são acionadas simultaneamente. Todavia, o acionamento de uma terceira tecla é aceito.

Avaliação: A observação informada não afeta a condução do voto pelo eleitor. Todavia, o conceito de múltiplas teclas estar limitada a somente duas pode ser revisto.

Plano de Teste 12:

- **Título**: Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JE-Connect
- **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
- **Resumo do teste**: A linguagem de programação Python apresenta uma vulnerabilidade na função Str.str.format(), a vulnerabilidade surge quando o aplicativo Python usa a função str.format e string-f na formatação de *string*. Essas vulnerabilidades podem fazer com que os invasores tenham acesso a informações confidenciais, ou inserir um código executável nesta.
- **Resultado obtido**: Foi verificado que o sistema JE-Connect realiza o reboot a cada três tentativas de erros de login. Todavia, a reinicialização é invocada de forma simples, permitindo que o usuário a interrompa e retorne à situação de solicitação de login e com o contador de tentativas zerado. Esta ação permite que novas tentativas possam ser realizadas, praticamente sem o limite estabelecido pelo sistema.

Avaliação: 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.

Plano de Teste 21:

- **Título**: Tentativa de reconhecimento das teclas digitadas usando IA
- **Investigador(es)**: Luis Antonio Brasil Kowada, Gabriel Cardoso de Carvalho, Caubi de Souza Loureiro Rosa, Camila Ferreira Alves
- **Resumo do teste**: O teste consiste em capturar o som das teclas digitadas numa urna eletrônica e identificar as teclas usando um modelo de rede neural, quebrando o sigilo dos votos.
- **Resultado obtido**: Foi obtido uma acurácia de 70% no reconhecimento do acionamento de uma tecla por meio da captação do som emitido pela urna e capturado usando um microfone para um mesmo modelo de urna. A acurácia média diminui para 50% considerando diferentes modelos de urna e posições variadas do microfone. Os resultados obtidos podem ser melhorados com o aprimoramento do algoritmo e uso de recursos computacionais emergentes.

Avaliação: O teste pode ser considerado uma contribuição para o aprimoramento dos componentes da urna eletrônica, na fase de desenvolvimento. O seu emprego em uma seção eleitoral é impraticável dadas as condições que este ambiente apresenta, tais como ruídos, para a captura dos sinais necessários e processamento da informação.

Plano de Teste 23:

- **Título**: Executar código espúrio na Urna Eletrônica modelo 2020
- **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- **Resumo do teste**: Utilizar um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.
- **Resultado obtido**: Foi verificado a existência de uma falha no BIOS da urna permitindo a abertura de uma janela de oportunidade para alteração de informação durante a execução do *bootloader*. A verificação da falha foi executada com a carga de uma mensagem não prevista exibida na tela da urna durante a inicialização.

Avaliação: 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.

Plano de Teste 24:

- **Título**: Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020
- **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- **Resumo do teste**: Caso o primeiro plano de testes obtenha sucesso, tentar extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.
- **Resultado obtido**: Foi explorado um comportamento não previsto nos procedimentos de carga controlados pelo BIOS/UEFI e *bootloader*, permitindo a geração de chave para decifração de um bloco do kernel do sistema operacional da urna carregado durante a inicialização.

Avaliação: 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.

Plano de Teste 26:

- **Título**: Recuperar a chave de criptografia do *Bitlocker* utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI
- **Investigador(es)**: Galileu Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida, João Vitor de Sá Hauck
- **Resumo do teste**: Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo *Bitlocker* para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.
- **Resultado obtido**: Foi obtido as chaves que protegem a partição protegida pelo *Bitlocker* (sistema de proteção nativa do Windows) e ter acesso à área onde ficam residentes o SIS e os sistemas eleitorais a serem carregados na urna.

Avaliação: 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.

Plano de Teste 35*:

- **Título**: Teste de escalação de privilégios no Windows (SIS)

- **Investigador(es)**: Prof. Dr. Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira, Mario de Araújo Carvalho
- **Resumo do teste**: Utilizar falha de permissão para escalar privilégio e acesso a arquivos críticos.
- **Resultado obtido**: Por meio de um acesso a uma conta com baixos privilégios no SIS, foi possível localizar um *endpoint* na aplicação VAP, Verificador de Autenticação de Programas, que permite a elevação de privilégios de leitura e escrita possibilitando o acesso e a edição de arquivos internos do sistema.

Avaliação: 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.

5.4 Considerações sobre as observações realizadas pela Comissão de Avaliação

O TPS 2023 apresentou um cenário mais abrangente que os demais eventos anteriores, em especial pela maior abrangência dos cenários de testes.

A complexidade dos sistemas e dos processos eleitorais foi constatada pela dificuldade que muitos investigadores tiveram em se situar e dominar os seus cenários de testes.

Os resultados alcançados também refletem esta complexidade sistêmica, mas conseguindo demonstrar algumas fragilidades em contextos mais específicos, mas relevantes.

Consequentemente, ainda que esses resultados alcançados pelos investigadores não comprometam a integridade, o sigilo do voto e o resultado das eleições, os riscos associados podem obstruir a boa e natural execução da eleição e merecem ser analisados, os riscos devidamente identificados e os processos consistentes com as evidências apresentadas.

A Comissão avaliadora recomenda que os investigadores dos seguintes testes sejam convidados para uma nova verificação dos achados e das soluções propostas: 12, 23, 24, 26 e 35.

7.17 Anexo Q – Lista de presença – Teste de Confirmação

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023 (Teste de Confirmação)

TESTE DA URNA

Dia 15/05

	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Carlos Alberto da Silva	G-4		
2	Ian Martinez Zimmermann	G-4		
3	Mário de Araújo Carvalho	G-4		
4	Matheus Vianna Silveira	G-4		
5	Breno Rangel Borges Marchetti	G-5		
6	Galileu Batista de Sousa	G-5		
7	João Paulo Vieira Almeida	G-5		
8	João Vitor de Sá Hauck	G-5		
9	Maria Isabel Vasconcelos Lima	G-5		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023 (Teste de Confirmação)

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 16/05				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Carlos Alberto da Silva	G-4		
2	Ian Martinez Zimmermann	G-4		
3	Mário de Araújo Carvalho	G-4		
4	Matheus Vianna Silveira	G-4		
5	Breno Rangel Borges Marchetti	G-5		
6	Galileu Batista de Sousa	G-5		
7	João Paulo Vieira Almeida	G-5		
8	João Vitor de Sá Hauck	G-5		
9	Maria Isabel Vasconcelos Lima	G-5		

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Lista de Presença
TPS 2023 (Teste de Confirmação)

TESTE PÚBLICO DE SEGURANÇA DA URNA

Dia 17/05				
	Nome do(a) Investigador(a)	Identificação	Assinatura (Manhã)	Assinatura (Tarde)
1	Carlos Alberto da Silva	G-4		
2	Ian Martinez Zimmermann	G-4		
3	Mário de Araújo Carvalho	G-4		
4	Matheus Vianna Silveira	G-4		
5	Breno Rangel Borges Marchetti	G-5		
6	Galileu Batista de Sousa	G-5		
7	João Paulo Vieira Almeida	G-5		
8	João Vitor de Sá Hauck	G-5		
9	Maria Isabel Vasconcelos Lima	G-5		

7.18 Anexo R – Termos de confirmação

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Termo de Confirmação
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Termo de Confirmação

Plano de Teste: Escalação de privilégio no Windows (SIS)

Equipe de Investigadores Grupo – G4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho

Considerando o disposto no §6º do art. 37, do EDITAL nº 1/2023, DO TESTE PÚBLICO DE SEGURANÇA DA URNA – TPS 2023, uma vez realizados os novos testes, confirmamos que a(s) falha(s) e/ou vulnerabilidade(s) encontrada(s) no decorrer da execução do plano de teste, acima descrito, foi/foram saneada(s) pela equipe técnica do TSE, nada restando a ser considerado pelos investigadores subscritos abaixo, em relação ao referido plano.

Brasília, 17 de maio de 2024.

Carlos Alberto da Silva

Ian Martinez Zimmermann

Matheus Vianna Silveira

Mário Araújo Carvalho

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600 – Tel.: (61) 3030-7000

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Termo de Confirmação
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Termo de Confirmação

Plano de Teste: Violar a confidencialidade, integridade e disponibilidade das informações no Python do *Software* JE-Connect

Equipe de Investigadores Grupo – G4	Carlos Alberto da Silva Ian Martinez Zimmermann Matheus Vianna Silveira Mário de Araújo Carvalho

Considerando o disposto no § 6º do art. 37, do EDITAL nº 1/2023, DO TESTE PÚBLICO DE SEGURANÇA DA URNA – TPS 2023, uma vez realizados os novos testes, confirmamos que a(s) falha(s) e/ou vulnerabilidade(s) encontrada(s) no decorrer da execução do plano de teste, acima descrito, foi/foram saneada(s) pela equipe técnica do TSE, nada restando a ser considerado pelos investigadores subscritos abaixo, em relação ao referido plano.

Brasília, 17 de maio de 2024.

Carlos Alberto da Silva

Ian Martinez Zimmermann

Matheus Vianna Silveira

Mário Araújo Carvalho

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600 – Tel.: (61) 3030-7000

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Termo de Confirmação
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Termo de Confirmação

Plano de Teste: Executar código espúrio na Urna Eletrônica modelo 2020

Equipe de Investigadores Grupo – G5	Breno Rangel Borges Marchetti Galileu Batista de Sousa João Paulo Vieira Almeida João Vitor de Sá Hauck Maria Isabel Vasconcelos Lima

Considerando o disposto no §6º do art. 37, do EDITAL nº 1/2023, DO TESTE PÚBLICO DE SEGURANÇA DA URNA – TPS 2023, uma vez realizados os novos testes, confirmamos que a(s) falha(s) e/ou vulnerabilidade(s) encontrada(s) no decorrer da execução do plano de teste, acima descrito, foi/foram saneada(s) pela equipe técnica do TSE, nada restando, portanto, a ser considerado pela investigadora e pelos investigadores subscritos abaixo:

Brasília, 17 de maio de 2024.

Breno Rangel Borges Marchetti

Galileu Batista de Sousa

João Paulo Vieira Almeida

João Vitor de Sá Hauck

Maria Isabel Vasconcelos Lima

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600 – Tel.: (61) 3030-7000

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Termo de Confirmação
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Termo de Confirmação

Plano de Teste: Extrair a chave que cifra-decifra o kernel da Urna Eletrônica modelo 2020

Equipe de Investigadores Grupo – G5	Breno Rangel Borges Marchetti Galileu Batista de Sousa João Paulo Vieira Almeida João Vitor de Sá Hauck Maria Isabel Vasconcelos Lima

Considerando o disposto no §6º do art. 37, do EDITAL nº 1/2023, DO TESTE PÚBLICO DE SEGURANÇA DA URNA – TPS 2023, uma vez realizados os novos testes, confirmamos que a(s) falha(s) e/ou vulnerabilidade(s) encontrada(s) no decorrer da execução do plano de teste, acima descrito, foi/foram saneada(s) pela equipe técnica do TSE, nada restando, portanto, a ser considerado pela investigadora e pelos investigadores subscritos abaixo:

Brasília, 17 de maio de 2024.

Breno Rangel Borges Marchetti

Galileu Batista de Sousa

João Paulo Vieira Almeida

João Vitor de Sá Hauck

Maria Isabel Vasconcelos Lima

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600 – Tel.: (61) 3030-7000

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação
TSE

Termo de Confirmação
TPS 2023

TESTE PÚBLICO DE SEGURANÇA DA URNA

Termo de Confirmação

Plano de Teste: Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS-GEDAI

Equipe de Investigadores Grupo – G5	Breno Rangel Borges Marchetti Galileu Batista de Sousa João Paulo Vieira Almeida João Vitor de Sá Hauck Maria Isabel Vasconcelos Lima

Considerando o disposto no §6º do art. 37, do EDITAL nº 1/2023, DO TESTE PÚBLICO DE SEGURANÇA DA URNA – TPS 2023, uma vez realizados os novos testes, confirmamos que a(s) falha(s) e/ou vulnerabilidade(s) encontrada(s) no decorrer da execução do plano de teste, acima descrito, foi/foram mitigada(s) pela equipe técnica do TSE, nada restando, portanto, a ser considerado pela investigadora e pelos investigadores subscritos abaixo:

Brasília, 17 de maio de 2024.

Breno Rangel Borges Marchetti

Galileu Batista de Sousa

João Paulo Vieira Almeida

João Vitor de Sá Hauck

Maria Isabel Vasconcelos Lima

Tribunal Superior Eleitoral
Setor de Administração Federal Sul (SAFS), Quadra 7, Lotes 1/2, Brasília/DF – CEP: 70070-600 – Tel.: (61) 3030-7000

7.19 Anexo S – Relatório final da Comissão Avaliadora

Relatório Final da Comissão Avaliadora

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 701, de 06 de setembro de 2023, alterada pela TSE nº 950, de 4 de dezembro de 2023, tem como atribuição validar a metodologia e os critérios de julgamento definidos no Edital do TPS e avaliar e homologar os resultados obtidos durante o teste. Cabe a ela, ao final, produzir relatório conclusivo contendo as ponderações quanto à aplicabilidade das possíveis falhas, às vulnerabilidades exploradas ou às fraudes porventura identificadas.

A Comissão, composta por 13 membros, contou nesta segunda etapa com a presença dos representantes dos seguintes órgãos:

- TSE - Rogério Marrone de Castro Sampaio - Juiz Auxiliar da Presidência;
- TSE - Paulo Rogério Bonini - Juiz Auxiliar da Presidência;
- Membros da comunidade acadêmica ou científica de notório saber na área de Segurança da Informação:
- Jamil Salem Barbar - Professor Doutor;
- Mamede Lima-Marques - Professor Doutor;
- Osvaldo Catsumi Imamura - Professor Doutor;
- Antônio Esio Marcondes Salgado - Professor Mestre;
- MPF - Renato Costa Salomão - Analista do MPU/Desenvolvimento de Sistemas;
- CFOAB - Watson Odilon Pereira de Faria - Supervisor do Processo Eletrônico;
- CN - Veneziano Vital do Rêgo - Senador da República;
- PF - Paulo César Herrmann Wanner - Perito Criminal Federal e Coordenador da CCAT/CGCIBER/DCIBER/PF;
- TCU - André Luiz Furtado Pacheco - Auditor Federal de Controle Externo;
- CONFEA - Rodrigo de Souza Borges - Engenheiro de Computação e Gerente de Tecnologia da Informação;
- SBC - Roberto Samarone dos Santos Araújo - Professor Doutor.

Obs: O Sr. Paulo César Herrmann Wanner foi substituído pelo Sr. Flavio Silveira da Silva e o Sr. Rodrigo de Souza Borges foi substituído pelo Sr. Fernando Batista da Silva, conforme a Portaria TSE nº397 de 03 de junho de 2024.

O propósito deste relatório é apresentar os resultados dos testes de confirmação dos investigadores e grupos de investigadores

1

2 Resultados do Teste de Confirmação

Nos dias 15, 16 e 17 de maio de 2024 foi realizada, no Tribunal Superior Eleitoral, a etapa Teste de Confirmação referente ao TPS 2023[1]. Tal etapa consiste em "reprodução, pelo investigador ou grupo de investigadores, do teste realizado durante o TPS, no qual foi identificada falha, vulnerabilidade explorada ou fraude, em uma nova versão ou revisão do sistema eleitoral, com as devidas correções, com o intuito de avaliar a melhoria implementada".

De acordo com a Seção 5.4 do Relatório da Comissão Avaliadora referente à 1a etapa do TPS 2023[2], estiveram presentes, nesta etapa, os grupos responsáveis pelos Planos de Teste: 12, 23, 24, 26 e 35.

2.1 Plano de Teste 12 [Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JE-Connect]:

Dos achados e da avaliação desta comissão em novembro/2023: Os investigadores identificaram uma vulnerabilidade na função Str.str.format() da linguagem de programação Python. Esta vulnerabilidade é ativada quando um aplicativo Python utiliza a função str.format e string-f para formatar strings. Tais vulnerabilidades podem permitir que invasores acessem informações confidenciais ou insiram um código executável.

Além disso, observou-se que o sistema JE-Connect executa uma reinicialização após três tentativas de login mal-sucedidas. No entanto, o processo de reinicialização é simples, permitindo que o usuário o interrompa e retorne ao estado de solicitação de login, com o contador de tentativas redefinido para zero. Essa ação possibilita a realização de novas tentativas, praticamente sem o limite imposto pelo sistema.

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.

Adequações realizadas pelo TSE: O código foi alterado para que o JE-Connect encerre a seção ao atingir o limite de tentativas de login.

[1] Edital do Teste Público de Segurança - TPS 2023, disponível em https://www.justicaeleitoral.jus.br/tps/arquivos/2023/edital/edital-2023.pdf e https://www.justicaeleitoral.jus.br/tps/arquivos/2023/edital/edital-2-2023.pdf

[2] https://www.justicaeleitoral.jus.br/tps/arquivos/2023/documentos/relatorio-da-comissao-avaliadora-2023primeira-etapa-TPS-2023-v2.pdf

Teste de confirmação: A etapa de login do JE-Connect considera qualquer tecla pressionada como tentativa de login, desconectando após atingir o limite estabelecido.

Avaliação do teste de confirmação: Considerou-se que as alterações realizadas foram efetivas.

2.2 Plano de Teste 23 [Executar código espúrio na Urna Eletrônica modelo 2020]:

Dos achados e da avaliação desta comissão em novembro/2023: Utilizou-se um equipamento para simular uma mídia de carga e executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use* ou "Tempo de Verificação, Tempo de Utilização"), alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.

Foi verificada a existência de uma falha no BIOS da urna permitindo a abertura de uma janela de oportunidade para alteração de informação durante a execução do *bootloader*. A verificação da falha foi executada com a carga de uma mensagem não prevista exibida na tela da urna durante a inicialização.

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.

Adequações realizadas pelo TSE: Correção no BIOS e no código do *bootloader* para verificar qualquer inserção de código não previsto.

Teste de confirmação: Não foi possível repetir o ataque com inserção de código externo.

Avaliação do teste de confirmação: Este ataque permitiu a identificação de falhas no BIOS e no *bootloader* consideradas de alto risco.

2.3 Plano de Teste 24 [Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020]:

Dos achados e da avaliação desta comissão em novembro/2023: Com o sucesso do primeiro plano de testes, foi possível extrair a chave que cifra/decifra o kernel da urna modelo 2020 a partir da execução de código arbitrário.

Foi explorado um comportamento não previsto nos procedimentos de carga controlados pelo BIOS/UEFI e bootloader, permitindo a geração de chave para decifração de um bloco do kernel do sistema operacional da urna carregado durante a inicialização.

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.

Adequações realizadas pelo TSE: Correção no BIOS e no código do bootloader para que verifique qualquer inserção de código não previsto.

Teste de confirmação: Não foi possível repetir o ataque com inserção de código externo.

Avaliação do teste de confirmação: O impedimento de execução de códigos não previstos impede a extração de informações da urna.

2.4 Plano de Teste 26 [: Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI]:

Dos achados e da avaliação desta comissão em novembro/2023: Utilizar técnicas avançadas para recuperar a chave guardada no TPM utilizada pelo Bitlocker para cifrar o disco da máquina onde roda os softwares SIS/GEDAI.

Foi obtido as chaves que protegem a partição protegida pelo Bitlocker (sistema de proteção nativa do Windows) e ter acesso à área onde ficam residentes o SIS e os sistemas eleitorais a serem carregados na urna.

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.

Adequações realizadas pelo TSE: Reconfiguração do BIOS para proteger a chave do Bitlocker.

Teste de confirmação: Com a reconfiguração do BIOS não foi mais possível recuperar as chaves que protegem a partição protegida pelo Bitlocker, exigindo uma chave de recuperação para reativar o computador.

Avaliação do teste de confirmação: A reconfiguração no BIOS não impede que ataques como este sejam realizados, mas reduz consideravelmente as possibilidades. Novas possibilidades de proteção devem ser exploradas no futuro.

2.5 Plano de Teste 35 [Teste de escalação de privilégios no Windows (SIS)]:

Dos achados e da avaliação desta comissão em novembro/2023: Utilizar falha de permissão para escalar privilégio e acesso a arquivos críticos.

Por meio de um acesso a uma conta com baixos privilégios no SIS, foi possível localizar um *endpoint* na aplicação VAP, Verificador de Autenticação de Programas, que permite a elevação de privilégios de leitura e escrita possibilitando o acesso e a edição de arquivos internos do sistema.

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.

Adequações realizadas pelo TSE: Realização de um ajuste nos privilégios das aplicações mais críticas.

Teste de confirmação: Não foi possível utilizar determinadas aplicações para escalar privilégios no sistema de arquivos.

Avaliação do teste de confirmação: Apesar do problema estar corrigido, seria recomendável verificar todos os códigos para poder atribuir privilégios necessários para a sua correta execução, mas sem gerar aberturas indesejáveis para futuras vulnerabilidades.

3 Comentários sobre recomendações dos TPS anteriores

3.1 Relativo ao modelo distribuído de conexão à rede da JE para envio dos dados de apuração da UE

Recomendação:

Uso de token criptográfico para armazenamento das chaves privadas usadas pelos agentes remotos. Avaliar se o uso de certificado sob a ICP-Brasil como um elemento de autorização no RecArquivos, caso adotado o modelo centralizado, não seria um fator inibidor de comprometimento de agentes internos, tendo em vista que o registro de quem fez o envio do boletim e RDV adulterados ficaria nos logs - há aqui um ponto de responsabilização que deve ser legalmente analisado. Algumas considerações devem ser observadas:

a) Um dos pontos positivos de uso do certificado ICP-Brasil é que esse modelo facilitaria a logística de distribuição de tokens, já que eles estariam de posse dos agentes externos previamente, para uso em outras atividades rotineiras;

b) Analisar como operacionalizar a homologação dos agentes remotos que terão acesso ao sistema RecArquivos durante o pleito (portal com duplo fator de autenticação com uso de login/senha e um *token* de autenticação?).

Resposta do TSE: Uso de token criptográfico, padrão ICP-Brasil, para armazenamento das chaves privadas usadas pelos agentes remotos

5

Não acolhida

Ainda que represente acréscimo de segurança no processo de transmissão, o uso de tokens criptográficos para conexão não representaria acréscimo real de segurança no processo como um todo. Há que se considerar que o sistema eletrônico de votação brasileiro assegura a integridade e autenticidade dos registros de votos a partir de inteligência localizada em dois pontos: na urna eletrônica e no RecArquivos. Assim, o investimento em tokens criptográficos não resultaria em um retorno-sobre-investimento suficiente que o justificasse, considerando as restrições do Erário. Em verdade, garantida – como de fato é – a segurança da urna e a respectiva inteligência do RecArquivos, qualquer elemento adicional que venha a pressionar o processo de transmissão pode mesmo vir a ser prejudicial. Se a garantia está nas pontas, melhor é facilitar o processo intermediário, torná-lo o mais simples possível, para que seja eficiente e célere. Considere-se, a critério de exemplo, a realidade díspar de várias regiões brasileiras, em que há transmissões de aldeias indígenas, com escassos recursos e dificílimo acesso. Nessas circunstâncias, o eventual bloqueio acidental de um token impediria a conclusão de uma totalização.

Ademais, não há também materialidade que justifique tal investimento financeiro: em 26 anos de eleições informatizadas, com respectivo transporte de arquivos, nunca houve ocorrência de tentativa de envio de BU ou RDV espúrio. Ainda que tivesse havido, mecanismos como as tabelas de correspondências, as verificações sintáticas e semânticas, bem como as verificações de assinaturas de hardware e de software interceptariam tal arquivo prontamente.

Considerações da Comissão: Em se tratando da urna eletrônica e os dados gerados, o processo atual está em nível de confiabilidade alta. Todavia, há outros processos no ambiente eleitoral que podem ter a sua segurança aprimorada e o uso de uma credencial com maior confiabilidade seria mais adequado.

3.2 Busca por novas abordagens para os desafios do Processo Eleitoral

Recomendação:

Considerando a evolução tecnológica, tanto em termo de infraestrutura quanto de plataformas/sistemas/algoritmos, sugere-se ao TSE avaliar possibilidade de promover ou participar de eventos como *hackathon* ou DEFCON, para a busca de novas abordagens aos problemas e desafios existentes no processo eleitoral, tais como modelos de detecção de anomalias, disponibilização dos dados de apuração de modo íntegro e auditável a todas as pessoas e entidades que tenham interesse. Visando reunir equipes excepcionais, além da premiação àqueles que obtiverem sucesso em identificar ou causar anomalias no processo eleitoral, sugere-se a criação de um prêmio por excepcionalidade da solução proposta, que é dado de forma discricionária, sem caráter obrigatório. A solução que foi objeto desta premiação deve ter ampla publicidade, com justificativas para embasamento de sua concessão.

Resposta do TSE:

Promover eventos (como *hackaton*) com premiação àqueles que obtiverem sucesso em identificar ou causar anomalias no processo eleitoral; sugere-se a criação de um prêmio por excepcionalidade da solução proposta.

Não acolhida

O TSE tenta promover em seus eventos abertos à comunidade, ambientes de colaboração, em detrimento de competição. Esse direcionamento foi construído a partir da experiência acumulada nas primeiras edições do TPS. Nessas ocasiões, havia premiação e, em decorrência, forte sentimento de competitividade entre os investigadores e o TSE e também entre os próprios investigadores. Como decorrência direta da competitividade, houve impactos negativos resultantes da postura de investigadores que se sentiram prejudicados, ora por não terem sido premiados, ora por não concordarem com o nível de importância dado pelo TSE a seus achados.

Ocorre que o caráter institucional e a visibilidade nacional obtida por investigadores no TPS é campo fértil para uma ambiência de competitividade. Assim, no sentido de melhor gerenciar expectativas, sentimentos e avanços técnicos, já há algumas edições, o TSE tem investido em um discurso de colaboração. Os investigadores são estimulados a colaborarem entre si e a colaborarem com a Justiça Eleitoral durante o TPS. Os reais vencedores são todos os brasileiros, que, através do processo de colaboração, obtêm um sistema eleitoral cada vez mais seguro. Entende-se que o caminho da colaboração – e não o da competição – têm dado excelentes frutos. Observe-se, a critério de exemplo, a repetida participação de universidades em edições recentes do TPS, como a UFMS. Em um ambiente colaborativo, investigadores e investigadoras sentem-se acolhidos e dispostos a ajudarem uns aos outros, geralmente obtendo resultados mais sólidos.

Criar "trilhas" para exercitar as investigações orientadas ao aprimoramento dos sistemas eleitorais e geração de novas proposições conceituais para as eleições do futuro.

Considerações da Comissão: Os estudos sobre a segurança de processos eletrônicos estão atualmente em alta no cenário acadêmico e profissional. Nesse contexto, torna-se crucial desenvolver novas abordagens para assegurar a qualidade das tecnologias utilizadas no desenvolvimento e na segurança dos sistemas eleitorais.

4 Recomendações

4.1 Recomendações quanto ao processo e ambiente de realização do TPS:

a. Disponibilizar documentos relativos aos processos e sistemas eleitorais de forma permanente, como apresentações sobre o processo eleitoral, módulos que compõem os sistemas e perguntas e respostas para dirimir dúvidas;

b. Disponibilizar acessórios de mercado, compatíveis com a urna, tais como: cabos, adaptadores, microfones, fones de ouvido e ferramentas para facilitar a execução dos testes pelos investigadores;

c. Apresentar e permitir acesso a todo o ambiente disponibilizado para os testes em um momento anterior ao TPS;

d. Disponibilizar uma visão sistêmica do código fonte de forma a nortear e facilitar a leitura do código, bem como, um mapa identificando os módulos e programas nos moldes do documento "Visão Sistêmica das Eleições";

e. Disponibilizar um espaço, quando necessário, que permita gravação de som de um ambiente de eleições com mínimo ruído;

f. Criar um período de esclarecimento de dúvidas, posterior ao período de disponibilização dos vídeos e apresentação dos sistemas eleitorais, para o melhor entendimento dos processos e do código fonte;

g. Avaliar a possibilidade de acesso ao código fonte além da estrutura do TSE, por exemplo, no ambiente dos TRE;

h. Disponibilizar infraestrutura de instalação de software no ambiente de Teste Público de Segurança a fim de agilizar a instalação de ferramentas pelas equipes para a realização dos testes aprovados;

i. Disponibilizar durante a fase de confirmação do TPS, uma ferramenta que permita a comparação de forma visual dos códigos alterados;

j. Providenciar a configuração do ambiente de TPS para cada equipe, conforme estabelecido no plano de teste aprovado. Para tal, é essencial:

    1. Examinar o plano de teste elaborado pelos investigadores, identificando a necessidade de quaisquer equipamentos externos necessários para a realização dos testes. Na eventualidade de tais equipamentos serem de responsabilidade do Tribunal Superior Eleitoral (TSE), estes deverão ser preparados e disponibilizados antecipadamente. No caso de os equipamentos serem providos pelos investigadores, recomenda-se que sejam entregues com antecipação, visando minimizar atrasos e otimizar o processo de espera e liberação deles no momento da execução dos testes.

2. Disponibilizar uma urna desmontada para facilitar a visualização dos componentes internos e dos cabos com a devida documentação fornecida pelos fabricantes.

4.2 Recomendações Gerais

a. A transparência e a rastreabilidade no processo eletrônico de votação são fundamentais para a manutenção da confiança pública nas eleições. Nesse contexto, é essencial que o TSE permita um acompanhamento amigável e detalhado do processo de votação eletrônica para os diversos segmentos da sociedade, incluindo partidos políticos, universidades, público especializado e participantes do Teste Público de Segurança (TPS).

   Para garantir um entendimento claro e abrangente do processo eleitoral, deve-se adotar uma abordagem que inclua explicações detalhadas e visuais das etapas de votação, processamento e totalização dos votos. A apresentação didática de cada fase, desde a inserção do voto até o armazenamento e totalização dos dados, é crucial para garantir a compreensão pública e a confiança no sistema.

   A apresentação dos códigos fonte aos diversos segmentos da sociedade, por exemplo, é essencial para assegurar a transparência e a confiabilidade do processo eleitoral. A disponibilização desses códigos deve ser acompanhada do uso de ferramentas adequadas para auditoria de código fonte, que permitam uma análise minuciosa e independente. Ao segmentar o código em módulos compreensíveis e auditáveis, e ao utilizar plataformas de auditoria que destacam possíveis vulnerabilidades, o TSE não apenas reforça a transparência e a confiança no processo eleitoral, mas também promove um ambiente de colaboração e escrutínio técnico que é essencial para a integridade e credibilidade das eleições.

   Outrossim, faz-se importante a implementação de metodologias robustas para assegurar a integridade dos dados. Disponibilizar mecanismos de auditoria detalhados e acessíveis permitirá que especialistas em segurança da informação, representantes de partidos políticos e cidadãos interessados verifiquem o funcionamento interno dos sistemas eleitorais.

   A adoção dessas medidas tornará o processo eleitoral mais acessível e confiável, fortalecendo a confiança pública e a legitimidade das eleições. É vital que o TSE continue a evoluir suas práticas, sempre com o objetivo de promover a transparência, a rastreabilidade, a integridade, a observabilidade e a verificabilidade do processo eleitoral, atendendo às expectativas de todos os envolvidos e promovendo uma democracia robusta e confiável.

b. O TSE tem buscado evoluir a segurança e a transparência do sistema eleitoral em parceria com universidades brasileiras. Um desses aperfeiçoamentos é o mecanismo conhecido como "verificabilidade fim-a-fim", que permite aos eleitores uma confiança ainda maior de que suas escolhas foram registradas corretamente, sem diminuir o sigilo dos votos lançados. Projetos desse tipo, desenvolvidos conjuntamente por técnicos do TSE e pesquisadores brasileiros,

abrem um novo caminho para a evolução contínua do sistema eleitoral brasileiro e devem ser incentivados;

c. Considerando que os códigos fontes dos sistemas eleitorais desenvolvidos para a realização das eleições são complexos e extensos, e que as documentações existentes ainda são insuficientes para ampliar as abordagens de verificação e auditoria, seria recomendável avaliar os meios e os processos que podem agregar novos caminhos facilitando o acompanhamento técnico e processual dos produtos empregados pela Justiça Eleitoral na preparação e operação das eleições, melhorando o fator "transparência" e "confiabilidade";

d. O FORTI, um encontro dos membros técnicos envolvidos em sistemas de tecnologia da informação, foi criado para compartilhamento dos conhecimentos técnicos e produtos internos desenvolvidos pelo TSE e TRE e trouxe um ganho sensível de produtividade e interação entre as equipes. Tendo em vista que a Justiça Eleitoral tem colhido muitos resultados positivos desta iniciativa, recomenda-se que seja avaliado a possibilidade de dar continuidade ao processo buscando o aprimoramento desta sinergia, em especial nas discussões e estudos de novas tecnologias de desenvolvimento de sistemas e segurança, assegurando a vanguarda na qualidade e tranquilidade das eleições no país;

e. A Comissão Avaliadora, composta por especialistas não vinculados à Justiça Eleitoral, poderia ter a sua missão melhor especificada para uma atuação mais completa no contexto do TPS. O TPS é um nome dado inicialmente para a realização de um evento pontual que reúne os candidatos interessados na verificação dos sistemas eleitorais desenvolvidos para as eleições do ano subsequente. Todavia, após a realização de vários eventos, verifica-se não somente a qualidade das abordagens propostas, mas uma diversificação das metodologias e focos, tornando cada evento mais abrangente que os anteriores. Uma característica evolutiva que faz com que a abrangência das informações buscadas sejam ampliadas desde a concepção até a finalização das eleições. Assim sendo, a atuação da Comissão Avaliadora poderia acompanhar esta visão, ampliando a sua participação em todo o sistema eleitoral, concluindo o processo com a realização do TPS.

7.20 Anexo T – Relatório técnico final do TSE

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 – 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 – EDIÇÃO 2023 36

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

INTRODUÇÃO

O Teste Público de Segurança 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 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.

TESTE PÚBLICO DE SEGURANÇA DA URNA

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

Tribunal Superior Eleitoral

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

TESTE PÚBLICO DE SEGURANÇA DA URNA

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.

Tribunal Superior Eleitoral

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 – EDIÇÃO 2023

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

O Teste Público de Segurança 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, 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.

TESTE PÚBLICO DE SEGURANÇA DA URNA

RESUMO DOS NÚMEROS DO TESTE PÚBLICO DE SEGURANÇA – 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

7.21 Anexo U – Relatório final da USP

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

Laboratório de Arquitetura e Redes de Computadores

Relatório Técnico: RT-TESTE-CONFIRMAÇÃO-USP-LARC
Projeto: TPS 2023

Parceiro: Tribunal Superior Eleitoral - TSE
Referência: Convênio TSE nº 15/2023

Data: 27/05/2024

2

Título	Relatório Técnico RT-TESTE-CONFIRMAÇÃO-USP-LARC
Versão	1.0
Data	27/05/2024
Autores	Equipe LARC-USP TPS
Projeto	TPS 2023

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

Sumário

Sumário 1
Sumário Executivo 2
1 Introdução 3
2 Sumário dos Planos de Testes no Teste de Confirmação 4
3 Detalhamento dos Planos de Teste 5
3.1 Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect 5
3.2 Escalação de privilégio no Windows-SIS 7
3.3 Executar código espúrio na Urna Eletrônica modelo 2020 9
3.4 Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020 11
3.5 Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI 12
4 Análise do Teste de Confirmação 14
4.1 Análise do perfil das solicitações dos investigadores 14
5 Recomendação para o próximo Teste de Confirmação 16
5.1 Atesto da mitigação pelos investigadores 16
6 Considerações Finais 17
7 Anexos 18

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

Sumário Executivo

Este relatório foi elaborado para evidenciar as observações da equipe do LARC, registrando sua participação no Teste de Confirmação – etapa complementar ao Teste Público de Segurança TPS 2023 – realizado nas dependências do TSE de 15 a 17 de maio de 2024.

Esta participação é uma atividade prevista no cronograma do projeto e tem por objetivo apoiar o TSE na execução do Teste de Confirmação, onde os representantes do LARC atuam como Apoio Técnico, acompanhando os investigadores na verificação das mitigações de achados. Tais atividades são previstas como objeto do Convênio-TSE nº15/2023 firmado entre o Tribunal Superior Eleitoral (TSE) e a Universidade de São Paulo (USP), cujo principal objetivo é avaliar e identificar vulnerabilidades, falhas ou potenciais pontos de melhoria em relação à integridade e ao anonimato dos votos em eleições brasileiras.

O presente relatório descreve os planos de teste alistados para o Teste de Confirmação, considerando as mitigações implementadas pelo TSE para cada achado.

Para cada plano de teste foram identificados os investigadores proponentes, os apoios técnicos que acompanharam os investigadores, bem como descritos o objetivo do plano de teste, os passos propostos pelo investigador, o relaxamento dos mecanismos de segurança para sua execução, o resultado e um breve comentário técnico.

Na última parte deste documento a equipe do LARC fez uma avaliação analítica, com estatísticas a partir dos números observados e coletados durante o evento, de forma a contribuir com o planejamento do próximo Teste de Confirmação.

Por fim, também foram feitas recomendações, sob o ponto de vista da preparação, do processo, da infraestrutura e da dinâmica de execução dos testes.

As considerações finais encerram este documento.

Nos anexos, encontram-se relatórios detalhados dos testes dos achados realizados pelo LARC em laboratório e as respectivas observações no Teste de Confirmação.

1 Introdução

Desde 2009 o Teste Público de Segurança (TPS) do sistema eletrônico de votação vem sendo aplicado com a finalidade de fortalecer a confiabilidade, transparência, segurança na captação e na apuração dos votos, além de propiciar melhorias no processo eleitoral. O principal objetivo do TPS é efetuar ações controladas com o objetivo de identificar e corrigir vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição.

Neste contexto, o TSE e a USP, firmaram o Convênio-TSE nº15/2023, com a finalidade do Laboratório de Arquitetura e Redes de Computadores (LARC) do Departamento de Engenharia de Computação e Sistemas Digitais (PCS) da Escola Politécnica da USP, planejar, executar testes que antecederam o TPS, relatar pontos de melhoria ao TSE, além de acompanhar o TPS, emitir relatórios de acompanhamento com recomendações, bem como verificar a eficácia das soluções empregadas para correção de possíveis vulnerabilidades ou falhas. É neste contexto que se insere o Teste de Confirmação, que visa encerrar um ciclo de colaboração entre o TSE e os investigadores iniciado no TPS 2023.

Para acompanhamento dos trabalhos do Teste de Confirmação, a equipe do LARC foi composta pelos seguintes pesquisadores:

- Marcos Antonio Simplicio Junior
- Eduardo Seiti Teruiya
- Felipe Kenzo Shiraishi
- Fernando Frota Redígolo
- Gabriel Soares dos Santos Nunes
- Matheus Tavares de Andrade
- Otávio Felipe de Freitas

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

2 Sumário dos Planos de Testes no Teste de Confirmação

Plano de Teste		Situação Final	Data Término	Investigador(es)	
				ID	Nome(s)
01	Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect	Mitigado	16/05	G-4 (UFMS)	Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho
02	Escalação de privilégio no Windows-SIS	Mitigado	17/05		
03	Executar código espúrio na Urna Eletrônica modelo 2020	Mitigado	17/05	G-5 (PF)	Galileo Batista de Sousa, Maria Isabel Vasconcelos Lima, Breno Rangel Borges Marchetti, João Paulo Vieira Almeida e João Vitor de Sá Hauck
04	Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020	Mitigado	17/05		
05	Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI	Mitigado	17/05		

LARC Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

USP

3 Detalhamento dos Planos de Teste

3.1 Violar a confidencialidade, integridade e disponibilidade das informações no Python do Software JEConnect

Investigadores: Grupo UFMS: Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho

Apoio Técnico: Marcos Antonio Simplicio Junior, Felipe Kenzo Shiraishi e Gabriel Soares dos Santos Nunes

Objetivo: Atacar o JE-Connect explorando a vulnerabilidade encontrada no TPS. O sistema JE-Connect foi planejado para, a cada três erros de credenciais, realizar o reboot do kit, de forma 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. Este parâmetro não foi implementado no JE-Connect disponibilizado no TPS, apesar de ser uma necessidade já mapeada pela equipe de desenvolvimento do JE-Connect. 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 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 um eleitor votou.

Resultado: **Mitigado**.

Etapas Propostas:

1. Acessar o BIOS sem controle de acesso baseado em senha;

2. Acessar a senha de um JE-Connect e um kit JE-Connect;
3. Após inserir alternativas de senhas erradas, interromper processamento de validação pressionando CTRL + C;
4. Derivar variações de combinações de teclas que possam incorrer no mesmo evento resultado.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS e Kit/senha do JE-Connect. Fornecimento de senha do BIOS da máquina SIS.

Considerações técnicas: A primeira atividade realizada pelo grupo foi a de revisitar a tela de login do JE-Connect. Reproduziram os passos de inserir 2 tentativas de PIN erradas e, ao inserir a terceira, tentar interromper o processo pressionando CTRL + C. O processo não foi interrompido e o JE-Connect foi encerrado, conforme a especificação. Variações foram exploradas com outras combinações de teclas, mas o mesmo resultado foi obtido. Desta forma, foi atestado pelos investigadores que o achado encontrado durante o TPS foi corrigido. Maiores detalhes poderão ser encontrados no relatório anexo “Relatório de Reteste – SIS e JE-Connect”, que compila todos os testes observados e realizados pelo LARC-USP.

3.2 Escalação de privilégio no Windows-SIS

Investigadores: Grupo UFMS: Carlos Alberto da Silva, Ian Martinez Zimmermann, Matheus Vianna Silveira e Mário de Araújo Carvalho

Apoio Técnico: Marcos Antonio Simplicio Junior, Felipe Kenzo Shiraishi e Gabriel Soares dos Santos Nunes

Objetivo: Atacar o SIS, promovendo escalação de privilégios. 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. Foi identificado no código fonte que o fechamento de proteção é solicitado, mas, 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. O privilégio permitiu aos investigadores ler, alterar ou apagar arquivos. A eventual alteração do conteúdo de arquivos assinados provocaria inconsistência e bloqueio do equipamento pelo SIS. Alterações também seriam detectadas com o uso do VAD ou VAP. Apesar do achado, a visualização dos arquivos mantidos no SIS e assinados digitalmente não produz efeitos sobre a integridade ou o sigilo do voto. A eventual alteração dos arquivos ensejaria incoerência de assinatura digital, uma vez que os arquivos são verificados pelo Gedai no momento de sua execução.

Resultado: **Mitigado**.

Etapas Propostas:

1. Acessar a funcionalidade de impressão de certificados do aplicativo de verificação de assinatura contido no SIS para a opção de imprimir como PDF;
2. Acessar diretórios não autorizados para o usuário fornecido;
3. Fazer análise exploratória de outras oportunidades similares de escalação de privilégios em aplicações autorizadas ao usuário fornecido.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS.

Considerações técnicas: No segundo dia, os investigadores reproduziram o achado do TPS ao tentarem acessar o conteúdo de diretórios não autorizados com a aplicação de verificação de assinaturas, usando sua funcionalidade de impressão de certificados. Ao não conseguirem tal acesso, reconheceram que a mitigação implementada corrigiu o achado. Em seguida, exploraram funcionalidades semelhantes em outras aplicações do SIS disponíveis no MS-Windows, como o Internet Explorer e o Painel de Controle, também sem sucesso. Apesar de não terem conseguido explorar exaustivamente todos os possíveis executáveis presentes no MS-Windows, os investigadores se deram por satisfeitos ao concluir que, para as aplicações e funcionalidades exploradas, havia a correta atribuição de permissões, de modo que o usuário não conseguiria extrapolar as suas próprias permissões de acesso. Maiores detalhes poderão ser encontrados no relatório anexo “Relatório de Reteste – SIS e JE-Connect”, que compila todos os testes observados e realizados pelo LARC-USP.

3.3 Executar código espúrio na Urna Eletrônica modelo 2020

Investigadores: Grupo Polícia Federal: Galileo 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, Otávio Felipe de Freitas e Matheus Tavares de Andrade

Objetivo: Executar um ataque do tipo TOCTOU (*Time Of Check to Time Of Use*), utilizando um equipamento Beaglebone para simular uma mídia de carga e alterando o conteúdo de uma biblioteca compartilhada após a verificação de sua assinatura.

Resultado: **Mitigado**.

Etapas Propostas:

1. Clonar mídia de carga;
2. Carregar sua imagem no Beaglebone;
3. Realizar uma carga na urna, utilizando o Beaglebone 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.

Relaxamento nos mecanismos e procedimentos de segurança: Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI. Fornecimento da senha para acesso da BIOS e para acesso ao ambiente Windows/SIS. Acesso aos códigos-fonte da Urna Eletrônica e do BIOS.

Considerações técnicas: Os investigadores da Polícia Federal identificaram que as vulnerabilidades de ToC-ToU exploradas no TPS foram sido corrigidas, não

sendo mais possível inserir código arbitrário nos mesmos elementos. Por outro lado, ao investigar mais detalhadamente a versão atualizada do sistema, identificaram um arquivo de configuração suscetível a ataques de ToC-ToU, ao ser lido mais de uma vez sem que fosse repetida sua verificação. A despeito disso, e após diversas tentativas, percebeu-se que a interceptação deste arquivo não permitia a execução de ações indevidas no sistema, em particular pela ausência de qualquer ponto nesse arquivo que pudesse ser tratado como instrução executável. Essa conclusão foi atingida após a consideração de diversos cenários, incluindo a eventual possibilidade de um teste de *buffer overflow* – hipótese descartada após análise do código-fonte, durante a qual foi possível perceber que o *buffer* era delimitado e, portanto, não seria suscetível a ataques dessa natureza. Ao final, exauridas as hipóteses de eventuais frentes de ataque, os investigadores chegaram a resultados similares àqueles obtidos pela equipe do LARC-USP e concluíram que a mitigação implementada mostrou-se adequada. Maiores detalhes poderão ser encontrados no relatório anexo "Relatório de Reteste – Bootloader/BIOS", que compila todos os testes observados e realizados pelo LARC-USP.

3.4 Extrair a chave que cifra/decifra o kernel da Urna Eletrônica modelo 2020

Investigadores: Grupo Polícia Federal: Galileo 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, Otávio Felipe de Freitas e Matheus Tavares de Andrade

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.

Resultado: **Mitigado**.

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.

Relaxamento nos mecanismos e procedimentos de segurança: Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI. Fornecimento da senha para acesso da BIOS e para acesso ao ambiente Windows/SIS. Acesso aos códigos-fonte da Urna Eletrônica e do BIOS.

Considerações técnicas: Com o insucesso na execução de código espúrio na Urna Eletrônica, não foi mais possível explorar esta vulnerabilidade. Maiores detalhes poderão ser encontrados no relatório anexo "Relatório de Reteste – Bootloader/BIOS", que compila todos os testes observados e realizados pelo LARC-USP.

3.5 Recuperar a chave de criptografia do Bitlocker utilizada para cifrar o disco do sistema Windows onde roda o SIS/GEDAI

Investigadores: Grupo Polícia Federal: Galileo 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, Otávio Felipe de Freitas e Matheus Tavares de Andrade

Objetivo: Utilizar técnicas avançadas para recuperar a chave guardada no TPM, utilizada pelo Bitlocker, para cifrar/decifrar o disco da máquina onde são executados os softwares SIS/GEDAI.

Resultado: **Mitigado**.

Etapas Propostas:

1. Utilizar a placa PCILeech para capturar a chave do Bitlocker que está na memória RAM.

Relaxamento nos mecanismos e procedimentos de segurança: Fornecimento de usuário/senha do SIS/GEDAI-EU e do BIOS. Autorização para abertura dos gabinetes da urna eletrônica e da máquina com o SIS/GEDAI.

Considerações técnicas: Os investigadores da Polícia Federal conseguiram reconfigurar e otimizar o ambiente de testes para a captura da memória total da máquina em 2 execuções do ataque. Como resultado, conseguiram a captura da chave do Bitlocker na memória, mesmo com a mitigação implementada (esta ainda apresentava uma pequena possibilidade de repetição do ataque pela forma como foi implementada). Em vista da limitação da mitigação e, após discussões técnicas entre os investigadores da PF, equipe do LARC e a equipe responsável pelo módulo SIS, foi implementada uma nova mitigação o ataque com a PCILeech. Na nova mitigação, caso uma das opções do BIOS seja desativada, possibilitando o ataque, o driver de subsistema responsável por verificar tal configuração apaga a chave do BitLocker localizada na placa-mãe da máquina.

Este comportamento inutiliza a máquina, sendo necessário possuir a chave de recuperação do BitLocker para restaurá-la. Assumindo que atacante não terá acesso a tal chave, o ataque foi efetivamente mitigado. Os investigadores da Polícia Federal puderam atestar que a nova mitigação com o apagamento da chave no BitLocker, foi eficaz para impedir o ataque utilizando o PCILeech. Maiores detalhes poderão ser encontrados no relatório anexo “Relatório de Reconhecimento – TPS 2023 – Ataque com PCILeech para descoberta da chave BitLocker no módulo SIS”, que compila todos os testes observados e realizados pelo LARC-USP.

4 Análise do Teste de Confirmação

4.1 Análise do perfil das solicitações dos investigadores

Com base nas solicitações feitas pelos investigadores durante o Teste de Confirmação, a equipe do LARC elaborou análises que poderão contribuir com o planejamento e dinâmica do próximo evento.

Do total de 15 solicitações/sugestões feitas pelos investigadores durante o evento para auxiliar na execução dos planos de testes, apenas 1 foi indeferida pela Comissão Reguladora.

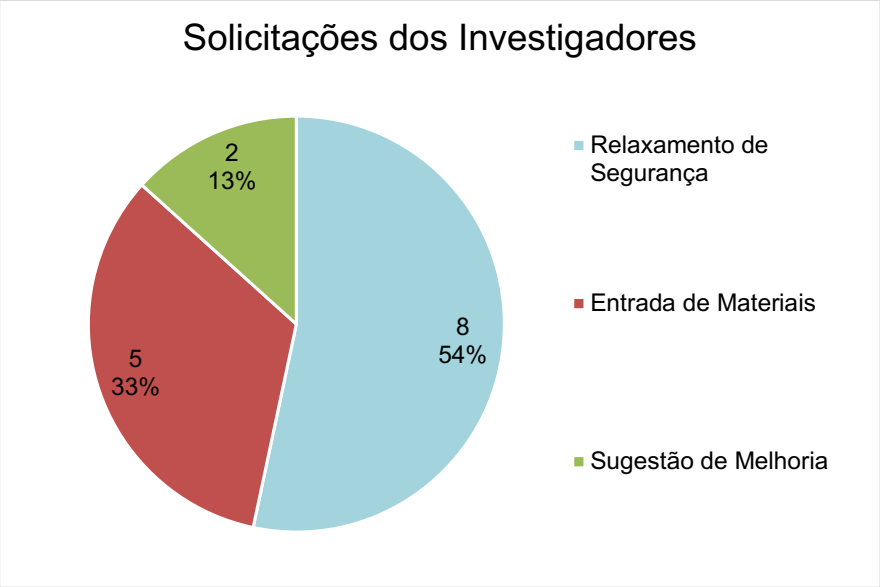


Gráfico 1: Classificação das Solicitações dos Investigadores durante o TPS

No gráfico 1, as solicitações para autorização de instalação e uso de softwares diversos foi agrupada nas solicitações de entrada de materiais, tornando o número bastante representativo.

O gráfico 2 indica que 60% das solicitações foram feitas no primeiro dia do evento, incluindo a maioria dos pedidos para relaxamento dos mecanismos e procedimentos de segurança e para entrada de materiais.

Gráfico 2: Solicitações dos Investigadores por Dia

5 Recomendação para o próximo Teste de Confirmação

5.1 Atesto da mitigação pelos investigadores

Na abertura dos trabalhos do Teste de Confirmação, sugere-se explicar a todos os presentes detalhadamente o procedimento em que o investigador atesta a efetividade da mitigação implementada pelo TSE para sanar o achado encontrado no TPS.

Neste Teste de Confirmação, o grupo de investigadores da UFMS havia associado equivocadamente o preenchimento do "Termo de Confirmação" ao encerramento imediato das atividades de teste daquele respectivo achado. Essa associação gerou resistência por parte do grupo ao preenchimento do termo, uma vez que já haviam verificado a efetividade da mitigação, porém, tinham a intenção de continuar explorando diferentes variações do procedimento de ataque respeitando o mesmo objetivo do plano de teste. Este escopo ampliado da execução do plano de teste foi objeto de análise pela equipe do Apoio Técnico juntamente com a Comissão Reguladora, que deferiu a possibilidade de continuar a exploração desde que não se desviasse do objetivo do plano de teste.

O esclarecimento deu-se apenas por ocasião do encerramento das atividades do referido grupo de investigadores, durante uma conversa informal que felizmente desfez a associação equivocada.

Por outro lado, essa resistência por parte do grupo de investigadores gerou situações de tensão, em alguns momentos, com os representantes do Apoio Técnico que acompanhavam o reteste.

6 Considerações Finais

Os trabalhos realizados envolveram os melhores esforços colaborativos entre as equipes do TSE e do LARC para atuar em três frentes principais no TPS:

- Acompanhamento dos investigadores na execução dos planos de testes propostos;
- Gestão das solicitações, conjuntamente com a Comissão Organizadora, feitas pelos investigadores durante o TPS para avaliação da Comissão Reguladora, de forma a obter autorizações para: entrada de materiais no ambiente de teste, procedimentos envolvendo os equipamentos disponibilizados na bancada (como abertura dos gabinetes das urnas eletrônicas) e relaxamento dos mecanismos de segurança;
- Avaliação geral do evento, acompanhando a execução dos planos de teste, interagindo com investigadores, Apoio Técnico, Comissão Organizadora, Comissão Reguladora e Comissão Avaliadora.

Além disso, a equipe do LARC esteve envolvida na etapa que antecedeu o Teste de Confirmação, onde interagiu com os técnicos do TSE para executar testes que exercitassem as mitigações implementadas pelo TSE para cada um dos achados.

Com a experiência adquirida pela equipe do LARC ao participar dos TPS 2021 e TPS 2023, espera-se uma integração cada vez maior com a equipe do TSE, com o intuito de aumentar as contribuições para aperfeiçoamento do evento e do sistema de votação eletrônica.

7 Anexos

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

Laboratório de Arquitetura e Redes de Computadores

Relatório de Reteste - SIS e JE-Connect

Projeto: Relato do teste de confirmação: Escalação de Privilégio no SIS e de Aumento de Tentativas de Login no JE-Connect

Cliente: Tribunal Superior Eleitoral (TSE)

Autores: LARC - EPUSP

Data: 25 de maio de 2024

Sumário

Resumo Executivo **3**

1. Introdução **4**

2. Testes do TPS 2023 **5**
2.1. Elevação de privilégio no ambiente SIS 5
2.2. Aumento de número de tentativas de inserção de PIN para a decifração do JE-Connect 5

3. Retestes em laboratório **7**

4. Atividades na semana do teste de confirmação **8**
4.1. Reteste do aumento do número de tentativas no JE-Connect 8
4.2. Reteste da elevação de privilégio no SIS 9

5. Comentários do apoio técnico **10**
5.1. Considerações sobre as atividades dos investigadores 10
5.2. Considerações sobre as mitigações 10
5.3. Observação de oportunidades de investigação 10

6. Conclusão **11**

Lista de Figuras

Resumo Executivo

Este relatório trata dos testes executados pelo grupo 4 no TPS de 2023 e respectivos achados, que foram objeto de revisão no teste de confirmação. As atividades do grupo de investigadores são sumarizadas e as propostas de mitigações são comentadas em termos de efetividade. Elaborações do teste ainda atinentes ao escopo permitiram verificar a robustez da solução e a não-reincidência de achados em outros contextos para a aplicação da mesma técnica.

Dessa forma, o teste de confirmação verificou a efetividade do controle implementado para limitar as 3 tentativas de inserção de PIN para a decifração do JE-Connect . Além disso, no teste de confirmação foi verificada a correta atribuição de políticas de segurança granularizadas por funcionalidade no SIS. Esta correção substitui a atribuição de permissões a uma aplicação de forma monolítica, corrigindo então o achado da equipe de investigadores relativo ao SIS.

1. Introdução

Este relatório apresenta as considerações técnicas da equipe do LARC-USP sobre: (1) os testes executados pelo grupo 4 no TPS de 2023; (2) suas atividades no teste de confirmação em 2024; e (3) as atividades de reteste realizadas pela equipe do LARC-USP antes do teste de confirmação.

O relatório organiza-se da seguinte maneira. Na seção 2 é feita uma recapitulação dos dois testes que levaram a achados no TPS 2023, apresentando-se considerações da equipe do LARC sobre possíveis correções. Cabe apontar que estes testes não são referentes aos planos de testes originalmente inscritos no TPS, mas sim são decorrentes de exploração e interação direta com os objetos de análise durante a semana do TPS; ou seja, trata-se de testes propostos durante o evento. Dessa forma, a sua referência se encontra apontada no relatório de avaliação geral disponibilizado no site do TPS, e não nos planos de testes originalmente inscritos.

As atividades de reteste realizadas nas dependências do LARC são apresentadas na seção 3. Estas atividades foram realizadas a pedido do TSE para verificar previamente a efetividade das mitigações implementadas. As atividades empreendidas pela equipe de investigadores durante a semana do teste de confirmação é documentada na seção 4. Por fim, na seção 5 são apresentadas considerações do apoio técnico responsável pelo acompanhamento, sobre: (1) as atividades dos investigadores; (2) mitigações feitas pelo TSE; e (3) observação de oportunidades de investigação que ainda podem ser realizadas dado o curso de ação explorado pelos investigadores;

2. Testes do TPS 2023

Durante o TPS 2023 a equipe G-4 relatou 2 achados, provenientes de testes novos, propostos e executados durante o próprio evento.

2.1. Elevação de privilégio no ambiente SIS

Este teste explorava uma privilégio de leitura e escrita da aplicação de verificação de assinaturas de arquivos no sistema de arquivos do ambiente SIS. O usuário fornecido aos investigadores possuía privilégios reduzidos de leitura e escrita neste sistema de arquivos, sendo incapaz de visualizar arquivos de aplicações e dados de alguns diretórios. Entretanto, para possibilitar a verificação da integridade e autenticidade dos arquivos em diretórios protegidos, a aplicação de verificação de assinaturas possuía privilégios mais elevados, que permitiam que ela acessasse o conteúdo de diretórios protegidos.

A vulnerabilidade encontrada revelou-se na funcionalidade de impressão de certificados desta aplicação. Como havia a possibilidade de imprimir um conteúdo como um arquivo PDF a ser salvo em disco, uma janela de navegação do sistema de arquivos era fornecida ao usuário, para que este pudesse escolher o local de salvamento. Em razão da aplicação estar com permissões de leitura e escrita para diretórios protegidos, por meio desta janela o usuário era capaz de acessar tais diretórios e extrair o seu conteúdo para um diretório onde tivesse permissões de examiná-los. Além disso, havia a possibilidade de substituição de arquivos destas pastas, dada a permissão de escrita em seu interior, havendo a possibilidade de adulteração de integridade de arquivos executáveis e de dados.

Dessa forma, a correção apropriada da vulnerabilidade era uma correta atribuição de permissões a esta aplicação e outras similares no SIS. Entretanto, isto deveria ser feito de forma a não remover da aplicação de verificação de assinaturas a capacidade do usuário verificar a integridade dos arquivos ali contidos. De forma geral, seria recomendável atribuir uma permissão de acesso por funcionalidade de uma aplicação em vez de se atribuir uma permissão de acesso à aplicação toda, de maneira a evitar comportamentos indesejados, como o explorado pelo grupo de investigadores.

2.2. Aumento de número de tentativas de inserção de PIN para a decifração do JE-Connect

Neste teste, o processo de inicialização do JE-Connect era interrompido por meio da combinação de teclas ”CTRL + C”durante o processamento da terceira tentativa de inserção de PIN. Tal ação provocava o reinício do processo de requisição do PIN, zerando o contador de tentativas de inserção de PIN e, assim, permitindo ao usuário testar um número de PINs superior ao limite estabelecido de 3. Isto ocorria pelo fato do processo não ser chamado com o parâmetro de execução ”forcefully”, que poderia evitar a sua interrupção.

A correção para o problema identificado seria a execução do processo de requisição de PIN em modo ”forcefully”. Além disso, como a vulnerabilidade encontrada consistia em uma exploração do domínio

de interações possíveis com entradas de teclado na tela de login, seria apropriado também revisar todos os controles relacionados à sanitização de entradas ou atalhos. Cabe entretanto reconhecer que, como a tela de inserção de PIN para a decifração do JE-Connect é apresentada na sua inicialização, dentro do contexto do *initramfs*, não seria apropriado carregar muitas dependências para este contexto como parte do procedimento de sanitização de entradas.

3. Retestes em laboratório

Deste conjunto de testes, apenas o de escalação de privilégios no SIS foi reavaliado nas dependências do LARC. O motivo para esse foco específico, em oposição a uma cobertura total, é que a equipe do laboratório teve seus esforços concentrados no reteste dos achados da Polícia Federal, conforme solicitação da equipe do TSE.

Para o reteste de escalação de privilégio, a equipe do LARC teve acesso a duas máquinas SIS, uma com versão mais antiga (apresentando a vulnerabilidade) e outra com a vulnerabilidade corrigida.

Em laboratório, a equipe reproduziu com sucesso os testes na máquina vulnerável, tendo acesso ao conteúdo de diretórios não permitidos. No entanto, a equipe não teve sucesso em acessar esses mesmos conteúdos na máquina com as correções, verificando que a nova versão mitigava o achado do TPS 2023.

Cabe apontar que outras aplicações e suas respectivas funcionalidades também foram exploradas, de modo a verificar a existência de uma vulnerabilidade similar em outras instâncias. Nenhuma vulnerabilidade foi encontrada dentro do escopo e tempo em que tais testes foram realizados.

4. Atividades na semana do teste de confirmação

A equipe de investigadores do G-4 elaborou um plano de investigação distribuído ao longo dos três

4.2. Reteste da elevação de privilégio no SIS

No segundo dia, os investigadores reproduziram o explorado no TPS: tentarem acessar o conteúdo de diretórios não autorizados com a aplicação de verificação de assinaturas, usando sua funcionalidade de impressão de certificados. Ao não conseguirem tal acesso, reconheceram que a mitigação implantada corrigia o achado. Em seguida, exploraram funcionalidades semelhantes em outras aplicações do SIS e disponíveis no windows, como o Internet Explorer e o Painel de Controle, também sem sucesso.

Apesar de não ter sido possível explorar exaustivamente todos os possíveis executáveis presentes no Windows, os investigadores se deram por satisfeitos ao concluir que, para as aplicações e funcionalidades exploradas, havia a correta atribuição de permissões, de modo que o usuário não conseguiria extrapolar as suas próprias permissões de acesso.

5. Comentários do apoio técnico

Após o acompanhamento dos investigadores, a equipe de apoio de técnico pôde emitir comentários sobre as atividades dos investigadores, a efetividade das mitigações realizadas pelo TSE, e sobre possível continuidade das investigações.

5.1. Considerações sobre as atividades dos investigadores

O grupo organizou o tempo e a investigação de forma apropriada, tirando o melhor proveito do período do reteste. Eles não se limitaram a reproduzir apenas os passos que levaram aos achados no TPS, mas também exploraram variações dentro do escopo para garantir a efetividade dos controles implementados pelo TSE. Este tipo de abordagem permitiu avaliar se as correções colocadas não seriam de caráter pontual, mas representavam uma correção sistêmica, refletindo um aprendizado da equipe técnica do TSE com o método de exploração adotado pelos investigadores.

5.2. Considerações sobre as mitigações

A equipe do LARC considera que as mitigações colocadas para os achados são suficientes para conter as técnicas adotadas pelos investigadores. É relevante apontar, no entanto, que no ambiente SIS há um desafio maior de segurança em razão do menor controle do sistema completo pelo TSE: é usada uma máquina com arquitetura de propósito geral, e um sistema operacional não mantido pela própria equipe. Logo, vulnerabilidades inesperadas podem surgir em razão de comportamentos de componentes alheios aos sistemas desenvolvidos pela equipe do TSE. Já em relação ao JE-Connect, ressalta-se o fato de que soluções robustas que cubram todas as oportunidades de exploração na tela de PIN podem enfrentar desafios com a concisão do contexto do *initram*.

5.3. Observação de oportunidades de investigação

Dentro do que foi possível acompanhar, a equipe de apoio técnico não enxerga lacunas na cobertura de testes realizada pela equipe de investigadores que suscitem encaminhamentos de exploração dentro do ambiente experimental do LARC. A equipe dá-se por satisfeita com o que foi avaliado em termos de código fonte e discussões realizadas com a equipe do TSE.

6. Conclusão

O teste de confirmação para os dois achados foi concluído com sucesso, atestando a efetividade dos controles implementados. A elaboração da exploração permitiu averiguar a não-recorrência de falhas ou vulnerabilidades em outros contextos quando aplicadas técnica similares às usadas durantes o TPS. A cobertura de teste realizada não apresentou lacunas que suscitassem curiosidade de escrutínio posterior pela equipe de apoio técnico.

Em compensação, tal como apontado pela equipe de investigadores, atestar a efetividade dos controles significa somente atestar a segurança das partes investigadas, não sendo possível inferir, por transitividade, a segurança do todo. O motivo para este comentário é o de reconhecer que as aplicações investigadas são constituídas de outras partes que não foram objeto do teste empreendido pelos investigadores. Desta forma, há ainda a possibilidade de se cogitar a existência de outros tipos de vulnerabilidades em outros componentes ou a existência de uma vulnerabilidade latente nos mesmos componentes investigados, mas que se expressem com a utilização de outras técnicas.

Em todo caso, considera-se que a equipe do G-4 contribuiu para a cobertura dos testes do sistema para as partes investigadas, e também com a elevação de sua segurança. Assim, é reconhecida a contribuição de seus testes com o amadurecimento da cultura de segurança da equipe de manutenção dos sistemas do SIS e do JE-connect.

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

Laboratório de Arquitetura e Redes de Computadores

Relatório de Reconhecimento - TPS 2023

Projeto: Ataque com PCILeech para descoberta da chave BitLocker no módulo SIS

Cliente: Tribunal Superior Eleitoral (TSE)

Autores: LARC - EPUSP

Data: 25 de maio de 2024

Sumário

Resumo Executivo **3**

1. Introdução **4**

2. Ambiente de Teste **5**
2.1. Hardware - Screamer Squirrel 5
2.1.1. Compilação 5
2.1.2. Gravação da Flash 6
2.2. Software - PCILeech 6
2.3. Volatility 7

3. Reteste com o PCILeech **9**
3.1. Máquina WIndows/SIS Vulnerável 9
3.2. Teste em Laboratório 11

4. Teste de Confirmação **12**

5. Considerações Finais **12**

Anexo A - flash_screamer_squirrel.cfg **15**

Lista de Figuras

1. Saída do volatility com as candidatas de chaves do BitLocker. 10
2. Chave BitLocker encontrada com sucesso, sendo possível visualizar o conteúdo da partição do SIS. 10

Resumo Executivo

Durante o Teste Público de Segurança de 2023, os investigadores do G5, composto por membros da Polícia Federal, foram capazes de extrair a chave BitLocker da máquina Windows/SIS. Para tanto, contaram não só com um relaxamento da configuração da BIOS da máquina, mas também com a utilização de uma placa especializada que acompanha uma biblioteca conhecida como PCILeech. Este equipamento foi instalado dentro da máquina alvo, e configurado para extrair o conteúdo da memória RAM diretamente do barramento da placa-mãe. A equipe do LARC-USP reproduziu os testes internamente, no mesmo modelo de máquina e nas mesmas condições de hardware/software do TPS, e constatou a vulnerabilidade do ambiente.

Uma vez recebida uma nova versão do SIS com a proposta inicial de mitigação do ataque, a sua efetividade também foi analisada nas dependêndias do LARC. Como resultado, verificou-se que a mitigacão inicial aplicada no módulo SIS comprometia de maneira significativa a taxa de sucesso do ataque: a mitigação diminiu de minutos para segundos a janela de tempo em que o conteúdo da memória do equipamento pode ser capturada. Assim, os resultados obtidos indicaram que tal característica, combinada com a baixa velocidade de captura da placa, deveria dificultar tentativas de ataque na prática, apesar de não o impedir completamente.

Durante o Teste de Confirmação, entretanto, os investigadores da Polícia Federal foram capazes de superar essa maior dificuldade imposta pela mitigação inicial, e capturaram a chave do BitLocker. Em particular, uma característica observada durante o Teste de Confirmação é que a velocidade de captura na máquina disponibilizada era bastante superior àquela observada dentro do ambiente do LARC, o que permitiu a execução do ataque após algumas tentativas. Em vista desse resultado negativo, e após conversa com os investigadores da PF e também da equipe do LARC, da equipe responsável pelo módulo SIS implementou uma nova solução para mitigar o ataque com a PCILeech. Essencialmente, a mitigação envolve o apagamento da chave do BitLocker ao observar a configuração indevida da BIOS que viabiliza o ataque, inutilizando a máquina em questão. Os investigadores e o apoio técnico responsável pelo teste concluíram que, na prática, a mitigação deve ser bastante eficaz contra o ataque.

1. Introdução

Durante o Teste Público de Segurança de 2023, os investigadores da Polícia Federal foram capazes de extrair a chave BitLocker da máquina Windows/SIS. Para tanto, contaram não só com um relaxamento da configuração da BIOS da máquina, mas também com a utilização de uma placa especializada que acompanha uma biblioteca conhecida como PCILeech. Este equipamento foi instalado dentro da máquina alvo, e configurado para extrair o conteúdo da memória RAM diretamente do barramento da placa-mãe. A equipe do LARC-USP reproduziu os testes internamente, no mesmo modelo de máquina e nas mesmas condições de hardware/software do TPS, e constatou a vulnerabilidade do ambiente. Após a disponibilização da versão Windows/SIS com uma mitigação inicial implementada, os testes foram refeitos, de maneira a se avaliar a efetividade da mitigação.

Este documento encontra-se organizado da seguinte maneira. O Capítulo 2 descreve o ambiente de teste utilizado pelos pesquisadores do LARC-USP. O Capítulo 3 detalha os testes na versão com e sem a mitigação. O Capítulo 4 apresenta as considerações sobre as atividades do Teste de Confirmação.

2. Ambiente de Teste

Esta sessão tem como objetivo detalhar os passos realizados pelos pesquisadores do LARC para reprodução do ataque no ambiente de teste.

O PCILeech é uma biblioteca que permite a leitura e escrita da memória de uma máquina-alvo, por meio um hardware PCIe especializado, capaz de se comunicar com a memória usando a funcionalidade de DMA no barramento PCIe. A biblioteca é compatível com múltiplos dispositivos de aquisição da memória. O dispositivo usado pelos investigadores da Polícia Federal foi a placa Screamer PCIe Squirrel, da empresa Lambda Concept, capaz de extrair até 190 MB/s da memória da máquina. A placa em questão foi adquirida pelo LARC-USP e preparada para a execução dos testes.

2.1. Hardware - Screamer Squirrel

A placa Screamer Squirrel é baseada em uma FPGA. Para o ataque, uma versão atualizada da imagem da FPGA deve ser compilada e instalada na placa.

2.1.1. Compilação

O repositório do PCILeech [ufrisk 2017] contém todos os arquivos fontes em Verilog necessários para a compilação. Especificamente, foram utilizados os fontes correspondentes à versão 4.15 do PCILeech, disponibilizados em 14/03/2024.

Comando 1 Comandos para clonar o repositório PCILeech com a versão utilizada.

```
$ git clone https://github.com/ufrisk/pcileech-fpga.git
$ git checkout ccc7f8ce16feaf1a0fc3d5922234273117ade52d
```

Com os códigos disponíveis, utiliza-se o software Vivado 2022.02 para realizar a compilação. No menu inicital, em `Windows -> Tcl Console`, são digitados os comandos apresentados na listagem 2.

Comando 2 Comandos para o Tcl Console.

```
$ cd /path/to/pcileech-fpga/PCIeSquirrel
$ source vivado_generate_project.tcl -notrace
$ source vivado_build.tcl -notrace
```

O resultado da compilação fica disponível no caminho da listagem 3.

Comando 3 Caminho do binário da placa Squireel

```
/path/to/pcileech-fpga/PCIeSquirrel/pcileech_squirrel/pcileec_squirrel.runs/impl_1/
    pcileech_squirrel_top.bin
```

2.1.2. Gravação da Flash

O processo de gravação na Flash possui variações a depender do sistema operacional. Este relatório foi escrito com a utilização de um Ubuntu 20.04.

O processo de gravação da memória flash da FPGA utiliza a ferramenta OpenOCD [openocd org 2008] [Project 2008] para depuração de dispositivos de hardware. Essa ferramenta permite adicionar uma interface de sinalização necessária para a depuração de cada tipo de dispositivo (Open On-Chip-Debugger). A versão adotada do OpenOCD é a do commit publicado em 01/04/2024

Inicialmente, antes de qualquer instalação, deve-se garantir o requisito mínimo para sistemas Linux.

Comando 4 Comandos para instalar o OpenOCD.

```
$ sudo apt install -y libusb-1.0-0-dev
$ git clone https://github.com/ntfreak/openocd.git
$ git checkout dd1758272276e20d5b60c16146a820ec8b5bfaa1
$ cd openocd ; ./bootstrap ; ./configure ; make
$ sudo make install
```

Em seguida, para manipular a memória flash, é necessário o LambdaConcept Flash Screamer disponível para download no website da documentação – `https://docs.lambdaconcept.com/screamer/programming.html`.

Comando 5 Comandos para Flash Screamer.

```
$ cd flash_screamer
$ cp /path/to/pcileech_squirrel_top.bin /path/to/flash_screamer
```

O arquivo `flash_screamer_squirrel.cfg` também deve ser alterado, conforme apresentado no Anexo 5. Em seguida, o OpenOCD é executado para iniciar a gravação na flash da FPGA.

Comando 6 Comando para gravar na flash da FPGA.

```
$ openocd -f flash_screamer_squirrel.cfg
```

2.2. Software - PCILeech

O software do PCILeech necessita de três bibliotecas obtidas por meio das 3 listagens a seguir: Comando 7, referente ao LeechCore (a versão adotada é a 2.18.1, publicada em 29/03/2024); Comando 8, referente ao MemprocFS (a versão usada foi a 5.9.5, publicada em 26/03/2024); e Comando 9, referente ao Leechcore-Plugins (a versão adotada é a 2.16.8 publicada em 28/11/2023).

Comando 7 Compilação da biblioteca LeechCore.

```
$ git clone https://github.com/ufrisk/LeechCore
$ git checkout 6ebec0adef99d267eb56d3eddc720b2d54eb4de7
$ cd LeechCore/leechcore
$ make
```

Comando 8 Compilação da biblioteca MemProcFS.

```
$ sudo apt-get install libusb-1.0 fuse openssl lz4
$ git clone https://github.com/ufrisk/MemProcFS
$ git checkout 11c6dedd3603e0b265e826c192d2e9073e3362f2
$ cd MemProcFS/vmm
$ make
```

Comando 9 Compilação da biblioteca LeechCore-plugins.

```
$ git clone https://github.com/ufrisk/LeechCore-plugins
$ git checkout 4c11afc5b68cc4b5e8e493788ab48d4f27fce954
$ cd LeechCore-plugins/leechcore_ft601_driver_linux
$ make
```

Por fim, em posse das outras bibliotecas compiladas, basta executar os comandos apresentados como Comando 10 para obter o binário que estará disponível em `pcileech/files`.

Comando 10 Compilação do PCILeech com as bibliotecas necessárias.

```
$ git clone https://github.com/ufrisk/pcileech/
$ git checkout f0c3b7330bcf091fdc45a92392d0541893168ea5
$ cd pcileech/pcileech
$ cp /path/to/MemProcFS/files/vmm.so /path/to/pcileech/files
$ cp /path/to/LeechCore/files/leechcore.so /path/to/pcileech/files
```

2.3. Volatility

Utilizou-se um plugin da ferramenta Volatility [volatilityfoundation 2020], em sua versão win10_19041 (publicada em 11/12/2020), para buscar chaves candidatas ao BitLocker. Os passos para compilação, tanto a ferramenta quanto do plugin, são apresentados na listagem nomeada Comando 11. A versão usada do Volatility-Bitlocker é aquela publicada no repositório em 27/01/2020.

Comando 11 Compilação do Volatility e seu plugin para BitLocker.

```
# Volatility
$ git clone https://github.com/volatilityfoundation/volatility
```

```
$ git checkout a438e768194a9e05eb4d9ee9338b881c0fa25937
$ cd volatility/
$ pip install --upgrade setuptools
$ sudo apt-get install python2-dev
$ pip2 install pycrypto
$ pip2 install distorm3

# Plugin
$ git clone https://github.com/breppo/Volatility-BitLocker
$ git checkout 4dc7e17df0557c4e18ef7fca685f8a1ad416128f
$ cp /path/to/Volatility-BitLocker/bitlocker.py /path/to/volatility/volatility/
    plugins/
```

3. Reteste com o PCILeech

Este capítulo descreve as atividades efetivas de reteste, considerando as configurações realizadas e descritas no capítulo anterior. O capítulo se divide em duas seções: uma seção inicial descrevendo os resultados do teste contra uma máquina Windows/SIS com a versão vulnerável do TPS e outra seção descrevendo os resultados obtidos ao testar contra uma máquina Windows/SIS com a proposta inicial de mitigação implementada.

É possível antecipar que a equipe do LARC conseguiu reproduzir o teste em laboratório, sendo possível montar uma partição Windows decifrada e explorar o seu conteúdo com a versão vulnerável, validando assim o método de reteste. Além disso, embora o resultado do teste em laboratório realizado na versão com a mitigação não tenha levado à decifração do disco, a principal razão deveu-se menos à efetiva mitigação da vulnerabilidade explorada do que a uma limitação do hardware utilizado. Especificamente, esbarrou-se em um limite de velocidade de leitura da memória RAM, o que dificulta o ataque de forma probabilística: na prática, reduz-se a chance do atacante conseguir obter a chave do BitLocker ao fazer apenas um dump parcial da memória em cada teste.

3.1. Máquina WIndows/SIS Vulnerável

Com a placa FPGA Screamer PCIe Squirrel carregada com o binário do PCILeech, a placa foi conectada à máquina Windows/SIS por meio da conexão PCIe. Antes de executar o comando de dump, deve-se realizar duas alterações na BIOS: (1) desabilitar a opção IOMMU e (2) desabilitar a opção AMD Secure Virtual Machine. Com ambas as opções desabilitadas, o Comando 12 é executado.

Comando 12 Comando para realizar o dump da memória RAM.

```
$ ./pcileech -force dump -min endereco1 -max endereco2
```

Realizando o dump de toda a memória RAM, há a garantia de que a chave do BitLocker está presente. Então, o Volatility é utilizado para encontrar chaves candidatas, lendo o arquivo bruto (.raw) retornado pelo PCILeech. O conteúdo desse arquivo pode ser verificado com o Comando 13.

Comando 13 Comando para procurar chaves candidatas no arquivo de dump.

```
$ python2 vol.py -f file.raw bitlocker --profile=Win10x64_19041 --dislocker /path/to
    /save/keys
```

Com as chaves candidatas encontradas, é necessário testá-las para observar se a abertura da partição com o Bitlocker é bem sucedida. Uma possibilidade para ajudar neste teste é o retorno do comando `bdeinfo`.

Comando 14 Padrão de chave utilizada no BitLocker.

```
$ bdeinfo /partition/SIS
```

Figura 1: Saída do volatility com as candidatas de chaves do BitLocker.

Sabendo-se o tipo de chave utilizada no BitLocker, pode-se testar as chaves em cada partição.

Comando 15 Comandos para testar as chaves encontradas pelo Volatility.

```
$ mkdir dislocker_mount
$ dislocker-fuse -V /path/to/partition -k key_name.fvek /path/to/dislocker_mount
```

Se a chave utilizada for a correta, será possível visualizar o conteúdo da partição.

Comando 16 Comandos para montar a partição do Bitlocker e visualizar seu conteúdo.

```
$ mkdir /mount
$ sudo mount -o loop,ro /path/to/dislocker_mount /path/to/mount
$ ls -lh /path/to/mount
```

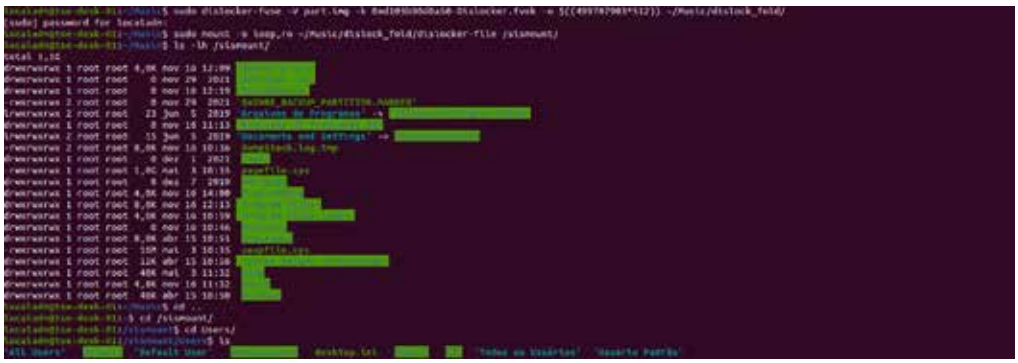


Figura 2: Chave BitLocker encontrada com sucesso, sendo possível visualizar o conteúdo da partição do SIS.

3.2. Teste em Laboratório

Antes do Teste de Confirmação, a equipe do LARC-USP recebeu duas máquinas iguais às usadas no TPS 2023. Em uma delas foi aplicada a versão do ambiente SIS com a mitigação do ataque.

A mitigação implementada consiste em um driver do SIS que, ao verificar a presença da configuração da BIOS que permite o ataque, leva a uma interrupção (”tela azul”) do Windows, impedindo a continuidade do ataque. Adicionalmente, o driver grava no registro do Windows a informação de que a configuração vulnerável está presente. Assim, mesmo que a configuração da BIOS seja restaurada, o driver continuará provocando um erro do sistema até que uma intervenção manual seja feita na máquina para restaurar o ambiente. Durante os testes realizados nas dependências do LARC, verificou-se que havia uma janela de tempo de aproximadamente 11s entre a digitação da chave de recuperação do BitLocker e a tela azul da mitigação.

Vale ressaltar que a chave de recuperação do bitlocker foi necessária para a instalação da versão com a mitigação no ambiente do laboratório, via software de clonagem de disco. A digitação da chave de recuperação ajudou a equipe nos testes, uma vez que ela delimitava mais claramente o momento inicial em que a chave do BitLocker era carregada em memória.

A conclusão dos testes foi de que, ao menos teoricamente, o ataque continua sendo possível com a mitigação inicial proposta. Porém, a mitigação reduz consideravelmente o intervalo de tempo disponível para o atacante, o que pode ser suficiente para inviabilizar o ataque dependendo do hardware utilizado. Em particular, nos testes realizados não foi possível encontrar a chave BitLocker após a mitigação inicial aplicada: com a janela de 11s e uma taxa de leitura da memória abaixo de 30 MB/s durante a maior do tempo do período vulnerável, foi possível capturar aproximadamente 1% da memória total da máquina. É possível diminuir o tamanho da memória RAM disponível para aumentar as chances de captura da chave BitLocker, mas a janela de aproximadamente 11 segundos disponível para realizar o dump torna-o mais difícil, em especial porque a chave BitLocker aparentemente é posicionada em endereços distintos a cada execução.

Por outro lado, é importante ressaltar que a mitigação inicial proposta diminui a chance de sucesso do ataque de forma inversamente proporcional à taxa de leitura da memória RAM pela FPGA. A Screamer PCIe Squirrel, segundo a documentação, pode atingir 190 MB/s. Então, durante 11 segundos, ela teria a capacidade de extrair 2090 MB da memória RAM. Portanto, caso a máquina faça uso de memórias de capacidades próximas a 2GB, o ataque apresentaria uma maior viabilidade. Além disso, um atacante com maiores recursos pode adquirir FPGAs de maior capacidade para facilitar o ataque. Por exemplo, a ZDMA [ufrisk 2024], que tem um custo aproximado de U$600, possui suporte ao PCILeech e pode realizar leituras com a taxa de 1 GB/s. Com essa velocidade, 11 GB poderiam ser extraídos da memória durante a janela vulnerável, representando 68.75% de 16 GB.

4. Teste de Confirmação

Durante o Teste de Confirmação, os investigadores da Polícia Federal conseguiram reconfigurar e otimizar o ambiente de testes para a captura da memória total da máquina em 2 execuções do ataque. Como resultado, a equipe conseguiu a captura da chave do Bitlocker na memória mesmo com a mitigação original implementada. Em vista dessa limitação da solução original, e após conversa com os investigadores da PF e também da equipe do LARC, da equipe responsável pelo módulo SIS implementou uma nova solução para mitigar o ataque com a PCILeech.

Na nova mitigação, caso uma das opções da BIOS seja desativada, possibilitando o ataque, o driver de subsistema responsável por verificar tal configuração apaga a chave do BitLocker localizada na placa-mãe da máquina. Este comportamento inutiliza a máquina em caso de alteração, sendo necessário possuir a chave de recuperação do BitLocker para restaurá-la. Assumindo que atacante não tenha acesso a tal chave, o ataque deve ser efetivamente mitigado na prática.

Os investigadores da Polícia Federal puderam testar esta nova versão com o apagamento da chave no BitLocker, que foi eficaz para impedir o ataque utilizando o PCILeech com as técnicas apresentadas.

5. Considerações Finais

Durante o Teste Público de Segurança de 2023, os investigadores da Polícia Federal foram capazes de extrair a chave BitLocker da máquina Windows/SIS. Isso foi feito com a combinação de um relaxamento de barreiras do sistema, com alteração de configurações na BIOS, e utilização de de uma placa FPGA ligada diretamente no barramento da máquina alvo. A equipe do LARC-USP reproduziu os testes internamente, no mesmo modelo de máquina e nas mesmas condições de hardware/software do TPS, e constatou a vulnerabilidade do ambiente.

Nos testes realizados pelo LARC com a versão atualizada do SIS, contendo a mitigação inicialmente proposta, o intervalo de tempo para o ataque foi reduzido para 11s. No ambiente de testes utilizado, isso permitia a captura de apenas 1% da memória RAM disponível antes que a mitigação interrompesse a máquina. Apesar de repetidas capturas terem sido feitas, a equipe do LARC não teve sucesso em identificar um chave do Bitlocker em nenhuma dessas capturas.

Durante o Teste de Confirmação, entretanto, a equipe da Polícia Federal obteve velocidades consideravelmente maiores de leitura da RAM do que aquelas observadas no ambiente de laboratório durante a avaliação da mitigação proposta. Como resultado, obtiveram sucesso na obtenção da chave do Bitlocker após algumas tentativas, a despeito da mitigação originalmente implementada. A mitigação foi então refinada durante o próprio Teste de Confirmação, passando a incluir o apagamento da chave do Bitlocker assim que configurações indevidas são encontradas na BIOS da máquina alvo. Esta versão refinada foi colocada em teste pelos investigadores da Polícia Federal, concluindo-se que ela deve dificultar consideravelmente ataques realizados com o PCILeech. Mais precisamente, a janela de vulnerabilidade passa a consistir apenas em 11s por máquina alvo, que seria inutilizada após eventual tentativa de execução do ataque.

Finalmente, caso julgado relevante, pode-se considerar como possível melhoria da mitigação a implementação de estratégias que reduzam a janela de tempo entre o ligamento da máquina e a execução da função de apagamento da chave do BitLocker. Em especial, a mitigação atual é executada por um driver do SIS, que é carregado apenas quando o sistema entra no ar. Assim, uma possibilidade de melhoria seria adiantar essa verificação para a etapa de inicialização da máquina, com o uso de bootloader modificado para realizar ações similares àquelas desse driver, antes de passar o controle para o bootloader do BitLocker. Embora essa não seja considerada uma melhoria crítica, ela pode aumentar a robustez do sistema ao: (1) reduzir o tamanho da janela de tempo do ataque, conforme mencionado; e (2) viabilizar uma dupla camada de verificação da correta configuração da BIOS, dificultando estratégias alternativas de ataques que porventura consigam desabilitar uma etapa de verificação, mas não ambas.

Referências

[openocd org 2008] openocd org (2008). openocd. https://github.com/openocd-org/openocd.

[Project 2008] Project, O. (2008). Openocd user's guide. https://openocd.org/doc/html/index.html.

[ufrisk 2017] ufrisk (2017). pcileech-fpga. https://github.com/ufrisk/pcileech-fpga.

[ufrisk 2024] ufrisk (2024). Lighting zdma - pcie to thunderbolt. https://github.com/ufrisk/pcileech-fpga/tree/master/ZDMA.

[volatilityfoundation 2020] volatilityfoundation (2020). volatility. https://github.com/volatilityfoundation/volatility.

Anexo A - flash_screamer_squirrel.cfg

```
adapter driver ftdi
transport select jtag
ftdi vid_pid 0x0403 0x6011
ftdi channel 0
ftdi layout_init 0x0098 0x008b
reset_config none

source [find cpld/xilinx-xc7.cfg]
source [find cpld/jtagspi.cfg]
adapter speed 10000

proc fpga_program {} {
global _CHIPNAME
virtex2 refresh xc7.pld
}

Init
jtagspi_init xc7.pld bscan_spi_xc7a35t.bit
jtagspi_program pcileech_squirrel_top.bin 0x0
fpga_program
shutdown
```

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

Laboratório de Arquitetura e Redes de Computadores

Relatório de Reteste - Bootloader/BIOS

Projeto: ToC-ToU na Mídia de Aplicação

Cliente: Tribunal Superior Eleitoral (TSE)

Autores: LARC - EPUSP

Data: 25 de maio de 2024

Sumário

Sumário Executivo **4**

1. Introdução **5**

2. Ambiente de Teste **6**
2.1. Sequência do ataque 6
2.2. Cópia do conteúdo da Mídia de Aplicação 7
2.3. Alterações nas configurações da BeaglePlay® 7
2.4. Alterações no *kernel* da BeaglePlay® 8
2.5. Compilação e passagem do novo *kernel* para a placa 9
2.6. Alterações no *hardware* da BeaglePlay® 9
2.7. Montagem e Resultados dos Testes pré-Mitigações 10

3. Testes pós-mitigações **13**
3.1. Testes no LARC-EPUSP 13
3.2. Teste de Confirmação 16

4. Conclusões **17**

Lista de Figuras

1. Comparação visual entre as Placas Beagle utilizadas 6
2. Alteração no *driver* "`f_mass_storage`" (Reprodução: Própria) 8
3. Placa BeaglePlay®, com o diodo em curto sinalizado (Reprodução: Própria) 10
4. Equipamentos utilizados para a realização do ataque (Reprodução: Própria) 10
5. Montagem completa do circuito de ataque (Reprodução: Própria) 11
6. Alteração da cadeia de caracteres na tela da UE2020 (Reprodução: Própria) 12
7. Tela de depuração da BeaglePlay® (Reprodução: Própria) 12
8. Lista de strings presentes no *bootloader* (Reprodução: Própria) 13
9. Alteração feita no `f_mass_storage` no *kernel* da BeaglePlay® (Reprodução: Própria) . 13
10. Trechos de log da BeaglePlay® (Reprodução: Própria) 14
11. Trechos de log da BeaglePlay®, com o novo bootloader (Reprodução: Própria) 15
12. Alteração feita no `f_mass_storage` no *kernel* da BeaglePlay® (Reprodução: Própria) . 15
13. Trechos de log da BeaglePlay®, com o ataque interrompido - Exemplo 1 (Reprodução: Própria) 16
14. Trechos de log da BeaglePlay®, com o ataque interrompido - Exemplo 2 (Reprodução: Própria) 16

Sumário Executivo

Durante o Teste Público de Segurança de 2023, os investigadores da Polícia Federal identificaram um problema do tipo tipo ToC-Tou (*Time-of-Check, Time-of-Use*, ou ”Tempo de Verificação, Tempo de Uso”) no boot pela Mídia de Aplicação de uma urna do modelo 2020. Por meio de uma placa BeaglePlay® ligada na porta USB da urna, a Mídia de Aplicação foi emulada, permitindo aos investigadores a interceptação e alteração de dados da mídia emulada antes de enviá-los à urna. Com isso, os investigadores puderam efetivamente inserir instruções que eram executadas pela urna durante a sua inicialização.

Durante o TPS, a falha foi identificada como um problema na BIOS da máquina. Este problema foi então corrigido pela Positivo no início de 2024. Entretanto, após a correção ser disponibilizada à equipe do LARC, esta última teve sucesso em reproduzir o ataque tanto em uma urna sem correção como em uma corrigida. Após investigação conjunta das equipes do LARC, SEVIN e Positivo, identificou-se que uma vulnerabilidade similar ocorria também no bootloader da urna, i.e., que ele tinha um comportamento suscetível a ToC-Tou análogo àquele apresentado pela BIOS. Uma vez identificado tal problema, ele também foi corrigido e retestado pela equipe do LARC, que pode atestar a efetividade da solução implementada.

Como esperado, no Teste de Confirmação os investigadores da Polícia Federal não obtiveram sucesso em executar o mesmo ataque de inserção de código observado durante o TPS, e puderam verificar a efetividade das correções na BIOS e no bootloader. Mais precisamente, eles identificaram um único arquivo vulnerável a ataques do tipo ToC-Tou, sem contudo ter obtido sucesso em usá-lo para a inserção de códigos como anteriormente, ou realizar qualquer outro tipo de ação relevante do ponto de vista de segurança.

1. Introdução

O relatório descreve o reteste de um ataque baseado na exploração de uma vulnerabilidade do tipo ToC-ToU(*Time-of-Check, Time-of-Use*, ou ”Tempo de Verificação, Tempo de Uso”) durante a inicialização de uma urna modelo UE2020 por meio da mídia de aplicação. O ataque, que faz uso de de uma placa BeaglePlay®, consiste em emular uma Mídia de Aplicação nessa placa, tornando possível a interceptação de dados e sua alteração no *buffer* de leitura. Para validar a existência de vulnerabilidade dessa natureza, a equipe de investigadores analisou os logs do dispositivo e notou que o código correspondente ao *bootloader* era lido duas vezes. A hipótese levantada foi, então, que a primeira leitura era feita para verificação do seu conteúdo, enquanto a segunda estava associada a sua execução. Essa hipóteses foi então confirmada por meio da BeaglePlay®, que foi configurada para ler o *buffer* e, ao detectar a passagem de uma determinada sequência de bytes na fase de execução pós verificação, realizava uma alteração dos dados. Como resultado, era mostrado um texto arbitrário na tela da UE2020.

Para sanar o problema, inicialmente foi proposta uma mitigação no nível da BIOS, que passou então a ter um comportamento atômico na sua interação com o bootloader: a sua verificação e execução passaram a acontecer na memória RAM, eliminando-se a sua dupla leitura a partir da mídia de aplicação. A mitigação foi então apresentada à equipe do LARC, para validação de sua efetividade. Nos testes realizados no laboratório, entretanto, observou-se que ainda era possível realizar um ataque similar mesmo após a atualização da BIOS contendo a mitigação inicialmente proposta. Foram então realizadas uma série de reuniões entre as equipes do LARC, SEVIN (TSE) e Positivo para identificar a origem do problema. Após algumas interações, conclui-se que, embora a mitigação no nível de BIOS fosse efetiva, ainda eram feitas leituras repetidas na mídia de aplicação após a carga do *bootloader*, sendo esse o elemento responsável pelo problema. De fato, a equipe da SEVIN já havia aventado em relatório interno sobre essa possível vulnerabilidade no nível do *bootloader*, atingindo-se então um consenso sobre a necessidade de um passo adicional para mitigar o achado. Foi então realizado um trabalho conjunto pela SEVIN e Positivo para especificar e implementar uma solução, a qual foi novamente testada pela equipe do LARC, desta vez comprovando-se a sua efetividade.

Durante o Teste de Confirmação, a mitigação foi novamente posta à prova pela equipe da Polícia Federal. O que se percebeu é que o conteúdo considerado sensível na mídia de aplicação era carregado e verificado apenas uma vez, impedindo que um ataque de ToC-ToU fosse efetuado para a execução de código arbitrário. A mitigação final foi, então, considerada suficientemente e satisfatória pela equipe de investigadores.

Este documento encontra-se organizado da seguinte maneira. O Capítulo 2 documenta a reprodução dos testes feitos pela equipe do LARC. O capítulo 3 descreve os resultados dos testes após as mitigações.

2. Ambiente de Teste

Esta seção tem como objetivo detalhar os passos realizados pelos pesquisadores do LARC para a construção do ambiente de testes em questão, facilitando eventual reprodução futura.

Um requisito para o funcionamento do ataque realizado pela Polícia Federal consiste em fazer com que um dispositivo computacional sob seu controle seja reconhecido como uma mídia externa de aplicação pela urna eletrônica. Para isso, foi utilizada uma placa do tipo BeagleBoard®, um equipamento de código aberto, projetado para simplificar o processo de adição de sensores, atuadores, indicadores, interfaces humanas e conectividade a um sistema embarcado.

Com o objetivo de reproduzir os testes em ambiente de laboratório, o LARC adquiriu alguns equipamentos do modelo BeaglePlay®, uma versão mais moderna dos BeagleBoard®-xM utilizados pela Polícia Federal durante a edição 2023 do Teste Público de Segurança. Embora similares, o BeaglePlay® tem um processador mais rápido e menos portas USB do que o BeagleBoard®-xM, que não foi encontrado para aquisição em sites especializados. A Figura 1 mostra ambos os dispositivos.

(a) BeaglePlay® (Créditos: BeagleBoard.org)

(b) BeagleBoard-xM® (Créditos: DigiKey)

Figura 1: Comparação visual entre as Placas Beagle utilizadas

2.1. Sequência do ataque

Para realização do ataque após a familiarização com a placa BeaglePlay®, a equipe do LARC realizou a seguinte sequência de passos:

1. Buscar o módulo responsável no kernel pela emulação de um dispositivo *mass storage*;
2. Realizar uma alteração no nome do dispositivo para ver se ele aparecia alterado no `dmesg` da UE2020;
3. Buscar o local onde ocorria a transmissão de dados via USB;

4. Copiar todo o conteúdo da mídia de carga para um arquivo de imagem. Este arquivo foi colocado na BeaglePlay® para que o dispositivo atuasse como a própria mídia de aplicação na interação com a urna;
5. Programar uma rotina que identificava uma determinada sequência de caracteres que aparecia na tela da UE2020 durante o boot;
6. Alterar a rotina para que substituísse a cadeia de caracteres quando detectada no *buffer* de leitura, enviando um novo texto a ser mostrado na tela da UE2020.

2.2. Cópia do conteúdo da Mídia de Aplicação

Após a geração de uma mídia de carga no GEDAI, foi feita uma cópia do seu conteúdo para um arquivo de imagem, por meio do comando "`dd`":

```
# dd if=/dev/sdX of=file.img obs=4096
```

onde `/dev/sdX` representa o dispositivo da mídia. O arquivo "file.img" foi utilizado em momento posterior, para a configuração da BeaglePlay®.

2.3. Alterações nas configurações da BeaglePlay®

Com o intuito de evitar possíveis conflitos com a UE2020, módulos legados foram desativados. Para isso, executou-se o seguinte comando

```
# vi /usr/bin/bb-start-usb-gadgets
```

Também foi comentada a linha que contém "`/usr/bin/bb-start-acm-ncm-rndis-old-gadget`". Em seguida, a placa foi reinicializada.

Também foi necessário fazer com que a BeaglePlay® se comportasse como uma Mídia de Aplicação. Isso é feito utilizando o seguinte comando:

```
# modprobe g_mass_storage file=file.img idVendor="0x1005" idProduct="0xb168"
iSerialNumber="1900152DB0CE4110" iManufacturer="" stall=0 cdrom=0 nofua=1
removable=1 ro=0
```

Uma observação: em caso de desligamento ou reinicialização da placa, este comando deve ser efetuado novamente.

2.4. Alterações no *kernel* da BeaglePlay®

A versão do *kernel* utilizada foi a 5.10.168, que já é padrão na placa. Embora a BeaglePlay® possua um desempenho aceitável, a compilação do *kernel* nela demora cerca de 4 horas, o que motivou a realização da compilação em uma outra máquina.

No computador onde foi feito o *build* do kernel alterado, foram necessários os seguintes comandos:

```
# apt update
# apt install git gcc-aarch64-linux-gnu g++-aarch64-linux-gnu libncurses-dev
libelf-dev flex libssl-dev xz-utils bison build-essential debhelper fakeroot
```

Também foi necessário clonar o repositório do *kernel* em questão:

```
# git clone --depth 1 --branch v5.10.168-ti-arm64-r111
https://openbeagle.org/beagleboard/linux.git
```

A única alteração feita foi no arquivo `f_mass_storage.c`, como pode ser visto na Figura 2. Especificamente, as linhas 231 e 232 foram alteradas apenas para verificação, enquanto nas linhas restantes foi implementada a rotina de leitura de *buffer*. Assim que o texto "Validando Kernel" é encontrado pela BeaglePlay®, um contador genérico sinaliza na tela de depuração (`dmesg`) o momento em que essa sequência de caracteres foi encontrada. Esse valor foi utilizado na linha 720 para realizar a substituição do texto, já que o período da execução não poderia ser antes da verificação da integridade do *bootloader*.

Por fim, é mostrado no `dmesg` que a cadeia de caracteres "Validando Kernel" é alterada (linha 721) pelo conteúdo presente na função da linha 722 (neste caso, "LARC/Sembei 2024").

```
231   #define FSG_DRIVER_DESC "Mass Storage Function Sembei"
232   #define FSG_DRIVER_VERSION "2024/04/06"
.
.
.
714         if (nread > 0) {
715             char * offset_target = strnstr(bh->buf, "Validando Kernel", nread);
716             static int occur_count = 0;
717             if (offset_target != NULL) {
718                 occur_count++;
719                 pr_debug("Sembei: Found Validando count=%d...\n", occur_count);
720                 if (occur_count > 2) {
721                         pr_debug("Sembei: Changing string\n");
722                         strncpy(offset_target, "LARC/Sembei 2024", 16);
723                 }
724             }
725         }
```

Figura 2: Alteração no *driver* "`f_mass_storage`" (Reprodução: Própria)

2.5. Compilação e passagem do novo *kernel* para a placa

Como previamente mencionado, realizar a compilação na própria BeaglePlay® demanda muito tempo e, por isso, foi necessário um *cross compiling* em outro computador.

Primeiramente, o comando abaixo foi realizado na placa, e o arquivo .config gerado foi movido para a máquina na qual ocorrerá a compilação do *kernel*:

```
# zcat /proc/config.gz > .config
```

No computador com o *source* do *kernel*, esse arquivo .config foi redirecionado para o diretório "5.10.168-ti-arm64-r111/". Em seguida foi executado o comando a seguir, dentro desta mesma pasta:

```
# make olddefconfig
```

Por fim,executou-se o seguinte comando dentro do repositório clonado do *kernel*:

```
# cd ..
# make -j<x> ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- -C ./v5.10.168-ti-
arm64-r111  KDEB_PKGVERSION=<v> bindeb-pkg
```

onde <x> representa o número de *threads* a serem utilizadas (para o ataque, foram utilizadas 12 *threads*) e <v> é um parâmetro para controle de versionamento (no caso, foi utilizado o valor "16sembei").

O comando gera um arquivo .deb, que foi movido para a BeaglePlay® e instalado em seguida. Finalmente, o *kernel* estava pronto para ser instalado, por meio do comando:

```
# cd ..
# dpkg -i linux-image-5.10.168+_<v>_arm64.deb
```

A placa foi então reinicializada após a instalação.

2.6. Alterações no *hardware* da BeaglePlay®

A única alteração realizada no *hardware* diz respeito à alimentação da placa. A entrada USB-C da BeaglePlay® seria utilizada para a conexão com a UE2020, no local onde originalmente estaria a Mídia de Aplicação. Contudo, mesmo que essa entrada possa servir como alimentação, observou-se que o tempo necessário para o boot da placa era superior ao tempo de boot da urna. Logo, percebe-se a necessidade de alimentar a BeaglePlay® externamente, para que ele estivesse operacional antes da própria urna.

Para isso, foi utilizado um pequeno pedaço de fio para realizar o curto em um dos diodos da placa (vide Figura 3). Este diodo era responsável por garantir uma saída de 5V de um *pin socket*; assim, para ser utilizado como entrada, foi necessário fazer esta pequena alteração.

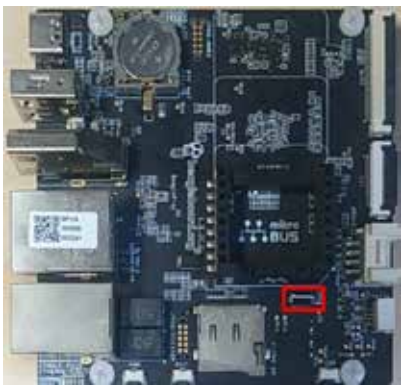


Figura 3: Placa BeaglePlay®, com o diodo em curto sinalizado (Reprodução: Própria)

2.7. Montagem e Resultados dos Testes pré-Mitigações

Com todas as alterações e configurações efetuadas, chegou-se ao momento em que as conexões entre a placa e a urna estão prontas para serem realizadas. Para isto, foram utilizados (vide Figura 4):

1. 2 fios *jumpers* macho-fêmea;
2. Power Bank 20.000mah (5V, 3.7A);
3. Módulo Adaptador USB Macho 2.0 para DIP;
4. Cabo USB-C para USB-A;
5. Cabo USB-A Fêmea para USB-A Macho, **com a alimentação cortada**.

O último item foi utilizado porque não havia um Cabo USB-C para USB-A disponível para que a alimentação fosse cortada. Este corte na alimentação foi realizado para evitar curtos com o *hardware* da urna, permitindo apenas a passagem de dados.

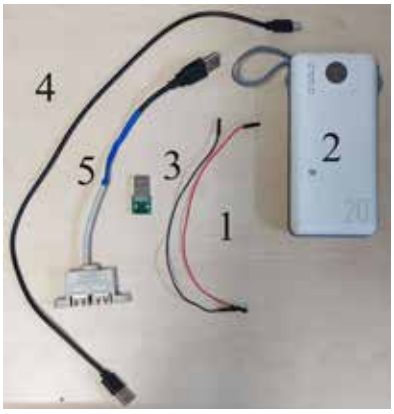


Figura 4: Equipamentos utilizados para a realização do ataque (Reprodução: Própria)

O processo de montagem consistiu em:

1. Conectar os terminais macho dos fios *jumpers* aos *pin sockets* correspondentes ao GND e 5V na placa BeaglePlay®;
2. Conectar o módulo USB ao *powerbank*;
3. Conectar os terminais fêmea dos fios *jumpers* aos *pin headers* correspondentes ao GND e 5V no módulo USB. Chegando neste ponto, a placa deve começar a inicializar;
4. Conectar o cabo USB-C na entrada da BeaglePlay®;
5. Conectar o terminal USB-A do cabo anterior ao cabo com a alimentação cortada;
6. Conectar o cabo com a alimentação cortada na entrada USB da Mídia de Aplicação da UE2020.

A Figura 5 mostra a montagem completa do circuito.

Figura 5: Montagem completa do circuito de ataque (Reprodução: Própria)

Com a montagem preparada, a placa é inicializada e configurada para se comportar como uma Mídia de Aplicação.

A seguir, liga-se a urna. Para analisar a depuração na BeaglePlay®, foi necessário usar o comando "`dmesg -w`" e um display HDMI ligado diretamente na placa. Os resultados da reprodução bem-sucedida do ataque em uma urna vulnerável encontram-se nas Figuras 6 e 7.

Figura 6: Alteração da cadeia de caracteres na tela da UE2020 (Reprodução: Própria)

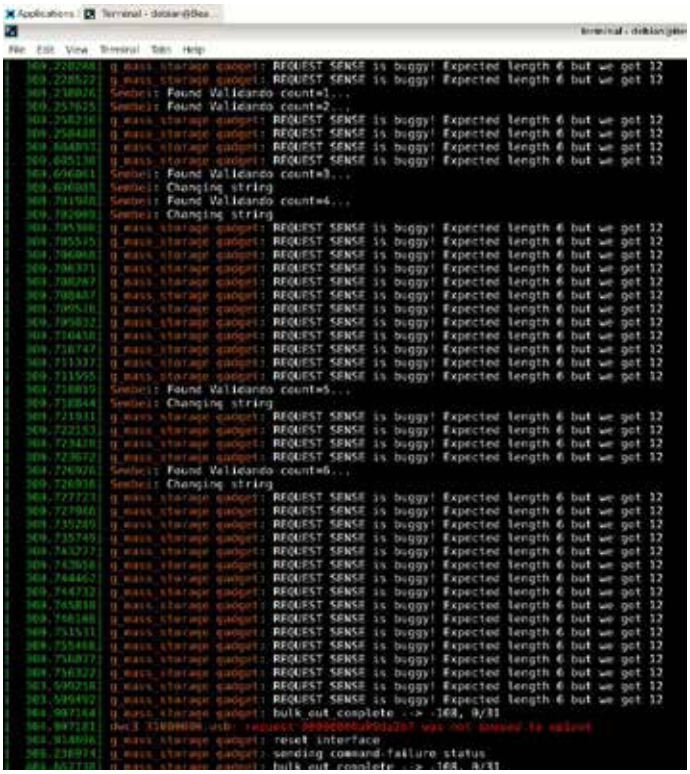


Figura 7: Tela de depuração da BeaglePlay® (Reprodução: Própria)

3. Testes pós-mitigações

Este capítulo discute os resultados dos testes realizados após a proposta de mitigação pelas equipes do TSE e Positivo, bem como as interações realizadas para chegar nas versões finais dessas mitigações.

3.1. Testes no LARC-EPUSP

Para os testes da mitigação do ataque foi necessário atualizar uma urna modelo UE2020. Para tanto, foi disponibilizada uma imagem do sistema fornecida pela Positivo, com atualizações do firmware da BIOS, MSE e de alguns periféricos internos.

Verificou-se que a mitigação inicialmente proposta para corrigir a ocorrência de ToC-ToU conduzida pela BIOS foi efetiva para o seu propósito. No entanto, percebeu-se a possibilidade de realização de um ataque de ToC-ToU durante a execução do boot, tanto em uma urna UE2020 atualizada como em uma urna UE2022 também atualizada. Para a investigação da origem do problema, o código para reprodução do ataque da Polícia Federal foi modificado para não mais alterar as mensagens após serem encontradas. Em vez disso, ele passou a apenas indicar quando os caracteres alvo eram encontrados (listados na Figura 8), bem como mostrar os respectivos LBA (*Logic Block Address*) e Offset no arquivo que estavam sendo requisitados na leitura (conforme Figura 9).

```
336
337  #define PHRASE_QTTY 12
338  const char * phrases[PHRASE_QTTY] = {
339      "Alocando g_ue_data",
340      "Loading linux",
341      "Detectando modelo do urna:",
342      "Carregando tipo de SO",
343      "Carregando numero de serie",
344      "Carregando crypto table",
345      "Carregando random number",
346      "Carregando kernel",
347      "Carregando chave de kernel",
348      "Decodificando kernel",
349      "Validando kernel",
350      "pronto!"
351  };
352
```

Figura 8: Lista de strings presentes no *bootloader* (Reprodução: Própria)

```
758
759          if (nread>0) {
760              pr_debug("Sembei: lba=0x%08x; file_offset=0x%016llx\n", lba, file_offset);
761              int phrase_count;
762              for(phrase_count=0; phrase_count<PHRASE_QTTY; phrase_count++) {
763                  char  * offset_target = strnstr(bh->buf, phrases[phrase_count], nread);
764                  if ( offset_target != NULL) {
765                      pr_debug("Sembei: Found: %s\n", phrases[phrase_count]);
766                  }
767              }
768          }
769
```

Figura 9: Alteração feita no `f_mass_storage` no *kernel* da BeaglePlay® (Reprodução: Própria)

Com esta alteração, e após diversas conversas e interações com as equipes da SEVIN e Positivo, identificou-se que o ataque realizado pela equipe do LARC era possível devido a uma vulnerabilidade de ToC-ToU remanescente no bootloader da urna. A equipe da Positivo elaborou então uma mitigação provisória para mitigar a vulnerabilidade observada que permitia ataques de ToC-ToU via Bootloader. Ao serem testadas no LARC, foi possível comprovar a efetividade da solução, sendo frustrado o ataque originalmente relatado pela equipe do laboratório e também novas tentativas de adulteração de posições de memórias contendo instruções.

Usando como base as alterações efetuadas pela Positivo, e após a confirmação da efetividade da correção em laboratório, a SEVIN efetuou uma correção no bootloader oficial para ser carregado na urna. Uma imagem da Mídia de Aplicação com esta correção nos enviada ao LARC pela Sevin, e foram então repetidos os testes para confirmar a correção. Especificamente, a primeira ação foi efetuar o boot da urna para apenas registrar os acessos aos blocos da imagem da mídia, bem como o momento em que são identificadas as mensagens na lista de busca. O resultado são os trechos de log mostrados na Figura 10.

```
1  [ 4036.065287] Sembei: lba=0x00000000; file_offset=0x0000000000000200
2  [ 4036.066166] Sembei: lba=0x00000001; file_offset=0x0000000000000400
3  [ 4036.067069] Sembei: lba=0x00000002; file_offset=0x0000000000004400
4  [ 4036.072440] Sembei: lba=0x80776fff; file_offset=0x0000000000ece00000
5  [ 4036.073538] Sembei: lba=0x00000002; file_offset=0x0000000000004400
6  [ 4036.093272] Sembei: lba=0x00000002; file_offset=0x0000000000004400
7  [ 4036.109318] Sembei: lba=0x00000800; file_offset=0x0000000000100200
8  [ 4036.110186] Sembei: lba=0x00000840; file_offset=0x0000000000108800
9  [ 4036.111454] Sembei: lba=0x00000800; file_offset=0x0000000000100200
10 [ 4036.112865] Sembei: lba=0x00000800; file_offset=0x0000000000100200
11 [ 4036.114677] Sembei: lba=0x00003801; file_offset=0x0000000000700400
12 [ 4036.115536] Sembei: lba=0x00003841; file_offset=0x0000000000708a00
13 [ 4036.116803] Sembei: lba=0x00003801; file_offset=0x0000000000700400
```

Figura 10: Trechos de log da BeaglePlay® (Reprodução: Própria)

Com o novo bootloader, notou-se que as mensagens eram lidas apenas uma vez, copm eventuais duplicidades ocorrendo apenas em razão da dupla ocorrência das mensagens no sistema (vide Figura 11).

```
125  [ 4641.254378] Sembei: lba=0x00002a4c; file_offset=0x0000000000555800
126  [ 4641.258935] Sembei: lba=0x00002a4c; file_offset=0x0000000000559800
127  [ 4641.258990] Sembei: Found: Alocando g_ue_data
128  [ 4641.259730] Sembei: Found: Carregando tipo de SO
129  [ 4641.259777] Sembei: Found: Carregando numero de serie
130  [ 4641.259830] Sembei: Found: Carregando crypto table
131  [ 4641.259881] Sembei: Found: Carregando random number
132  [ 4641.259933] Sembei: Found: Carregando kernel
133  [ 4641.259986] Sembei: Found: Carregando chave de kernel
134  [ 4641.260041] Sembei: Found: Decodificando kernel
135  [ 4641.260098] Sembei: Found: Validando kernel
136  [ 4641.260144] Sembei: Found: pronto!
137  [ 4641.260642] Sembei: lba=0x00002acc; file_offset=0x000000000055d800
138  [ 4641.264886] Sembei: lba=0x00002acc; file_offset=0x0000000000561800
139  [ 4641.270642] Sembei: lba=0x00002acc; file_offset=0x0000000000565800
140  [ 4641.276526] Sembei: lba=0x00002acc; file_offset=0x0000000000569800
141  [ 4641.281432] Sembei: lba=0x00002b4c; file_offset=0x000000000056d800
142  [ 4641.285665] Sembei: lba=0x00002b4c; file_offset=0x0000000000571800
143  [ 4641.289942] Sembei: lba=0x00002b4c; file_offset=0x0000000000575800
144  [ 4641.294687] Sembei: lba=0x00002b4c; file_offset=0x0000000000579800
145  [ 4641.299858] Sembei: lba=0x00002bcc; file_offset=0x000000000057d800
146  [ 4641.300028] Sembei: Found: Alocando g_ue_data
147  [ 4641.300888] Sembei: Found: Carregando tipo de SO
148  [ 4641.301033] Sembei: Found: Carregando numero de serie
149  [ 4641.301235] Sembei: Found: Carregando crypto table
150  [ 4641.301387] Sembei: Found: Carregando random number
151  [ 4641.301536] Sembei: Found: Carregando kernel
152  [ 4641.301689] Sembei: Found: Carregando chave de kernel
153  [ 4641.301842] Sembei: Found: Decodificando kernel
154  [ 4641.301998] Sembei: Found: Validando kernel
155  [ 4641.302121] Sembei: Found: pronto!
156  [ 4641.302206] Sembei: lba=0x00002bcc; file_offset=0x0000000000581800
157  [ 4641.306422] Sembei: lba=0x00002bcc; file_offset=0x0000000000583800
```

Figura 11: Trechos de log da BeaglePlay®, com o novo bootloader (Reprodução: Própria)

Em seguida, foi testado o boot com modificações nas mensagens, como no ataque original, modificando-se dados tanto na sua primeira ocorrência como em eventuais ocorrências posteriores, de forma alternada (vide exemplo na Figura 12).

```
759         if (nread>0) {
760             char  * offset_target = strnstr(bh->buf, "Validando kernel", nread);
761             static int occur_count = 0;
762             if ( offset_target != NULL) {
763                 occur_count++;
764                 pr_debug("Sembei: Found Carregando count=%d lba=0x%08x file_offset=0x%016llx\n", occur_count, lba, file_o
765
766                 if (occur_count==1) {
767                     pr_debug("Sembei: Changing string\n");
768                     strncpy(offset_target, "LARC/Sembei 2024", 16);
769                 }
770
771             }
772
```

Figura 12: Alteração feita no `f_mass_storage` no *kernel* da BeaglePlay® (Reprodução: Própria)

O resultado é que, contrariamente ao observado em testes anteriores, os ataques não foram bem-sucedidos: sempre que era feita uma modificação, o bootloader interrompia o processo de carga, conforme ilustram as Figuras 13 e 14.

Figura 13: Trechos de log da BeaglePlay®, com o ataque interrompido - Exemplo 1 (Reprodução: Própria)

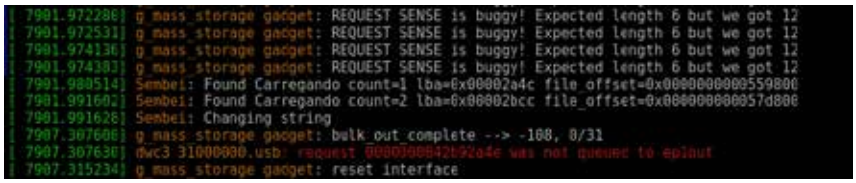


Figura 14: Trechos de log da BeaglePlay®, com o ataque interrompido - Exemplo 2 (Reprodução: Própria)

3.2. Teste de Confirmação

No Teste de Confirmação 2024, os investigadores da Polícia Federal identificaram que as vulnerabilidades de ToC-ToU usadas previamente tinham sido corrigidas, não sendo mais possível inserir código arbitrário nos mesmos elementos.

Por outro lado, ao investigar mais detalhadamente a versão atualizada do sistema, eles identificaram um arquivo de configuração suscetível a ataques de ToC-ToU, ao ser lido mais de uma vez sem que fosse repetida sua verificação. A despeito disso, e após diversas tentativas, percebeu-se que a interceptação deste arquivo não permitiria a execução de ações indevidas no sistema, em particular pela ausência de qualquer ponto nesse arquivo que pudesse ser tratado como instrução executável. Essa conclusão foi atingida após a consideração de diversos cenários, incluindo a eventual possibilidade de um teste de *buffer overflow* – hipótese descartada após análise do código fonte, durante a qual foi possível perceber que o *buffer* era delimitado e, portanto, não seria suscetível a ataques dessa natureza.

Ao final do Teste de Confirmação e exauridas as hipóteses de eventuais frentes de ataque, os investigadores da Polícia Federal chegaram a resultados similares àqueles obtidos pela equipe do LARC: de que a mitigação apresentada mostrou-se adequada. Desta forma, os investigadores deram-se por satisfeito com os experimentos realizados.

4. Conclusões

A mitigação inicialmente proposta para corrigir a ocorrência de ToC-ToU conduzida pela BIOS foi efetiva para o seu propósito. No entanto, em laboratório, foi percebido um problema de ToC-ToU não provocado pela BIOS, mas pelo próprio bootloader que carregaria seções de dados da mídia de aplicação em tempo de execução – problema não coberto pela mitigação na BIOS em si. Uma vez identificado o problema, foi possível, de forma colaborativa, descobrir as suas origens problema e implementar uma solução cuja efetividade foi verificada pela equipe do LARC em laboratório.

As mitigações apresentadas foram então colocadas à prova no Teste de Confirmação, para análise da equipe de investigadores da Polícia Federal. Como seria esperado, eles não tiveram sucesso em executar código arbitrário na urna por meio da exploração de técnicas de ToC-ToU. Mais especificamente, o único ponto identificado que seria potencialmente vulnerável a esse tipo de ataque consistia em um arquivo de configuração, o qual não era validado em todas as ocasiões de sua leitura. Entretanto, após diversos testes e hipóteses, não foram identificadas possibilidades de ataque envolvendo eventual modificação desse arquivo em um ataque de ToC-ToU. Portanto, embora seja relevante considerar a possibilidade de aprimorar os mecanismos envolvendo a leitura desse arquivo, pode-se considerar que a mitigação atual apresentada pelo TSE é satisfatória e suficiente para eliminar tentativas de ataque na prática.

7.22 Anexo V – Res.-TSE n. 23.673/2021

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

RESOLUÇÃO Nº 23.673, DE 14 DE DEZEMBRO DE 2021.

Dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das suas atribuições legais e regimentais,

RESOLVE:

Art. 1º Os procedimentos de fiscalização e auditoria do sistema eletrônico de votação serão regidos pelas disposições desta Resolução.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos desta Resolução e de suas regulamentações, aplicam-se as seguintes definições:

I - assinatura digital: é uma forma eletrônica de garantir a autenticidade de um documento ou sistema. Para isso, são utilizadas operações matemáticas com algoritmos de criptografia assimétrica que atestam sua origem. A criptografia assimétrica faz uso de pares de chaves: chaves públicas, que podem ser amplamente disseminadas; e chaves privadas, que são conhecidas apenas pelo proprietário;

II - auditoria: exame sistemático sobre o funcionamento de softwares, que averigua se estão implementados de acordo com as normas legais, e procedimentos, para aferir suas conformidades;

III - Boletim de Urna (BU): documento digital ou impresso que contém os resultados de uma seção eleitoral apurados pela urna eletrônica;

IV - cadeia de custódia: no contexto legal, refere-se à documentação cronológica ou histórica que registra a sequência de custódia, controle, transferência, análise e disposição de evidências físicas ou eletrônicas;

V - Cerimônia de Assinatura Digital e Lacração dos Sistemas: cerimônia constituída para se cumprir o estabelecido no § 2º do art. 66 da Lei nº 9.504/1997 (https://www.planalto.gov.br/ccivil_03/leis/l9504.htm#art66) , ocasião em que os sistemas eleitorais são apresentados às entidades fiscalizadoras, na forma de programas-fonte e executáveis, e, após apresentação e conferência, assinados e lacrados;

VI - compilação: ato de criar um arquivo que será executado por um computador, a partir da tradução dos arquivos com código-fonte (escritos em linguagem de alto nível, compreensível por humanos) para uma linguagem de máquina;

VII - inspeção: ato de examinar algo com o fim de verificar seu estado ou funcionamento;

VIII - fiscalização: ato de verificar se algo está ocorrendo como fora previsto, ou seja, em conformidade;

IX - lacração dos sistemas: procedimento executado na Cerimônia de Assinatura Digital e Lacração dos Sistemas que consiste na gravação dos programas assinados em mídia não regravável e em posterior acondicionamento desta em envelope assinado fisicamente e guardado em cofre do Tribunal Superior Eleitoral (TSE);

X - lacração das urnas: procedimento executado na Cerimônia de Preparação de Urnas que consiste em colocar o lacre físico nas interfaces de conexão dos dispositivos externos de acesso da urna e seu gabinete;

XI - Registro Digital do Voto (RDV): arquivo gerado pela urna eletrônica, no qual os votos são gravados separados, por cargo, e ordenados aleatoriamente;

XII - resumo digital (hash): pequena sequência de caracteres gerada por um cálculo matemático a partir de um conjunto de dados (arquivos, relatórios), que permite identificá-los de forma inequívoca. Qualquer alteração no arquivo original implica a geração de novo resumo digital;

XIII - sistemas eleitorais: programas de computador relacionados no art. 3º desta Resolução que automatizam o processo eleitoral e são executados tanto em computadores quanto nas urnas eletrônicas;

XIV - tabelas de correspondência: instrumento de segurança do processo eleitoral que consiste na associação entre determinada seção e a urna preparada para votação especificamente nesta seção;

XV - Teste de Autenticidade dos Sistemas Eleitorais: evento de auditoria de verificação de autenticidade dos sistemas eleitorais instalados nas urnas eletrônicas, a ser realizado no dia da votação;

XVI - Teste de Integridade das Urnas Eletrônicas: evento de auditoria de verificação de funcionamento das urnas eletrônicas em condições normais de uso, previsto no § 6º do art. 66 da Lei nº 9.504/1997 (https://www.planalto.gov.br/ccivil_03/leis/l9504.htm#art66) ; e

XVII - Teste Público de Segurança (TPS): evento permanente do calendário da Justiça Eleitoral (JE), que visa aprimorar os sistemas eleitorais, mediante a participação e colaboração de especialistas, na busca por problemas ou fragilidades que, uma vez identificados, serão resolvidos antes da realização das eleições.

Art. 3º Serão fiscalizados, auditados, assinados digitalmente, lacrados e verificados os seguintes sistemas eleitorais:

I - Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE): sistema responsável por gerar as mídias de carga, de votação, de resultado e de ativação de aplicativos da urna, além de receber e enviar as correspondências para o Sistema de Gerenciamento da Totalização;

II - Sistema de Gerenciamento da Totalização (Sistot): conjunto de programas que tem como objetivo principal acompanhar os recebimentos e gerenciar as totalizações dos resultados das eleições a partir dos arquivos processados pelo Receptor de Arquivos de Urna (RecArquivos);

III - Transportador de Arquivos: sistema responsável pela transmissão dos arquivos da urna eletrônica para a base de dados da JE;

IV - Informação de Arquivos de Urna (InfoArquivos): sistema responsável por fornecer ao Transportador de Arquivos a situação dos arquivos enviados e recebidos na base de dados da JE;

V - JE-Connect: ferramenta que viabiliza a transmissão do Boletim de Urna diretamente de alguns locais de votação, por meio de um canal privado, garantindo agilidade na totalização dos votos, sem comprometimento da segurança;

VI - Receptor de Arquivos de Urna (RecArquivos): sistema responsável por receber os pacotes gerados pelo Transportador de Arquivos e colocá-los à disposição para serem consumidos pelo Sistema de Gerenciamento da Totalização (Sistot);

~~VII - Votação, Justificativa Eleitoral, Apuração da Urna Eletrônica e demais aplicativos da urna eletrônica (Ecossistema da Urna): conjunto de programas executados na urna eletrônica que permite a escolha do voto, a justificativa de não comparecimento para votar, a apuração de resultados da seção eleitoral, entre outras funcionalidades; e~~

VII - Votação, Apuração da Urna Eletrônica e demais aplicativos da urna eletrônica (Ecossistema da Urna): conjunto de programas executados na urna eletrônica que permite a escolha do voto, a justificativa de não comparecimento para votar, a apuração de resultados da seção eleitoral, entre outras funcionalidades; (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

VIII - Uenux - sistema operacional e de segurança da urna: distribuição Linux desenvolvida por equipe técnica do TSE para uso nas urnas eletrônicas; é composto por bootloader, kernel do Linux, drivers, bibliotecas e aplicativos.

Parágrafo único. ~~Serão ainda fiscalizados, auditados, assinados digitalmente, lacrados e verificados os seguintes programas:~~ (Revogado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~I~~ IX - Subsistema de Instalação e Segurança (SIS): sistema que promove a segurança na instalação e na utilização dos sistemas eleitorais; (Renumerado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~II~~ X - bibliotecas-padrão e especiais: bibliotecas-padrão das linguagens C e C++, bibliotecas de código aberto, utilizadas para criptografia e interface gráfica, entre outras funcionalidades; (Renumerado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~III~~ XI - HotSwapFlash (HSF): serviço utilizado pelo Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE) para particionamento, formatação, leitura e escrita das mídias da urna; (Renumerado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~IV~~ XII - programas de criptografia utilizados nos sistemas de coleta, totalização e transmissão dos votos; e (Renumerado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~V~~ XIII - compiladores dos códigos-fonte de todos os sistemas desenvolvidos e utilizados no processo eleitoral. (Renumerado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

XIV - SAVP-Sorteio: aplicativo de apoio ao processo de sorteio de seções para diversas modalidades de auditoria previstas nesta Resolução; (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

XV - SAVP-Votação: aplicativo de apoio ao teste de integridade, que auxilia na verificação dos votos registrados durante a auditoria. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 4º Para fins de fiscalização e auditoria, serão utilizados os seguintes programas de computador assinados digitalmente e lacrados:

I - Verificador de integridade e autenticidade de sistemas eleitorais (AVPART): destinado à verificação da equivalência entre os programas instalados nas urnas eletrônicas e os sistemas eleitorais lacrados. Sistema desenvolvido pelo TSE e que pode ter programas com a mesma funcionalidade desenvolvidos pelas entidades fiscalizadoras;

II - Verificador de Assinaturas Digitais (VAD): destinado à averiguação da autenticidade dos sistemas eleitorais instalados em microcomputadores, utilizando os programas de verificação das entidades fiscalizadoras que foram assinados digitalmente na Cerimônia de Assinatura Digital e Lacração dos Sistemas;

III - Verificador de Autenticação de Programas (VAP): destinado à verificação dos resumos digitais (hash) dos programas instalados em microcomputadores; e

~~IV - Verificador Pré/Pós-Eleição (VPP): destinado à verificação da integridade dos sistemas instalados na urna; à demonstração da votação; à visualização das informações de candidatas e candidatos e de eventos de log da urna; e à impressão do BU, Justificativa Eleitoral (RJE) e RDV.~~

IV - Verificador Pré/Pós-Eleição (VPP): destinado à verificação da integridade dos sistemas instalados na urna e da autenticidade dos dados; à demonstração da votação; à visualização das informações de candidatas e candidatos e de eventos de log da urna; e à impressão do BU, Justificativa Eleitoral (RJE) e RDV. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Parágrafo único. É vedada a utilização, pelos órgãos da Justiça Eleitoral, de qualquer outro sistema em substituição ou com finalidade similar aos desenvolvidos ou autorizados pelo TSE. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 5º A fiscalização dos sistemas eleitorais ocorrerá de acordo com os seguintes momentos e mecanismos:

I - durante o desenvolvimento, a compilação, a assinatura digital, e a lacração dos sistemas eleitorais, mediante:

a) acompanhamento da especificação e do desenvolvimento dos sistemas eleitorais, com acesso ao código-fonte dos programas;

b) criação dos programas de verificação de integridade e autenticidade dos sistemas eleitorais; e

c) assinatura digital e lacração dos sistemas eleitorais;

II - durante as cerimônias destinadas à geração de mídias e preparação das urnas eletrônicas:

a) verificação de integridade e autenticidade dos sistemas eleitorais;

b) verificação da regularidade dos procedimentos adotados para geração de mídias e preparação de urnas eletrônicas;

c) verificação dos dados da urna por meio de demonstração; e

d) acompanhamento e verificação da afixação do lacre físico nas urnas;

III - durante a cerimônia destinada à verificação da integridade e autenticidade dos sistemas eleitorais instalados no TSE;

IV - na audiência destinada à verificação dos sistemas destinados à transmissão de BUs;

~~V - durante os procedimentos preparatórios para realização de teste de integridade e no dia da votação:~~

V - durante os procedimentos preparatórios para realização dos testes de integridade e de autenticidade e no dia da votação: (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

a) verificação da regularidade da designação da Comissão de Auditoria da Votação Eletrônica;

b) verificação da conformidade do sorteio das seções eleitorais para auditoria;

c) verificação da conformidade do preenchimento das cédulas utilizadas na auditoria; e

d) verificação da conformidade da remessa das urnas eletrônicas escolhidas e sorteadas;

VI - durante o Teste de Integridade das Urnas Eletrônicas:

a) verificação da regularidade dos procedimentos de votação e encerramento;

b) conferência do resultado apresentado, com os votos realizados na urna eletrônica; e

c) verificação da conformidade da conclusão dos trabalhos;

~~VII - durante o Teste de Autenticidade dos Sistemas Eleitorais:~~

VII - durante o Teste de Autenticidade dos Sistemas Eleitorais: (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

a) verificação da regularidade dos relatórios de controle;

b) exame da conformidade dos procedimentos de verificação;

~~c) verificação da integridade dos programas instalados na urna eletrônica; e~~

c) verificação da integridade e da autenticidade dos programas instalados na urna eletrônica; e (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

d) verificação da afixação dos lacres na urna eletrônica para início da votação;

VIII - após os procedimentos de totalização das eleições:

a) verificação de relatórios e cópias de arquivos de sistemas; e

b) verificação da correção da contabilização dos votos por meio da comparação com os BUs impressos.

Art. 6º Para efeito dos procedimentos previstos nesta Resolução, salvo disposição específica, são consideradas entidades fiscalizadoras, legitimadas a participar das etapas do processo de fiscalização:

I - partidos políticos, federações e coligações;

II - Ordem dos Advogados do Brasil;

III - Ministério Público;

IV - Congresso Nacional;

V - ~~Supremo Tribunal Federal;~~ (Revogado pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

VI - Controladoria-Geral da União;

VII - Polícia Federal;

VIII - Sociedade Brasileira de Computação;

IX - Conselho Federal de Engenharia e Agronomia;

X - Conselho Nacional de Justiça;

XI - Conselho Nacional do Ministério Público;

XII - Tribunal de Contas da União;

XIII - ~~Forças Armadas;~~ (Revogado pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

XIV - Confederação Nacional da Indústria, demais integrantes do Sistema Indústria e entidades corporativas pertencentes ao Sistema S;

XV - entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e

XVI - departamentos de tecnologia da informação de universidades credenciadas junto ao TSE.

§ 1º As entidades relacionadas nos incisos XV e XVI deste artigo interessadas em participar do acompanhamento do desenvolvimento dos sistemas deverão manifestar seu interesse por meio de ofício dirigido à Presidência do TSE, com antecedência mínima de 10 (dez) dias, contados do início pretendido para a inspeção.

§ 2º Os partidos políticos serão representados pelas pessoas designadas, respectivamente, no TSE, pelos órgãos nacionais; nos tribunais regionais eleitorais (TREs), pelos órgãos estaduais; nos juízos eleitorais, pelos órgãos municipais.

§ 3º As federações e coligações se farão presentes, após sua formação, por meio de representantes ou delegadas e/ou delegados indicados, nos Tribunais eleitorais;

§ 4º As entidades listadas neste artigo poderão se consorciar para os fins de que tratam a presente Resolução.

§ 5º Para fins do caput, a fiscalização poderá ser feita por entidades de âmbito estadual congêneres às previstas neste artigo. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

Art. 7º Os procedimentos descritos nesta Resolução serão realizados por servidoras, servidores, colaboradoras ou colaboradores da JE, excetuando-se os casos em que a competência seja de pessoas legitimadas, desde que expressos nesta Resolução, garantindo-se a representantes das entidades fiscalizadoras o acompanhamento das atividades e a solicitação dos esclarecimentos que se fizerem necessários.

Art. 8º Todos os procedimentos de fiscalização previstos nesta Resolução serão registrados em ata a ser assinada pelas pessoas presentes.

CAPÍTULO II

DA FISCALIZAÇÃO DURANTE O DESENVOLVIMENTO, A COMPILAÇÃO, A ASSINATURA DIGITAL E A LACRAÇÃO DOS SISTEMAS ELEITORAIS

Seção I

Do Acompanhamento da Especificação e do Desenvolvimento dos Sistemas Eleitorais

~~Art. 9º É garantido, às entidades fiscalizadoras, a partir de 12 (doze) meses antes do primeiro turno das eleições, o acesso antecipado aos sistemas eleitorais desenvolvidos pelo TSE e o acompanhamento dos trabalhos para sua especificação e desenvolvimento, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal.~~

Art. 9º É garantido, às entidades fiscalizadoras, a partir de 12 (doze) meses antes do primeiro turno das eleições, até a compilação dos sistemas, prevista no art. 19 desta Resolução, o acesso antecipado aos sistemas eleitorais desenvolvidos pelo Tribunal Superior Eleitoral e o acompanhamento dos trabalhos para sua especificação e seu desenvolvimento, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 1º As entidades fiscalizadoras e as pessoas participantes do último TPS serão convidadas pelo TSE para o acompanhamento das fases de especificação e de desenvolvimento dos sistemas.

§ 2º As entidades fiscalizadoras apresentarão as pessoas que as representam para credenciamento pela Secretaria de Tecnologia da Informação do TSE (STI/TSE) no ato de seu primeiro comparecimento ao Tribunal.

§ 3º As pessoas participantes do TPS devem manifestar à STI/TSE o interesse em acompanhar a fase de especificação e desenvolvimento dos sistemas eleitorais antes de seu primeiro comparecimento ao Tribunal.

Art. 10. O acompanhamento dos trabalhos será realizado no TSE, em ambiente controlado, sem acesso à internet, sendo vedado portar qualquer dispositivo que permita o registro ou a gravação de áudio ou imagem e retirar, sem a expressa autorização da STI/TSE, qualquer elemento ou fragmento dos sistemas ou programas elaborados ou em elaboração.

§ 1º É vedada a introdução, nos equipamentos da JE, de comando, instrução ou programa de computador que objetive, a partir do acesso aos sistemas, copiá-los ou modificá-los.

§ 2º As pessoas participantes assinarão termo de sigilo e confidencialidade, apresentado a elas pela STI/TSE na oportunidade do primeiro acesso ao ambiente controlado.

§ 3º No período de acompanhamento da especificação e do desenvolvimento dos sistemas, poderão ser disponibilizadas múltiplas versões dos sistemas abertos para análise, as quais estarão disponíveis no ambiente descrito no caput para comparação das mudanças efetuadas pelas equipes de desenvolvimento.(Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 11. Os pedidos, assim como dúvidas e questionamentos técnicos, formulados durante o acompanhamento dos sistemas, serão formalizados pelas pessoas participantes à STI/TSE para análise e posterior resposta, no prazo de até 10 (dez) dias úteis, prorrogável por igual período em razão da complexidade da matéria.

§ 1º As respostas previstas no caput deste artigo serão apresentadas antes do início da Cerimônia de Assinatura Digital e Lacração dos Sistemas.

§ 2º As respostas decorrentes de pedidos formalizados nos 10 (dez) dias úteis que antecedem a Cerimônia de Assinatura Digital e Lacração dos Sistemas serão, se possível, apresentadas durante a cerimônia, resguardado, em qualquer hipótese, o direito à dilação do prazo em razão da complexidade da matéria.

Art. 12. As entidades fiscalizadoras poderão utilizar, exclusivamente em equipamentos da JE, programas específicos para a análise estática do software, desde que sejam de conhecimento público, normalmente comercializados ou disponíveis no mercado e devidamente licenciados para proceder à fiscalização.

§ 1º As pessoas interessadas em utilizar o programa a que se refere o caput deste artigo oficiarão ao TSE, encaminhando plano de uso, com a antecedência mínima de 15 (quinze) dias da data prevista para a sua primeira utilização.

§ 2º O plano de uso conterá, obrigatoriamente, o nome do programa, o nome da empresa fabricante, os documentos de comprovação de licenciamento de uso, os eventuais recursos a serem providos pelo TSE, com as respectivas configurações necessárias ao funcionamento do programa e demais informações pertinentes à avaliação de sua aplicabilidade.

~~§ 3º As pessoas representantes das entidades fiscalizadoras poderão apenas consultar os resultados dos testes e dados estatísticos obtidos com o respectivo programa de análise de código apresentado, não sendo permitida sua extração, impressão ou reprodução por nenhuma forma, sendo autorizado seu compartilhamento às demais entidades e instituições legitimadas, desde que restrinja-se ao ambiente de verificação dos códigos-fonte.~~

§ 3º As pessoas representantes das entidades fiscalizadoras poderão apenas consultar os resultados dos testes e dados estatísticos obtidos com o respectivo programa de análise de código apresentado, não sendo permitida sua extração, impressão ou reprodução por nenhuma forma, sendo autorizado seu compartilhamento às demais entidades e instituições legitimadas, desde que se restrinja ao ambiente de verificação dos códigos-fonte. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Seção II

Dos Programas de Verificação de Integridade e Autenticidade dos Sistemas Eleitorais

Art. 13. Os programas de verificação aferirão a integridade e autenticidade dos sistemas eleitorais.

§ 1º Para fins de verificação da integridade dos sistemas eleitorais, os programas calcularão o resumo digital (hash) de cada arquivo assinado na forma do art. 24 desta Resolução, utilizando-se do mesmo algoritmo público e na mesma forma de representação utilizada pelo TSE.

§ 2º Para fins de verificação da autenticidade dos sistemas eleitorais, os programas validarão a assinatura dos arquivos na forma do art. 19 desta Resolução.

Art. 14. O TSE desenvolverá programas de verificação dos sistemas eleitorais.

Parágrafo único. Os programas de que trata o caput deste artigo não poderão ser comercializados pelo Tribunal ou por pessoa física ou jurídica.

Art. 15. As entidades fiscalizadoras poderão desenvolver programas próprios de verificação, devendo, até 90 (noventa) dias antes da realização do primeiro turno das eleições, apresentar, para homologação, o seguinte material:

I - códigos-fonte dos programas de verificação, que deverão estar em conformidade com a especificação técnica disponível na STI/TSE; e

II - chave pública correspondente àquela que será utilizada pelos representantes na Cerimônia de Assinatura Digital e Lacração dos Sistemas.

~~Parágrafo único. Caso o TSE não possua as licenças de uso das ferramentas de desenvolvimento empregadas na construção do programa, a STI/TSE requisita-las-á à entidade fiscalizadora, para uso e guarda do TSE até a realização das eleições.~~

Parágrafo único. O Tribunal Superior Eleitoral, por sua Secretaria de Tecnologia da Informação, requisitará à entidade fiscalizadora as licenças de uso das ferramentas de desenvolvimento empregadas na construção do programa, se não as possuir, para uso e guarda até a realização das eleições. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 16. Detectada qualquer falha de segurança ou problema no funcionamento dos programas de verificação, a STI/TSE informará o fato à entidade fiscalizadora para que, em até 5 (cinco) dias contados da data do recebimento do laudo, providencie o ajuste, submetendo-os a novos testes.

§ 1º A homologação dos programas de verificação somente se dará depois de realizados todos os ajustes solicitados pela equipe da STI/TSE e ocorrerá em até 15 (quinze) dias antes da data determinada para a Cerimônia de Assinatura Digital e Lacração dos Sistemas.

§ 2º Caso os representantes não providenciem os ajustes solicitados, observado o prazo estabelecido no caput deste artigo, a equipe designada pela STI/TSE expedirá laudo fundamentado em que declara o programa inabilitado para os fins a que se destina.

Art. 17. Compete exclusivamente às entidades fiscalizadoras que apresentaram programa próprio de verificação a sua respectiva distribuição.

~~Parágrafo único. Os programas de verificação desenvolvidos poderão ser cedidos a quaisquer outros interessados.~~

Parágrafo único. Os programas de verificação desenvolvidos poderão ser cedidos a qualquer entidade fiscalizadora. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 18. Não será permitida a gravação, na urna ou nos computadores da JE, de nenhum tipo de dado ou função pelos programas de verificação apresentados pelas entidades fiscalizadoras.

Parágrafo único. Os programas apresentados pelas entidades fiscalizadoras poderão utilizar a impressora da urna para emitir relatórios, desde que não comprometam a capacidade de papel disponível.

Seção III

Da Assinatura Digital e da Lacração dos Sistemas Eleitorais

Art. 19. Uma vez concluídos e até 20 (vinte) dias antes das eleições, os sistemas eleitorais e os programas de verificação desenvolvidos pelas entidades fiscalizadoras serão lacrados, mediante apresentação, compilação, assinatura digital e guarda das mídias pelo TSE na Cerimônia de Assinatura Digital e Lacração dos Sistemas, cujos procedimentos terão duração mínima de 3 (três) dias.

Parágrafo único. A convocação das entidades fiscalizadoras para a cerimônia será realizada pelo TSE com pelo menos 10 (dez) dias de antecedência, da qual constarão a data, o horário e o local do evento.

Art. 20. Os sistemas eleitorais e os programas de verificação desenvolvidos pelas entidades fiscalizadoras serão apresentados para inspeção na forma de programas-fonte e programas executáveis, enquanto as chaves privadas e as senhas de acesso serão mantidas em sigilo pela JE.

Parágrafo único. Previamente à cerimônia, as imagens dos ambientes de desenvolvimento poderão ser instaladas nos equipamentos em que serão realizados os trabalhos de compilação e de assinatura dos programas, ficando à disposição das pessoas representantes credenciadas para fins de auditoria.

Art. 21. Os sistemas eleitorais e os programas de verificação desenvolvidos pelas entidades fiscalizadoras serão compilados e assinados digitalmente por servidoras e/ou servidores do TSE, por meio de certificados emitidos por autoridade certificadora credenciada pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Art. 22. As pessoas representantes das entidades fiscalizadoras que demonstrarem interesse poderão assinar digitalmente os sistemas eleitorais e seus próprios programas de verificação.

§ 1º Até 5 (cinco) dias antes da data fixada para a cerimônia, as pessoas representantes das entidades fiscalizadoras que tiverem interesse em assinar digitalmente os programas deverão informar, mediante ofício, a STI/TSE e apresentar, para conferência de sua validade, o certificado digital com o qual irão assinar os programas.

§ 2º As pessoas representantes das entidades fiscalizadoras poderão fazer uso dos programas desenvolvidos e distribuídos pelo TSE.

Art. 23. Encerrado o processo de compilação e geração dos instaladores, serão disponibilizados, no mesmo ambiente utilizado para a inspeção dos códigos-fonte, os arquivos binários gerados durante o processo de compilação, para que as entidades fiscalizadoras possam aferir a correspondência entre o binário gerado e os códigos-fonte analisados.

Parágrafo único. Poderão ser utilizados os mesmos recursos aprovados para a fase de acompanhamento da especificação e do desenvolvimento dos sistemas eleitorais.

Art. 24. Após os procedimentos de compilação e assinatura digital, serão calculados os resumos digitais hashes de todos os programas-fonte, programas executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital e chaves públicas.

Parágrafo único. O arquivo com os resumos digitais será assinado digitalmente pela pessoa que preside o TSE e pela pessoa que responda pela STI/TSE, ou pelas pessoas substitutas formalmente designadas, e pelas pessoas representantes presentes que tenham manifestado interesse, nos termos do § 1° do art. 22 desta Resolução.

Art. 25. A cópia dos resumos digitais será entregue a representantes das entidades fiscalizadoras presentes na cerimônia e publicada no sítio eletrônico do TSE.

Art. 26. Os arquivos referentes aos programas-fonte, programas executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital, chaves públicas e resumos digitais dos sistemas eleitorais e dos programas de assinatura digital e verificação apresentados pelas entidades e instituições serão gravados em mídias não regraváveis.

Parágrafo único. As mídias serão acondicionadas em invólucro lacrado, assinado pelas pessoas presentes, e armazenadas em cofre da STI/TSE.

Art. 27. A Cerimônia de Assinatura Digital e Lacração dos Sistemas será finalizada com a lavratura da ata, que será assinada pelas pessoas presentes, na qual constarão, obrigatoriamente:

I - nomes, versões e datas dos sistemas compilados e lacrados;

II - relação das consultas e dos pedidos apresentados pelas entidades e datas em que as respostas foram apresentadas; e

III - relação de todas as pessoas que assinaram digitalmente os sistemas, na qual se discriminam os programas utilizados e os respectivos fornecedores.

Art. 28. Encerrada a Cerimônia de Assinatura Digital e Lacração dos Sistemas, havendo necessidade de modificação dos programas a serem utilizados nas eleições, o fato será divulgado no sítio eletrônico do TSE e comunicado às entidades fiscalizadoras para que sejam novamente analisados, compilados, assinados digitalmente e lacrados.

§ 1º As modificações nos programas já lacrados somente poderão ser executadas após prévia autorização de quem preside o TSE ou de a pessoa substituta formalmente designada.

§ 2º Na hipótese prevista no caput deste artigo, a comunicação será feita com antecedência mínima de 2 (dois) dias do início da nova cerimônia, cuja duração será estabelecida pelo TSE, não podendo ser inferior a 2 (dois) dias.

Art. 29. Identificada a necessidade de realizar nova assinatura digital e lacração dos sistemas eleitorais, em prazo inferior a 20 (vinte) dias das eleições, o TSE poderá, mediante autorização de quem o preside ou de pessoa substituta formalmente designada, realizar nova cerimônia.

§ 1º Autorizada a realização de nova cerimônia, as entidades fiscalizadoras serão comunicadas para que, imediatamente, possam comparecer ao TSE com o propósito de aferir as mudanças realizadas.

§ 2º A cerimônia terá a duração necessária para que as alterações procedidas sejam apresentadas a representantes das entidades fiscalizadoras e concluídos os demais procedimentos previstos nesta seção.

§ 3º Os procedimentos realizados serão registrados em ata, nos termos do art. 27 desta Resolução.

§ 4º Caso a necessidade seja identificada no dia das eleições, os procedimentos necessários serão aferidos por representantes das entidades fiscalizadoras presentes no TSE, sem prejuízo de verificações posteriores.

Art. 30. Havendo necessidade de modificação dos programas a serem utilizados nas eleições suplementares, será dado conhecimento do fato aos representantes das entidades fiscalizadoras para análise, compilação e assinatura digital dos programas modificados, seguidos de nova lacração.

Art. 31. As pessoas representantes das entidades fiscalizadoras assinarão digitalmente os respectivos programas e chaves públicas.

Art. 32. Os programas de verificação não homologados e aqueles homologados cujas pessoas representantes não comparecerem à Cerimônia de Assinatura Digital e Lacração dos Sistemas serão desconsiderados para todos os efeitos.

Art. 33. No prazo de 5 (cinco) dias contados do encerramento da Cerimônia de Assinatura Digital e Lacração dos Sistemas, as entidades fiscalizadoras poderão impugnar os programas apresentados, em petição fundamentada (§ 3º do art. 66 da Lei n° 9.504/1997 (https://www.planalto.gov.br/ccivil_03/leis/l9504.htm#art66)).

Parágrafo único. A impugnação será autuada na classe Petição (Pet) e distribuída a relatora ou relator que a apresentará para julgamento pelo Plenário do Tribunal, em sessão administrativa, após ouvir a STI/TSE e o Ministério Público, e determinará as diligências que entender necessárias.

CAPÍTULO III

DA VERIFICAÇÃO DOS SISTEMAS ELEITORAIS

Seção I

Das Disposições Gerais das Verificações

Art. 34. Nas verificações dos sistemas eleitorais a serem realizadas no âmbito dos TREs ou das zonas eleitorais, a pessoa representante da entidade fiscalizadora informará se utilizará o programa de verificação de autenticidade e integridade da JE ou programa próprio, nos termos do art. 15 desta Resolução.

Art. 35. O juízo eleitoral poderá determinar de ofício, no âmbito de sua jurisdição, a realização das verificações previstas nesta Resolução.

Seção II

Da Verificação dos Sistemas Eleitorais na Cerimônia de Geração de Mídias

Art. 36. Durante a Cerimônia de Geração de Mídias, prevista na Resolução de Atos Gerais do Processo Eleitoral, as entidades fiscalizadoras poderão verificar a integridade e autenticidade do Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE), Subsistema de Instalação e Segurança (SIS) e HotSwapFlash (HSF).

§ 1º Os pedidos de verificação serão dirigidos à autoridade responsável pela geração de mídias, que decidirá e adotará providências imediatas.

§ 2º A fiscalização poderá ser realizada utilizando o programa de verificação fornecido pelo TSE ou desenvolvido pela entidade fiscalizadora nos termos do art. 15 desta Resolução.

§ 3º Qualquer cidadã ou cidadão presente à cerimônia poderá levantar dúvidas ou reportar eventual irregularidade observada, por escrito, ao juízo eleitoral ou autoridade competente sem, no entanto, dirigir-se diretamente às técnicas, aos técnicos, às servidoras e aos servidores da JE, durante o exercício das suas atividades.

Seção III

Da Verificação dos Sistemas Eleitorais na Cerimônia de Preparação de Urnas

Art. 37. Durante a Cerimônia de Preparação de Urnas, prevista na Resolução de Atos Gerais do Processo Eleitoral, as entidades fiscalizadoras poderão verificar a integridade e autenticidade dos sistemas eleitorais instalados em urnas eletrônicas.

~~§ 1º A verificação por amostragem será realizada em até 3% (três por cento) das urnas preparadas escolhidas por representantes das entidades fiscalizadoras presentes na cerimônia entre as urnas de votação e as de contingência, ou na ausência de escolhas, pela autoridade eleitoral responsável, observado o mínimo de:~~

~~§ 1º A verificação por amostragem será realizada em no mínimo 3% (três por cento) e no máximo de 6% (seis por centos) das urnas preparadas para cada zona eleitoral e ao menos uma urna por município, escolhidas pelos representantes das entidades fiscalizadoras, de forma aleatória, entre as urnas de votação e as de contingência. (Redação dada pela Resolução nº 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)~~

§ 1º A verificação por amostragem será realizada em até 6% (seis por cento) das urnas preparadas para cada zona eleitoral, escolhidas pelos representantes das entidades fiscalizadoras, de forma aleatória, entre as urnas de votação e as de contingência. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

I - ~~1 (uma) urna por município para cada zona eleitoral nas eleições municipais;~~ (Revogado pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

II - ~~1 (uma) urna por zona eleitoral nas eleições gerais.~~ (Revogado pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

§ 2º Os pedidos de verificação serão dirigidos à autoridade responsável pela preparação das urnas, que determinará imediatamente a separação das urnas indicadas e adotará as providências para a sua verificação.

§ 3º A verificação da integridade e autenticidade dos programas da urna eletrônica será realizada nos locais de preparação das urnas mediante:

I - utilização do programa de verificação de autenticidade dos programas da urna (AVPART), desenvolvido pelo Tribunal Superior Eleitoral;

II - utilização do programa de Verificação Pré/Pós-Eleição (VPP) da urna eletrônica, desenvolvido pelo TSE; e

III - utilização de programas de verificação de integridade e autenticidade dos sistemas eleitorais, desenvolvidos pelas entidades fiscalizadoras.

§ 4º Qualquer cidadã ou cidadão presente à cerimônia poderá levantar dúvidas ou reportar eventual irregularidade observada, por escrito, ao juízo eleitoral ou autoridade competente sem, no entanto, dirigir-se diretamente às técnicas, aos técnicos, às servidoras e aos servidores da JE, durante o exercício das suas atividades.

~~§ 5º Na ocorrência de inconsistência em urna objeto da verificação por amostragem, a autoridade judiciária ampliará o percentual adotado nos termos do § 1º, até que não mais se encontre, nas urnas verificadas, nenhum tipo de incongruência. (Incluído pela Resolução nº 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)~~

§ 5º Na ocorrência de inconsistência em urna objeto da verificação por amostragem, a autoridade judiciária determinará que: (Redação dada pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

I - seja identificado o tipo de divergência; (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

II - seja verificado se tal inconsistência se aplica a uma urna em particular ou se se repete em mais do que uma urna, utilizando-se, para tanto, o número de urnas que considerar adequado; (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

III - sejam imediatamente interrompidos os trabalhos, e: (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

a) em caso de a ocorrência estar relacionada a sistemas, atualizar as versões e reiniciar os dados dos sistemas e das urnas, de forma a garantir que o ambiente de trabalho passe a operar com as versões mais recentes; (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

b) em caso de a ocorrência estar relacionada aos dados importados, reiniciar arquivos e tabelas de versões incompatíveis, seguido da importação desses; (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

c) nos demais casos, o juiz eleitoral adotará as medidas que julgar adequadas. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

§ 6º Todos os procedimentos relacionados ao § 5º deverão constar de ata específica. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

§ 7º A conferência visual dos dados de candidatas, candidatos e partidos, prevista no art. 86 da Resolução TSE nº 23.699/2021, poderá ser realizada em qualquer das urnas selecionadas para os procedimentos do § 1º, por meio do aplicativo VPP. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

Art. 38. O Programa de verificação de autenticidade dos programas da urna (AVPART) permitirá:

I - emissão do hash dos programas instalados durante a carga das urnas eletrônicas; e

II - validação das assinaturas digitais dos arquivos da urna eletrônica.

Art. 39. O Programa Verificador Pré/Pós-Eleição (VPP) da urna eletrônica permitirá a:

I - conferência visual dos dados de pessoas candidatas e partidos;

II - emissão do hash dos programas instalados durante a carga das urnas eletrônicas; e

III - demonstração do processo de votação, a fim de aferir o correto funcionamento do equipamento.

Art. 40. As urnas eletrônicas serão lacradas depois de realizadas todas as verificações.

Parágrafo único. Em caso de inconsistência, é facultada aos partidos, às coligações e às federações a indicação de assistentes técnicos para acompanharem as verificações que se seguirem à Cerimônia de Preparação de Urnas. (Incluído pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

Seção IV

Da Verificação dos Sistemas Eleitorais Instalados no Tribunal Superior Eleitoral

Art. 41. As entidades fiscalizadoras poderão verificar a integridade e autenticidade dos sistemas eleitorais instalados nos equipamentos do TSE.

§ 1º Para os fins previstos neste artigo, poderão ser verificados os sistemas Gerenciamento da Totalização, Receptor de Arquivos de Urnas, InfoArquivos e Transportador WEB.

§ 2º O TSE comunicará as entidades fiscalizadoras mediante ofício sobre a necessidade de comparecimento na véspera da eleição. Art. 42. Será lavrada ata circunstanciada da verificação, nos termos do art. 8º desta Resolução, a qual especificará:

I - a identificação e versão dos sistemas verificados, com o resultado obtido;

II - a data, o local e o horário de início e término das atividades; e

III - o nome e a qualificação das pessoas presentes.

Seção V

Da Verificação dos Sistemas Destinados à Transmissão de Boletins de Urna

~~Art. 43. As entidades fiscalizadoras poderão solicitar audiência destinada à verificação da integridade e autenticidade dos sistemas Transportador de Arquivos e JE-Connect, instalados nos microcomputadores.~~

~~Art. 43. Na antevéspera do dia das eleições, o juiz eleitoral realizará audiência destinada à verificação da integridade e autenticidade dos sistemas Transportador e JE-Connect, instalados nos microcomputadores. (Redação dada pela Resolução nº 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)~~

Art. 43. Até a antevéspera do dia das eleições, a juíza ou o juiz eleitoral realizará audiência destinada à verificação da integridade e autenticidade dos sistemas Transportador e JEConnect, instalados nos microcomputadores. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~§ 1º Os pedidos de verificação serão, mediante petição encaminhada até 5 (cinco) dias antes do pleito, dirigidos ao juízo eleitoral, que designará data, horário e local para realização do procedimento.~~

§ 1º Até cinco dias antes do pleito, o juiz eleitoral designará horário e local para o procedimento. (Redação dada pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

§ 2º ~~A audiência de verificação somente poderá ser realizada a partir da antevéspera do dia das eleições, não podendo ultrapassar as 17 horas do dia da eleição.~~ (Revogado pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

~~§ 3º A fiscalização poderá ser realizada por meio do programa de verificação fornecido pelo TSE ou desenvolvido pela entidade fiscalizadora nos termos do art. 15 desta Resolução.~~

§ 3º A fiscalização poderá ser feita por meio do programa de verificação fornecido pelo Tribunal Superior Eleitoral ou desenvolvido pela entidade fiscalizadora nos termos do art. 15 desta Resolução. (Redação dada pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

§ 4º A verificação prevista neste artigo deverá ser realizada em 1 (um) computador que possua o Sistema Transportador instalado e em 1 (um) dispositivo com o JE-Connect configurado para uso nas eleições, a critério do Juízo Eleitoral, considerando a logística de deslocamento de equipamentos. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

Art. 44. Será lavrada ata circunstanciada da verificação, nos termos do art. 8º, a qual especificará:

I - a identificação e versão dos sistemas verificados, com o resultado obtido;

II - a data, o local e o horário de início e término das atividades; e

III - o nome e a qualificação das pessoas presentes.

Seção VI

Da Entrega de Dados, Arquivos e Relatórios

Art. 45. Após a conclusão dos trabalhos de preparação das urnas eletrônicas, as entidades fiscalizadoras poderão solicitar:

I - os arquivos de log do Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (Gedai-UE); e

II - os arquivos de dados alimentadores do Sistema de Gerenciamento da Totalização, referentes a pessoas candidatas, partidos políticos, coligações, federações, municípios, zonas e seções.

Art. 46. Após a conclusão dos trabalhos de totalização, as entidades fiscalizadoras poderão solicitar:

I - arquivos de log do Transportador, do Receptor de Arquivos de Urna e do banco de dados da totalização;

II - arquivos de imagens dos Boletins de Urnas (BUs);

III - arquivos de Registro Digital do Voto (RDV);

IV - arquivos de log das urnas;

V - relatório de BUs que estiveram em pendência, sua motivação e respectiva decisão;

~~VI - relatório de urnas substituídas;~~

VI - relatório Resultado da Totalização emitido pelo Sistema de Gerenciamento da Totalização (SISTOT), incluindo a relação das seções em que o boletim de urna tenha sido gerado em urna substituta; (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

VII - arquivos de dados de votação por seção; e

VIII - relatório com dados sobre o comparecimento e a abstenção em cada seção eleitoral.

Parágrafo único. O Registro Digital do Voto será fornecido em arquivo único por seção eleitoral, devendo estar intacto, no mesmo formato e leiaute em que foi gravado originalmente.

Art. 47. A solicitação especificará a abrangência dos dados requeridos, sendo dirigidas, preferencialmente:

I - à zona eleitoral, caso o pedido esteja restrito a dados da zona eleitoral;

II - ao TRE, caso o pedido abranja dados de mais de uma zona eleitoral de uma mesma unidade da federação;

III - ao TSE, caso o pedido abranja dados de mais de uma unidade da Federação.

Art. 48. Os arquivos de dados previstos nesta seção, solicitados à JE para fins de auditoria com a necessidade de preservação da cadeia de custódia, poderão ser solicitados em até 100 (cem) dias, contados a partir do dia do primeiro turno das eleições, devendo ser preservados pela zona eleitoral em igual prazo.

~~Parágrafo único. Os arquivos recebidos pelo TSE serão por ele mantidos nos prazos estabelecidos no seu Plano de Classificação, Avaliação e Destinação das Informações e dos Documentos.~~

Parágrafo único. Os arquivos de dados listados nesta seção ficarão disponíveis pelo prazo estabelecido no Plano de Classificação, Avaliação e Destinação das Informações e dos Documentos. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 49. A entrega dos arquivos e dos relatórios solicitados será atendida, pela autoridade à qual foi destinada a solicitação, em até 5 (cinco) dias úteis.

~~Art. 50. A pessoa requerente deverá fornecer as mídias necessárias para a gravação dos arquivos.~~

Art. 50. Se for necessário, a pessoa requerente deverá fornecer as mídias para a gravação dos arquivos, contando-se o prazo previsto no art. 49 desta Resolução a partir da data em que fornecê-las. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Seção VII

Das Verificações Extraordinárias dos Sistemas Eleitorais após as Eleições

~~Art. 51. As entidades fiscalizadoras poderão solicitar verificação extraordinária após o pleito, desde que sejam relatados fatos e apresentados indícios e circunstâncias que a justifiquem, sob pena de indeferimento liminar.~~

Art. 51. As entidades fiscalizadoras poderão solicitar verificação após o pleito, desde que sejam relatados fatos e apresentados indícios e circunstâncias que a justifiquem, sob pena de indeferimento liminar. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 1º O prazo para o pedido de verificação posterior ao pleito se encerra em 5 (cinco) dias antes da data-limite estabelecida no Calendário Eleitoral para manutenção dos lacres das urnas e para liberação da desinstalação dos sistemas.

~~§ 2º A solicitação, acompanhada de plano de trabalho, será dirigida à autoridade competente, que decidirá sobre o pedido.~~

§ 2º A solicitação, acompanhada de plano de trabalho, será dirigida ao tribunal eleitoral competente, que decidirá sobre o pedido. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 3º O plano de trabalho conterá, no mínimo, as verificações pretendidas, como serão aferidas e os objetivos a serem alcançados.

Art. 52. Após as eleições, é possível verificar:

I - sistemas instalados nos microcomputadores, aplicando-se, no que couber, o disposto nas Seções II e V deste capítulo;

II - sistemas instalados nas urnas eletrônicas, aplicando-se, no que couber, o disposto na Seção III deste capítulo, adicionadas a exibição de logs da urna eletrônica e a reimpressão do boletim de urna, por meio do sistema de Verificação Pré/Pós-Eleição (VPP);

III - sistemas instalados nos equipamentos servidores do TSE, aplicando-se, no que couber, o disposto na Seção IV deste capítulo

Parágrafo único. ~~As verificações previstas neste artigo serão realizadas mediante o espelhamento dos sistemas, preservando-se os originais intactos.~~(Revogado pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

CAPÍTULO IV

DAS AUDITORIAS DE FUNCIONAMENTO DAS URNAS ELETRÔNICAS

Seção I

Disposições Preliminares

Art. 53. Os tribunais regionais eleitorais realizarão, por amostragem, no dia da votação:

I - em ambiente controlado, o Teste de Integridade das Urnas Eletrônicas, nos termos do Capítulo V desta Resolução, em cada unidade da Federação, em local público e com expressiva circulação de pessoas, designado pelo TRE, no mesmo dia e horário da votação oficial, em ambos os turnos;

II - a verificação de autenticidade e integridade dos sistemas instalados nas urnas, nos termos do Capítulo VI desta Resolução, em cada unidade da Federação, nas seções eleitorais escolhidas ou sorteadas de acordo com o disposto na Seção III do presente capítulo.

Art. 53-A. A Justiça Eleitoral realizará Teste de Integridade com Biometria, a partir das eleições de 2024, em locais de votação designados. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Art. 53-B. O Teste de Integridade com Biometria será realizado mediante o emprego de biometria de eleitores voluntários em local próximo ao da votação. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Parágrafo único. Após votarem, eleitoras e eleitores serão convidados a participar do teste com biometria, mantidos os demais procedimentos do Teste de Integridade das Urnas Eletrônicas, no que couber. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Art. 53-C. A regulamentação, a coordenação e a implementação do Teste de Integridade com Biometria serão realizadas de acordo com a viabilidade técnica, logística, orçamentária e financeira da Justiça Eleitoral e a sua realização observará os seguintes requisitos: (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

I - as seções eleitorais para a realização do teste com biometria, em cada Tribunal Regional Eleitoral, serão: (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

a) no mínimo de 5% (cinco por cento) e no máximo de 10% (dez por cento) do total de urnas eletrônicas destinadas ao teste de integridade, previsto no art. 58 desta Resolução, compondo o seu respectivo quantitativo total; (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

~~b) instaladas em, no mínimo, 5 (cinco) capitais de Estados e no Distrito Federal; e (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)~~

b) instaladas necessariamente em todas as capitais dos Estados e no Distrito Federal; e (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

c) indicadas pelas Comissões de Auditoria da Votação Eletrônica, instituídas nos termos do art. 55 desta Resolução, que definirão as localidades das seções eleitorais para a realização do teste com biometria até 10 (dez) dias antes do dia da votação. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Parágrafo único. Outros requisitos poderão ser especificados em portaria da Presidência do Tribunal Superior Eleitoral. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Art. 53-D. As seções eleitorais em que se realizarão o Teste de Integridade com Biometria serão abertas a quaisquer pessoas interessadas, mas a circulação na área onde as urnas e os computadores estiverem instalados ficará restrita a integrantes da Comissão de Auditoria de Votação Eletrônica, a auxiliares por ela designados e a pessoas previamente credenciadas para executar a auditoria, assegurada a fiscalização de todas as fases do processo. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Art. 53-E. As eleitoras e os eleitores que aceitarem participar do Teste de Integridade com Biometria assinarão termo de consentimento padrão elaborado pelo TSE. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Art. 54. Os trabalhos de auditoria de funcionamento das urnas eletrônicas, previstos nos Capítulos V e VI desta Resolução, são públicos e poderão ser acompanhados por qualquer pessoa interessada. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

§ 1º Os tribunais regionais eleitorais informarão, em edital e mediante divulgação nos respectivos sítios eletrônicos em até 20 (vinte) dias antes das eleições, os locais onde serão realizadas as auditorias de funcionamento das urnas eletrônicas de que trata o inciso I do art. 53 desta Resolução. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

§ 2º No mesmo prazo mencionado no § 1º deste artigo, a Comissão de Auditoria da Votação Eletrônica de cada TRE expedirá ofício aos partidos políticos comunicando-os sobre o horário e o local onde será realizada a escolha ou o sorteio das seções eleitorais cujas urnas serão auditadas. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

§ 3º A Justiça Eleitoral dará ampla divulgação à realização dos eventos em todas as unidades da Federação. (Incluído pela Resolução nº 23.722/2023) (https://www.tse.jus.br/legislacao/compilada/res/2023/resolucao-no-23-722-de-26-de-setembro-de-2023)

Seção II

Da Comissão de Auditoria da Votação Eletrônica

~~Art. 55. Para a organização e a condução dos trabalhos referidos nos Capítulos V e VI desta Resolução, será designada pelos tribunais regionais eleitorais, em sessão pública, em até 30 (trinta) dias antes das eleições, Comissão de Auditoria da Votação Eletrônica composta por:~~

Art. 55. Para a organização e a condução dos trabalhos mencionados nos capítulos V e VI desta Resolução, será designada pelos tribunais regionais eleitorais, em sessão pública, até 60 (sessenta) dias antes das eleições, Comissão de Auditoria da Votação Eletrônica composta por: (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

I - 1 (uma) juíza ou 1 (um) juiz de direito, que a presidirá;

II - no mínimo 6 (seis) pessoas servidoras da Justiça Eleitoral, sendo pelo menos 1 (uma) da Corregedoria Regional Eleitoral, 1 (uma) da Secretaria Judiciária e 1 (uma) da Secretaria de Tecnologia da Informação.

§ 1º A procuradora regional eleitoral ou o procurador regional eleitoral indicará 1 (uma) pessoa representante do Ministério Público para acompanhar os trabalhos.

§ 2º As entidades fiscalizadoras poderão indicar representantes para acompanhar os trabalhos.

Art. 56. As entidades fiscalizadoras poderão, no prazo de 3 (três) dias contados da divulgação dos nomes das pessoas que comporão a Comissão de Auditoria da Votação Eletrônica, impugnar, justificadamente, as designações.

Seção III

Da definição das Seções Eleitorais para Auditoria

~~Art. 57. A Comissão de Auditoria da Votação Eletrônica promoverá, entre as 9 horas e as 12 horas do dia anterior às eleições, no primeiro e no segundo turnos, em local e horário previamente divulgados, a definição das seções eleitorais que serão submetidas às auditorias a que se referem os capítulos V e VI desta Resolução.~~

Art. 57. A Comissão de Auditoria da Votação Eletrônica promoverá, entre as 7 horas e as 12 horas, do dia anterior às eleições, no primeiro e no segundo turno, em local e horário previamente divulgados, a definição das seções eleitorais que serão submetidas às auditorias a que se referem os capítulos V e VI desta Resolução. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 1º Entre as seções eleitorais elegíveis, a definição daquelas que serão submetidas às auditorias seguirão os seguintes critérios e sequência:

I - cada entidade fiscalizadora presente escolherá uma seção eleitoral;

II - no caso de a quantidade de seções escolhidas ser superior ao quantitativo estabelecido nos arts. 58 e 59 desta Resolução, será promovido sorteio entre as seções eleitorais escolhidas; e

III - no caso de ausência de entidades fiscalizadoras ou no caso de a quantidade de seções escolhidas ser inferior ao quantitativo estabelecido nos arts. 58 e 59 desta Resolução, será promovido um sorteio de forma a complementar o quantitativo. § 2º As seções agregadas não serão consideradas para fins de escolha ou sorteio de que trata o caput deste artigo.

Art. 58. Nas eleições gerais, para a realização da auditoria de funcionamento das urnas, serão definidos, em ambos os turnos, em cada unidade da Federação, os seguintes quantitativos de seções eleitorais:

~~I - 9 (nove) nas unidades da Federação com até 15.000 (quinze mil) seções no Cadastro Eleitoral, sendo as 6 (seis) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais;~~

I - 23 (vinte e três) nas unidades da Federação com até 15.000 (quinze mil) seções no Cadastro Eleitoral, sendo as 20 (vinte) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais; (Redação dada pela Resolução n° 23.693/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-693-de-29-de-marco-de-2022)

~~II - 16 (dezesseis) nas unidades da Federação que tenham de 15.001 (quinze mil e uma) a 30.000 (trinta mil) seções no Cadastro Eleitoral, sendo as 8 (oito) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais; e~~

II - 35 (trinta e cinco) nas unidades da Federação que tenham de 15.001 (quinze mil e uma) a 30.000 (trinta mil) seções no Cadastro Eleitoral, sendo as 27 (vinte e sete) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais; e (Redação dada pela Resolução n° 23.693/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-693-de-29-de-marco-de-2022)

~~III - 20 (vinte) nas demais unidades da Federação, sendo as 10 (dez) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais.~~

III - 43 (quarenta e três) nas demais unidades da Federação, sendo as 33 (trinta e três) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais. (Redação dada pela Resolução n° 23.693/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-693-de-29-de-marco-de-2022)

§ 1º Para o Teste de Integridade das Urnas Eletrônicas, pelo menos 1 (uma) seção eleitoral escolhida ou sorteada será da capital.

~~§ 2º Não poderá ser escolhida ou sorteada mais de 1 (uma) seção por zona eleitoral.~~

§ 2º Não poderá ser escolhida ou sorteada mais de 1 (uma) seção por zona eleitoral, salvo nas hipóteses em que o número de zonas eleitorais vinculadas ao Tribunal Regional seja inferior ao exigido para atender ao quantitativo previsto neste artigo. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 59. Nas eleições municipais, para a realização da auditoria de funcionamento das urnas, serão observados, no primeiro turno, os mesmos quantitativos das eleições gerais definidos no artigo 58.

§ 1º Havendo segundo turno, serão observados os seguintes quantitativos:

I - 9 (nove) nas unidades da Federação com até 5.000 (cinco mil) seções funcionando no segundo turno de votação, sendo as 6 (seis) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais;

II - 16 (dezesseis) nas unidades da Federação que tenham de 5.001 (cinco mil e uma) a 10.000 (dez mil) seções funcionando no segundo turno de votação, sendo as 8 (oito) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais; e

III - 20 (vinte) nas demais unidades da Federação, sendo as 10 (dez) primeiras urnas escolhidas ou sorteadas submetidas ao Teste de Integridade das Urnas Eletrônicas e as demais, ao Teste de Autenticidade dos Sistemas Eleitorais.

§ 2º Somente poderá ser escolhida ou sorteada mais de 1 (uma) seção por zona eleitoral, para o mesmo tipo de auditoria, quando não se atingir o quantitativo fixado de urnas a serem auditadas no segundo turno de votação, previsto nos incisos I, II e III deste artigo.

§ 3º A escolha ou o sorteio de mais de 1 (uma) seção por zona eleitoral serão restritos ao Teste de Integridade das Urnas Eletrônicas e limitado a até três seções por zona eleitoral.

§ 4º Havendo eleição para o segundo turno na capital, pelo menos 1 (uma) seção eleitoral escolhida ou sorteada para o Teste de Integridade das Urnas Eletrônicas será desse município.

§ 5º Se o número de zonas eleitorais dos Municípios da unidade da federação onde houver segundo turno for inferior aos quantitativos previstos nos incisos I, II e III, o teste de autenticidade será realizado em urnas equivalentes ao número de zonas eleitorais. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~Art. 60. A Comissão de Auditoria da Votação Eletrônica poderá restringir, de comum acordo com representantes das entidades fiscalizadoras, a abrangência das escolhas e dos sorteios a determinados municípios ou zonas eleitorais, na hipótese da existência de localidades de difícil acesso, onde o tempo hábil para o recolhimento da urna seja inviável.~~

Art. 60. A Comissão de Auditoria da Votação Eletrônica poderá, de comum acordo com representantes das entidades fiscalizadoras: (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

I - dividir os Municípios da unidade da federação em grupos, a fim de assegurar a representatividade regional das seções eleitorais escolhidas ou sorteadas para a realização do teste de integridade das urnas eletrônicas; (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

II - excluir do sorteio ou da escolha as seções eleitorais instaladas em localidades de difícil acesso, onde seja inviável recolher a urna em tempo hábil para a realização do teste. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

CAPÍTULO V

DO TESTE DE INTEGRIDADE DAS URNAS ELETRÔNICAS

Seção I

Da Remessa das Urnas

Art. 61. Finalizada a escolha ou o sorteio das seções eleitorais destinadas ao Teste de Integridade das Urnas Eletrônicas, a presidência da Comissão de Auditoria da Votação Eletrônica comunicará imediatamente o resultado ao juízo eleitoral da zona correspondente à seção escolhida ou sorteada.

~~§ 1º O juízo eleitoral providenciará o imediato transporte da urna para o local indicado, devidamente acondicionada em sua caixa, com a respectiva ata de carga.~~

§ 1º O juízo eleitoral providenciará o imediato transporte, para o local indicado pela Comissão de Auditoria da Votação Eletrônica, da urna, devidamente acondicionada em sua caixa, e de cópias da ata da cerimônia de carga e do extrato de carga, o qual deverá mostrar a numeração da cartela de lacres utilizada. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 2º Caso seja verificada, pelo juízo eleitoral, circunstância peculiar da seção eleitoral escolhida ou sorteada que impeça a remessa da urna em tempo hábil, a Comissão de Auditoria da Votação Eletrônica providenciará a escolha ou o sorteio de outra seção da mesma zona eleitoral.

§ 3º Os tribunais regionais eleitorais providenciarão meio de transporte para a remessa da urna correspondente à seção eleitoral escolhida ou sorteada, que poderá ser acompanhada pelas entidades fiscalizadoras e pessoas credenciadas para executar a auditoria.

§ 4º As pessoas representantes das entidades fiscalizadoras poderão acompanhar o transporte da urna, arcando com suas respectivas despesas.

Art. 62. Realizadas as providências previstas no art. 61 desta Resolução, o juízo eleitoral, de acordo com a logística estabelecida pelo TRE, providenciará:

I - a preparação de urna substituta;

II - a substituição da urna; e

III - a atualização das tabelas de correspondência entre urna e seção eleitoral.

Parágrafo único. De todo o procedimento de recolhimento, preparação de urna substituta e remessa da urna original, será lavrada ata circunstanciada, a ser assinada pelo juízo responsável pela preparação e pelas pessoas representantes das entidades fiscalizadoras presentes, as quais poderão acompanhar todas as fases.

Seção II

Da Preparação da Auditoria

Art. 63. A Comissão de Auditoria da Votação Eletrônica providenciará o número de cédulas de votação, por seção eleitoral escolhida ou sorteada, que corresponda a, aleatoriamente, a número entre 75% (setenta e cinco por cento) e 82% (oitenta e dois por cento) do número de eleitoras e eleitores registrados na respectiva seção eleitoral, as quais serão preenchidas por representantes dos partidos políticos, das federações e das coligações que estiverem presentes e guardadas em urnas de lona lacradas.

~~§ 1º Na ausência de representantes dos partidos políticos, das federações e das coligações, a Comissão de Auditoria da Votação Eletrônica providenciará o preenchimento das cédulas por terceiras pessoas, excluídas as que servem a JE.~~

§ 1º Na ausência de representantes dos partidos políticos, das federações e das coligações, a Comissão de Auditoria da Votação Eletrônica providenciará o preenchimento das cédulas por terceiras pessoas, excluídas as que servem à Justiça Eleitoral, podendo ser chamadas as servidoras e os servidores nomeados nos termos do § 2º do art. 67 desta Resolução e previamente

convocados para a cerimônia. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~§ 2º As cédulas serão preenchidas com os números correspondentes a candidatas e candidatos registrados, a votos nulos e a votos de legenda, e existirão cédulas com votos em branco.~~

§ 2º Cada participante definirá os números utilizados para preenchimento da cédula, podendo optar por voto nominal, voto de legenda ou voto em branco. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 3º Se o número utilizado para preencher a cédula não corresponder à candidatura registrada ou à legenda habilitada na eleição, o voto será considerado nulo. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 64. O ambiente em que se realizarão os trabalhos será aberto a qualquer pessoa interessada, mas a circulação na área onde as urnas e os computadores estiverem instalados ficará restrita a integrantes da Comissão, a auxiliares por ela designados e a pessoas credenciadas para executar a auditoria, assegurando-se a fiscalização de todas as fases do processo pelas pessoas previamente autorizadas.

§ 1º A área de circulação restrita de que trata o caput deste artigo será isolada por meio de fitas, cavaletes ou outro material disponível que permita total visibilidade a pessoas interessadas para acompanhamento e fiscalização dos trabalhos.

~~§ 2º A auditoria de funcionamento das urnas eletrônicas será filmada pela JE ou por empresa contratada.~~

§ 2º A auditoria de funcionamento das urnas eletrônicas será filmada pela Justiça Eleitoral ou por empresa contratada para esse fim e transmitida ao vivo através da rede mundial de computadores, sendo veiculada, preferencialmente, no canal oficial de cada Tribunal Regional Eleitoral no YouTube. (Redação dada pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

§ 3º Os tribunais regionais eleitorais que ainda não disponham de canal no YouTube deverão providenciá-lo até sessenta dias antes da data das eleições. (Incluído pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

Seção III

Do Processo Complementar de Auditoria

Art. 65. O TSE firmará convênio com instituições públicas de fiscalização ou contratará empresa especializada em auditoria para fiscalizar os trabalhos da auditoria de funcionamento das urnas eletrônicas.

~~§ 1º A fiscalização será realizada, em todas as fases dos trabalhos da auditoria de funcionamento das urnas eletrônicas, nos tribunais regionais eleitorais, por representante das instituições conveniadas ou das empresas previamente credenciadas pelo TSE.~~

§ 1º A fiscalização será realizada, em todas as fases dos trabalhos da auditoria de funcionamento das urnas eletrônicas, nos Tribunais Regionais Eleitorais, com exceção da coleta e do transporte desses equipamentos, por representante das instituições conveniadas ou das empresas previamente credenciadas pelo TSE. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 2º A pessoa representante credenciada reportar-se-á exclusivamente à Comissão de Auditoria da Votação Eletrônica.

~~Art. 66. A instituição conveniada ou a empresa de auditoria encaminhará ao TSE, em até 3 (três) dias úteis após cada turno, relatório conclusivo da fiscalização realizada na auditoria de funcionamento das urnas eletrônicas.~~

Art. 66. A instituição conveniada ou a empresa de auditoria encaminhará ao Tribunal Superior Eleitoral, em até 5 (cinco) dias úteis após cada turno, relatório conclusivo da fiscalização realizada na auditoria de funcionamento das urnas eletrônicas. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 1º Os relatórios de auditoria incluirão, necessariamente, os seguintes itens:

I - resultado da contagem independente dos votos realizada manualmente por fiscal, em pelo menos uma das urnas utilizadas no local da auditoria, sem utilizar o sistema de apoio do TSE; e

II - descrição de qualquer evento que possa ser entendido como fora da rotina de uma votação normal, mesmo que ocorrido antes do início da votação e da emissão da zerésima até a impressão final do BU, relacionando o evento descrito à normatização correspondente.

~~§ 2º Os relatórios de auditoria, após a homologação pelo TSE, serão publicados no sítio eletrônico da JE, em até 30 (trinta) dias após o segundo turno.~~

§ 2º Os relatórios individuais de auditoria de cada Tribunal Regional Eleitoral e o relatório consolidado conclusivo, elaborados pela instituição pública de fiscalização ou pela empresa especializada em auditoria contratada, serão publicados no sítio eletrônico da Justiça Eleitoral em até 30 (trinta) dias após o segundo turno. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Seção IV

Dos Procedimentos de Votação e Apuração

Art. 67. Após a emissão da zerésima, expedida pela urna e pelo sistema de apoio à auditoria de funcionamento das urnas eletrônicas, serão iniciados os trabalhos de auditoria, conforme os procedimentos e horários estabelecidos pelo TSE para a votação oficial.

~~Parágrafo único. A votação não seguirá a mesma ordem em que as eleitoras e os eleitores estão relacionados na folha de votação.~~

§ 1º A ordem de votação será aleatória em relação à folha de votação. (Incluído pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

~~§ 2º Os votos serão lançados na urna eletrônica por servidor efetivo da Justiça Eleitoral. (Incluído pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)~~

§ 2º Os votos serão lançados na urna eletrônica por servidor efetivo do Poder Judiciário ou do Ministério Público. (Redação dada pela Resolução n° 23.693/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-693-de-29-de-marco-de-2022)

Art. 68. Na hipótese de a urna em auditoria apresentar defeito que impeça o prosseguimento dos trabalhos, a Comissão de Auditoria da Votação Eletrônica adotará os mesmos procedimentos de contingência das urnas de seção.

Parágrafo único. Persistindo o defeito, a auditoria será interrompida, considerando-se a votação realizada até o momento.

Art. 69. Às 17 horas, será encerrada a votação, mesmo que a totalidade das cédulas não tenha sido digitada, adotando a Comissão de Auditoria da Votação Eletrônica as providências necessárias para a conferência dos resultados obtidos nas urnas verificadas.

Art. 70. Detectada a coincidência entre os resultados obtidos nos BUs e os dos relatórios emitidos pelo sistema de apoio à votação, será lavrada ata circunstanciada de encerramento dos trabalhos.

Art. 71. Na hipótese de divergência entre o BU e o resultado esperado, serão adotadas as seguintes providências:

I - localização das divergências; e

II - conferência da digitação das respectivas cédulas divergentes, com base no horário de votação.

~~Parágrafo único. Persistindo a divergência da votação eletrônica, proceder-se-á à conferência de todas as cédulas digitadas e ao registro minucioso em ata de todas as intercorrências, ainda que solucionadas.~~

§ 1º Persistindo a divergência da votação eletrônica, proceder-se-á à conferência de todas as cédulas digitadas e ao registro minucioso em ata de todas as intercorrências, ainda que solucionadas. (Renumerado pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

§ 2º No caso de indisponibilidade do sistema de apoio à auditoria de funcionamento das urnas eletrônicas, o Presidente da Comissão determinará a recontagem dos votos das cédulas no Sistema de Apuração instalado em urna eletrônica de contingência, para confirmação do resultado obtido na urna da seção submetida ao teste de integridade. (Incluído pela Resolução nº 23.711/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-711-de-20-de-setembro-de-2022)

Seção V

Da Conclusão dos Trabalhos

Art. 72. A ata de encerramento dos trabalhos será encaminhada ao respectivo TRE, que a remeterá ao TSE, em até 100 (cem) dias corridos, contados a partir do dia do primeiro turno das eleições.

§ 1º Os demais documentos e materiais produzidos serão lacrados, identificados como sendo da auditoria de funcionamento das urnas eletrônicas e encaminhados à Secretaria Judiciária do TRE, para arquivamento, durante o mesmo tempo estabelecido no Calendário Eleitoral para a manutenção dos arquivos de eleição, manutenção dos lacres dos equipamentos e instalação dos sistemas eleitorais.

§ 2º Os documentos e a identificação dos materiais produzidos serão rubricados pela Comissão de Auditoria da Votação Eletrônica, por fiscais e representante da empresa de auditoria presentes.

~~§ 3º As urnas utilizadas na auditoria de funcionamento das urnas eletrônicas permanecerão lacradas pelo mesmo tempo estabelecido no Calendário Eleitoral para as demais urnas de votação.~~

§ 3º As urnas e os equipamentos utilizados na auditoria de funcionamento das urnas eletrônicas, como os computadores utilizados com o SAVP, permanecerão armazenados e lacrados pelo mesmo tempo estabelecido no Calendário Eleitoral para as demais urnas de votação, sendo observado, no que couber, o previsto no Capítulo VII desta Resolução. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 4º Havendo questionamento por escrito quanto ao resultado da auditoria, o material permanecerá guardado até o trânsito em julgado da respectiva decisão.

Art. 73. A Comissão de Auditoria da Votação Eletrônica comunicará o resultado dos trabalhos ao juízo eleitoral do qual foram originadas as urnas auditadas.

Seção VI

Da Auditoria nas Eleições Suplementares

Art. 74. A realização de Teste de Integridade das Urnas Eletrônicas ocorrerá nas eleições suplementares para municípios com 100.000 (cem mil) ou mais eleitoras e/ou eleitores, podendo, a critério do TRE, ser realizada para os demais municípios:

Parágrafo único. A realização de Teste de Integridade das Urnas Eletrônicas em eleições suplementares seguirá todos os dispositivos desta Resolução, com as seguintes ressalvas:

I - realização em pelo menos 1 (uma) seção eleitoral por município, limitado às quantidades estabelecidas no art. 58 desta Resolução;

II - definição da seção eleitoral a ser submetida ao Teste de Integridade das Urnas Eletrônicas por meio de sorteio;

III - realização em ambiente controlado, em local público e com expressiva circulação de pessoas, podendo, a critério do TRE, ser realizada na capital ou no município onde ocorrerá a eleição suplementar;

IV - possibilidade de ser dispensada a presença de auditoras e auditores de instituição conveniada ou de empresa de auditoria contratada, desde que assegurada a presença de pessoas legitimadas junto ao TRE para fiscalizar o processo ou, na ausência destas, que o evento seja transmitido de forma on-line; e

V - possibilidade de flexibilização dos prazos estabelecidos nesta Resolução para a divulgação, organização e condução dos trabalhos e designação da Comissão de Auditoria da Votação Eletrônica, a critério do TRE e de forma a serem adequados ao calendário da eleição.

CAPÍTULO VI

DO TESTE DE AUTENTICIDADE DOS SISTEMAS ELEITORAIS

Seção I

Da Preparação da Auditoria

Art. 75. Finalizada a escolha ou o sorteio das seções eleitorais destinadas ao Teste de Autenticidade dos Sistemas Eleitorais, a pessoa que presidir a Comissão de Auditoria da Votação Eletrônica providenciará:

I - o relatório das correspondências entre as urnas e as seções escolhidas ou sorteadas, obtido pelo Sistema de Gerenciamento da Totalização do TRE, para compor a ata do evento; e

II - a comunicação imediata ao juiz eleitoral correspondente, informando-o sobre a seção escolhida ou sorteada e o número da respectiva correspondência da urna eletrônica.

Art. 76. A juíza ou o juiz cuja zona eleitoral realizará Teste de Autenticidade dos Sistemas Eleitorais, tão logo receba a comunicação de que trata o inciso II do art. 75 desta Resolução:

I - convocará os partidos políticos e os representantes da Ordem dos Advogados do Brasil e do Ministério Público, e dará publicidade às demais entidades fiscalizadoras sobre a necessidade de comparecimento ao local de votação com pelo menos 1 (uma) hora antes do início da votação, de modo a acompanhar a auditoria da urna eletrônica na seção eleitoral sorteada;

II - comunicará a pessoa que presidir a mesa receptora de votos sobre a auditoria na urna da respectiva seção eleitoral, repassando-lhe as devidas orientações sobre os procedimentos a serem adotados, observado o constante no § 4º do art. 72 desta Resolução, sem prejuízo de outras providências a critério do juízo eleitoral; e

III - providenciará o seguinte material, que ficará aos seus cuidados ou da pessoa que designou para conduzir a auditoria, no dia da votação, na seção eleitoral escolhida ou sorteada:

~~a) cópia do Comprovante de Carga, com a identificação do conjunto de lacres relativo à urna da seção eleitoral escolhida ou sorteada, para apresentá-lo à fiscalização durante os procedimentos de auditoria no dia da votação;~~

a) cópia do extrato de carga, com a identificação do conjunto de lacres relativo à urna da seção eleitoral escolhida ou sorteada, para apresentá-lo à fiscalização durante os procedimentos de auditoria no dia da votação; (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

b) Mídia de Resultado de ativação do VPP;

c) Mídia de Resultado para verificação da assinatura do TSE; e

d) lacre de reposição para a tampa do compartimento da Mídia de Resultado da urna.

Art. 77. Verificada a necessidade de substituição de urna no período entre a escolha ou o sorteio e o início da votação ou circunstância peculiar da seção eleitoral escolhida ou sorteada que impeça a realização dos trabalhos, o juízo eleitoral designará, de comum acordo com os representantes das entidades fiscalizadoras presentes, outra seção do mesmo local de votação ou de local próximo.

Seção II

Dos Procedimentos de Verificação

Art. 78. Na seção eleitoral cuja urna eletrônica será auditada, o juízo eleitoral determinará a realização dos seguintes procedimentos, por pessoa ou pessoas por ele designadas, cuidando para que sejam realizados, necessariamente, antes da emissão da zerésima pela urna:

~~I - exame do Comprovante de Carga, para verificar que se trata da urna da seção eleitoral escolhida ou sorteada;~~

I - exame do extrato de carga, para verificar que se trata da urna da seção eleitoral escolhida ou sorteada; (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

II - rompimento do lacre do compartimento da Mídia de Resultado;

III - retirada da Mídia de Resultado nela inserida; e

IV - verificação das assinaturas e dos resumos digitais pelo programa do TSE ou pelo programa de verificação apresentado pela pessoa interessada, ou ambos.

§ 1º Caso o programa de verificação de assinatura e do resumo digital a ser utilizado seja distinto do desenvolvido pelo TSE, a pessoa interessada providenciará, até a véspera da auditoria, cópia do programa em mídia apropriada, de acordo com orientações técnicas publicadas no sítio do Tribunal.

§ 2º O relatório de resumos digitais deverá ser impresso em até 3 (três) vias, mantendo-se, obrigatoriamente, 1 (uma) cópia para compor a ata da auditoria e colocando-se as demais à disposição das entidades fiscalizadoras para eventual futura conferência dos resumos digitais com aqueles publicados no sítio do TSE.

§ 3º Todas as vias do relatório de resumos digitais serão assinadas pelo juízo eleitoral ou por pessoa por ele designada, pela pessoa que preside a mesa receptora e por representantes das entidades presentes.

§ 4º A realização da auditoria será consignada na ata da mesa receptora da seção eleitoral, sem prejuízo da lavratura da ata prevista no art. 79, IV, desta Resolução.

Seção III

Da Conclusão dos Trabalhos

Art. 79. Concluída a verificação da assinatura e a impressão do relatório para verificação da integridade dos sistemas, serão adotados os seguintes procedimentos:

I - retirada das mídias de acionamento dos sistemas de verificação;

II - reinserção da Mídia de Resultado da urna eletrônica, retirada no início da auditoria;

III - lacração da tampa do compartimento da Mídia de Resultado com novo lacre, o qual será assinado pelo juízo eleitoral ou por pessoa por ele designada; e

IV - lavratura da ata circunstanciada de encerramento dos trabalhos, assinada pelo juízo eleitoral ou pessoa por ele designada e pelas demais pessoas presentes.

Parágrafo único. A partir da lavratura da ata da auditoria, o juízo eleitoral determinará o início dos trabalhos de votação na seção eleitoral.

Art. 80. A ata de encerramento dos trabalhos de verificação da autenticidade e integridade dos sistemas e a cópia impressa do relatório de resumos digitais, assinadas pelas pessoas presentes, serão encaminhadas ao respectivo cartório eleitoral para posterior envio à Comissão de Auditoria da Votação Eletrônica.

§ 1º A Comissão de Auditoria da Votação Eletrônica, de posse de todo o material remetido pelos cartórios eleitorais, encaminhá-lo-á à Secretaria Judiciária do TRE, para arquivamento.

§ 2º Havendo questionamento quanto ao resultado da auditoria, o material permanecerá guardado até o trânsito em julgado da respectiva decisão.

§ 3º Na hipótese do § 2º, é facultada aos partidos, às coligações e às federações a indicação de assistentes técnicos para acompanharem as verificações realizadas no curso do processo administrativo ou judicial. (Incluído pela Resolução n° 23.687/2022) (https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-687-de-3-de-marco-de-2022)

CAPÍTULO VII

DA PRESERVAÇÃO E CUSTÓDIA DOS DADOS

Art. 81. Os meios de armazenamento de dados utilizados pelos sistemas eleitorais e as cópias de segurança dos dados, serão identificados e mantidos em condições apropriadas, até a data estabelecida no Calendário Eleitoral.

Parágrafo único. Após a data mencionada no caput, os pedidos de auditoria que tenham por objeto computadores e mídias formatados ficarão prejudicados, sendo possível o acesso somente às cópias dos arquivos armazenados pela Justiça Eleitoral. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 82. Os meios de armazenamento de dados e as cópias de segurança dos dados serão ser descartados, e os sistemas eleitorais, desinstalados a partir de data estabelecida no Calendário Eleitoral, desde que os procedimentos a eles inerentes não estejam sendo objeto de discussão em procedimento administrativo ou processo judicial impugnando ou auditando a votação.

~~Art. 83. A JE preservará a integridade dos arquivos de log gerados durante o processo de envio, recebimento e processamento dos BUs.~~

Art. 83. A Justiça Eleitoral preservará a integridade dos arquivos de log gerados durante o processo de envio, recebimento e processamento dos boletins de urna até a data estabelecida no Calendário Eleitoral. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

CAPÍTULO VIII

DOS CASOS OMISSOS

Art. 84. Procedimentos de fiscalização e auditoria não previstos nesta Resolução somente serão realizados se autorizados pelo(a) presidente do TSE ou do TRE, no âmbito de sua jurisdição, observados os limites estabelecidos no art. 86 desta Resolução.

Art. 85. Todo procedimento previsto neste capítulo que venha a ser autorizado será realizado por pessoa técnica da JE ou da Polícia Federal, nos seguintes locais:

I - nas dependências do Tribunal Superior Eleitoral para verificações análogas às dispostas no capítulo III desta Resolução (verificação da integridade do código);

II - onde estiver instalado o programa de computador;

III - nos tribunais regionais eleitorais; ou

IV - em qualquer outro local estabelecido na autorização.

§ 1º Caso o procedimento autorizado exija acesso aos dados gravados em mídias digitais, os trabalhos serão precedidos de sua duplicação, de forma a preservar sua integridade antes da execução.

§ 2º Os equipamentos, mídias e documentos utilizados serão preservados até a conclusão dos procedimentos de fiscalização e auditoria ou até o trânsito em julgado de eventual processo constituído.

Art. 85-A. O procedimento administrativo não previsto nesta Resolução e a ação judicial que questionarem o funcionamento dos sistemas de votação ou de apuração somente serão admitidos se apresentados indícios substanciais de anomalia técnica atestados sob responsabilidade de profissional habilitado. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§1º O procedimento administrativo disciplinado no caput será dirigido ao Tribunal Eleitoral competente. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§2º A(o) requerente, a autora ou o autor responderão em caso de atuação temerária ou de litigância de má-fé, devendo ser aplicada multa proporcional à gravidade na conduta e, se for ocaso, adotadas as providências para apuração de infração ético-disciplinar e ilícitos penais. (Incluído pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

~~Art. 86. Havendo ação judicial relativa aos sistemas de votação ou de apuração, a autoridade judiciária designará dia e hora para realização de audiência pública, intimando o partido, coligação ou a federação reclamante, o Ministério Público, a Ordem dos Advogados do Brasil e demais pessoas interessadas, ocasião em que será escolhida e separada uma amostra das urnas eletrônicas alcançadas pela ação.~~

Art. 86. Admitida a petição apresentada nos termos do caput do art. 85-A, a autoridade judiciária designará dia e hora para realização de audiência pública, intimando o partido, a coligação ou a federação reclamante, o Ministério Público, a Ordem dos Advogados do Brasil e as demais pessoas interessadas, sendo então escolhida e separada uma amostra das urnas eletrônicas questionadas na ação. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 1º As urnas eletrônicas que comporão a amostra serão sorteadas entre todas aquelas que foram utilizadas nas seções eleitorais ou considerando-se delimitação a ser apontada pela pessoa recorrente, hipóteses em que ficarão lacradas até o encerramento do processo de auditoria.

§ 2º Para as eleições municipais, a quantidade de urnas que representará a amostra observará os seguintes percentuais, considerando-se o número de seções do município:

I - até 37 - 92% (noventa e dois por cento);

II - de 38 a 83 - 83% (oitenta e três por cento);

III - de 84 a 156 - 72% (setenta e dois por cento);

IV - de 157 a 271 - 59% (cinquenta e nove por cento);

V - de 272 a 445 - 47% (quarenta e sete por cento);

VI - de 446 a 671 - 37% (trinta e sete por cento);

VII - de 672 a 989 - 28% (vinte e oito por cento);

VIII - de 990 a 1.389 - 22% (vinte e dois por cento);

IX - de 1.390 a 1.940 - 17% (dezessete por cento);

X - de 1.941 a 2.525 - 13% (treze por cento);

XI - de 2.526 a 3.390 - 10% (dez por cento);

XII - de 3.391 a 4.742 - 8% (oito por cento);

XIII - de 4.743 a 6.685 - 5% (cinco por cento);

XIV - de 6.686 a 11.660 - 3% (três por cento); e XV - acima de 11.661 - 2% (dois por cento).

§ 3º Para as eleições gerais, a quantidade de urnas que representará a amostra observará os seguintes percentuais, considerando-se o número de seções do município:

I - até 1.000: 69% (sessenta e nove por cento);

II - de 1.001 a 1.500: 52% (cinquenta e dois por cento);

III - de 1.501 a 2.000: 42% (quarenta e dois por cento);

IV - de 2.001 a 3.000: 35% (trinta e cinco por cento);

V - de 3.001 a 4.000: 27% (vinte e sete por cento);

VI - de 4.001 a 5.000: 21% (vinte e um por cento);

VII - de 5.001 a 7.000: 18% (dezoito por cento);

VIII - de 7.001 a 9.000: 14% (quatorze por cento);

IX - de 9.001 a 12.000: 11% (onze por cento);

X - de 12.001 a 15.000: 8% (oito por cento);

XI - de 15.001 a 20.000: 7% (sete por cento);

XII - de 20.001 a 30.000: 5% (cinco por cento);

XIII - de 30.001 a 40.000: 3,5% (três e meio por cento);

XIV - acima de 40.000: 3% (três por cento).

§ 4º Caso haja ação judicial entre o primeiro e o segundo turno com decisão de constituição de amostra das urnas eletrônicas, a amostra será constituída após o segundo turno, podendo o juízo eleitoral ou a autoridade competente decidir pela constituição antecipada da amostra caso esta não traga prejuízos para realização do segundo turno.

§ 5º O partido, a coligação ou a federação requerente indicará técnicas ou técnicos ou auditoras e /ou auditores próprios para acompanharem os trabalhos de auditoria, que serão realizados por integrantes do quadro de pessoal ou pessoas devidamente designadas pela autoridade administrativa do órgão.

~~§ 6º Na hipótese do caput deste artigo, até o encerramento do processo de auditoria, os cartões de memória de carga permanecerão lacrados e as mídias de resultado com os dados das respectivas urnas escolhidas serão preservadas.~~

§ 6º Até o encerramento do processo de auditoria a que se refere o caput deste artigo, os cartões de memória de carga permanecerão lacrados e as mídias de resultado com os dados das respectivas urnas escolhidas e os computadores utilizados para a geração das mídias serão preservados. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

§ 7º Caso seja verificada qualquer inconsistência nas urnas conferidas por amostragem ou diante de fato relevante, a autoridade judiciária poderá ampliar os percentuais previstos nos § 2º e § 3º deste artigo até a totalidade das urnas do município.

~~Art. 87. Nas Eleições 2022, no dia da eleição, todas as unidades da federação, sem exceção, observarão o mesmo horário oficial de Brasília.~~

Art. 87. No dia das eleições, o horário oficial de Brasília será observado em todas as unidades da federação, desde a instalação das seções eleitorais até a divulgação de resultados. (Redação dada pela Resolução nº 23.728/2024) (https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-728-de-27-de-fevereiro-de-2024)

Art. 88. Fica revogada a Resolução nº 23.603 (https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-603-de-12-de-dezembro-de-2019) , de 12 de dezembro de 2019.

Art. 89. Esta Resolução entra em vigor na data de sua publicação oficial.

Brasília, 14 de dezembro de 2021.

MINISTRO EDSON FACHIN - RELATOR

Este texto não substitui o publicado no DJE-TSE, nº 236, de 23.12.2021, p. 28-48.
(https://sintse.tse.jus.br/documentos/2021/Dez/23/diario-da-justica-eletronico-tse-edicao-eleitoral/resolucao-no-23-673-de-14-de-dezembro-de-2021-dispoe-sobre-os-procedimentos-de-fiscalizacao-e-audito)

7.23 Anexo W – Res.-TSE n. 23.728/2024

Tribunal Superior Eleitoral
Secretaria de Gestão da Informação e do Conhecimento
Coordenadoria de Jurisprudência e Legislação
Seção de Legislação

RESOLUÇÃO Nº 23.728, DE 27 DE FEVEREIRO DE 2024

Altera a Resolução-TSE nº 23.673, de 14 de dezembro de 2021, que dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação.

O TRIBUNAL SUPERIOR ELEITORAL, no uso das atribuições que lhe conferem o inciso IX do art. 23 do Código Eleitoral (http://www.planalto.gov.br/ccivil_03/leis/L4737.htm#art23) e o art. 105 da Lei nº 9.504, de 30 de setembro de 1997 (http://www.planalto.gov.br/ccivil_03/leis/l9504.htm#art105),

RESOLVE:

Art. 1º A Res.-TSE nº 23.673/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021) passa a vigorar com as seguintes alterações:

"Art. 3º (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art3) .....

.....

VII - Votação, Apuração da Urna Eletrônica e demais aplicativos da urna eletrônica (Ecossistema da Urna): conjunto de programas executados na urna eletrônica que permite a escolha do voto, a justificativa de não comparecimento para votar, a apuração de resultados da seção eleitoral, entre outras funcionalidades;

.....

XIV - SAVP-Sorteio: aplicativo de apoio ao processo de sorteio de seções para diversas modalidades de auditoria previstas nesta Resolução;

XV - SAVP-Votação: aplicativo de apoio ao teste de integridade, que auxilia na verificação dos votos registrados durante a auditoria." (NR)

"Art. 4º (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art4) .....

.....

IV - Verificador Pré/Pós-Eleição (VPP): destinado à verificação da integridade dos sistemas instalados na urna e da autenticidade dos dados; à demonstração da votação; à visualização das informações de candidatas e candidatos e de eventos de log da urna; e à impressão do BU, Justificativa Eleitoral (RJE) e RDV.

.....

Parágrafo único. É vedada a utilização, pelos órgãos da Justiça Eleitoral, de qualquer outro sistema em substituição ou com finalidade similar aos desenvolvidos ou autorizados pelo TSE." (NR)

"Art. 5º (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art5) .....

.....

V - durante os procedimentos preparatórios para realização dos testes de integridade e de autenticidade e no dia da votação:

.....

VII - durante o Teste de Autenticidade dos Sistemas Eleitorais:

.....

c) verificação da integridade e da autenticidade dos programas instalados na urna eletrônica; e

....." (NR)

"Art. 9º É garantido, às entidades fiscalizadoras, a partir de 12 (doze) meses antes do primeiro turno das eleições, até a compilação dos sistemas, prevista no art. 19 desta Resolução, o acesso antecipado aos sistemas eleitorais desenvolvidos pelo Tribunal Superior Eleitoral e o acompanhamento dos trabalhos para sua especificação e seu desenvolvimento, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal.

....." (NR)

"Art. 10 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art10). .....

.....

§ 3º No período de acompanhamento da especificação e do desenvolvimento dos sistemas, poderão ser disponibilizadas múltiplas versões dos sistemas abertos para análise, as quais estarão disponíveis no ambiente descrito no caput para comparação das mudanças efetuadas pelas equipes de desenvolvimento." (NR)

"Art. 12. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art12) .....

.....

§ 3º As pessoas representantes das entidades fiscalizadoras poderão apenas consultar os resultados dos testes e dados estatísticos obtidos com o respectivo programa de análise de código apresentado, não sendo permitida sua extração, impressão ou reprodução por nenhuma forma, sendo autorizado seu compartilhamento às demais entidades e instituições legitimadas, desde que se restrinja ao ambiente de verificação dos códigos-fonte." (NR)

"Art. 15. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art15) .....

Parágrafo único. O Tribunal Superior Eleitoral, por sua Secretaria de Tecnologia da Informação, requisitará à entidade fiscalizadora as licenças de uso das ferramentas de desenvolvimento empregadas na construção do programa, se não as possuir, para uso e guarda até a realização das eleições."(NR)

"Art. 17. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art17) .....

Parágrafo único. Os programas de verificação desenvolvidos poderão ser cedidos a qualquer entidade fiscalizadora." (NR)

"Art. 37. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art37) .....

§ 1º A verificação por amostragem será realizada em até 6% (seis por cento) das urnas preparadas para cada zona eleitoral, escolhidas pelos representantes das entidades fiscalizadoras, de forma aleatória, entre as urnas de votação e as de contingência.

....." (NR)

"Art. 43. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art43) Até a antevéspera do dia das eleições, a juíza ou o juiz eleitoral realizará audiência destinada à verificação da integridade e autenticidade dos sistemas Transportador e JEConnect, instalados nos microcomputadores.

....." (NR)

"Art. 46. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art46) .....

.....

VI - relatório Resultado da Totalização emitido pelo Sistema de Gerenciamento da Totalização (SISTOT), incluindo a relação das seções em que o boletim de urna tenha sido gerado em urna substituta;

....." (NR)

"Art. 48. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art48) .....

Parágrafo único. Os arquivos de dados listados nesta seção ficarão disponíveis pelo prazo estabelecido no Plano de Classificação, Avaliação e Destinação das Informações e dos Documentos.

....." (NR)

"Art. 50. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art50) Se for necessário, a pessoa requerente deverá fornecer as mídias para a gravação dos arquivos, contando-se o prazo previsto no art. 49 desta Resolução a partir da data em que fornecê-las."(NR)

"Art. 51. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art51) As entidades fiscalizadoras poderão solicitar verificação após o pleito, desde que sejam relatados fatos e apresentados indícios e circunstâncias que a justifiquem, sob pena de indeferimento liminar.

.....

§ 2º A solicitação, acompanhada de plano de trabalho, será dirigida ao tribunal eleitoral competente, que decidirá sobre o pedido.

....." (NR)

"Art. 53-C. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art53c) .....

I - .....

.....

b) instaladas necessariamente em todas as capitais dos Estados e no Distrito Federal; e

....." (NR)

"Art. 55. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art55) Para a organização e a condução dos trabalhos mencionados nos capítulos V e VI desta Resolução, será designada pelos tribunais regionais eleitorais, em sessão pública, até 60 (sessenta) dias antes das eleições, Comissão de Auditoria da Votação Eletrônica composta por:

....." (NR)

"Art. 57. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art57) A Comissão de Auditoria da Votação Eletrônica promoverá, entre as 7 horas e as 12 horas, do dia anterior às eleições, no primeiro e no segundo turno, em local e horário previamente divulgados, a definição das seções eleitorais que serão submetidas às auditorias a que se referem os capítulos V e VI desta Resolução.

....." (NR)

"Art. 58. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art58) .....

.....

§ 2º Não poderá ser escolhida ou sorteada mais de 1 (uma) seção por zona eleitoral, salvo nas hipóteses em que o número de zonas eleitorais vinculadas ao Tribunal Regional seja inferior ao exigido para atender ao quantitativo previsto neste artigo." (NR)

"Art. 59. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art59) .....

.....

§ 5º Se o número de zonas eleitorais dos Municípios da unidade da federação onde houver segundo turno for inferior aos quantitativos previstos nos incisos I, II e III, o teste de autenticidade será realizado em urnas equivalentes ao número de zonas eleitorais." (NR)

"Art. 60. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art60) A Comissão de Auditoria da Votação Eletrônica poderá, de comum acordo com representantes das entidades fiscalizadoras:

I - dividir os Municípios da unidade da federação em grupos, a fim de assegurar a representatividade regional das seções eleitorais escolhidas ou sorteadas para a realização do teste de integridade das urnas eletrônicas;

II - excluir do sorteio ou da escolha as seções eleitorais instaladas em localidades de difícil acesso, onde seja inviável recolher a urna em tempo hábil para a realização do teste." (NR)

"Art. 61. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art61) .....

§ 1º O juízo eleitoral providenciará o imediato transporte, para o local indicado pela Comissão de Auditoria da Votação Eletrônica, da urna, devidamente acondicionada em sua caixa, e de cópias da ata da cerimônia de carga e do extrato de carga, o qual deverá mostrar a numeração da cartela de lacres utilizada.

....." (NR)

"Art. 63. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art63) .....

§ 1º Na ausência de representantes dos partidos políticos, das federações e das coligações, a Comissão de Auditoria da Votação Eletrônica providenciará o preenchimento das cédulas por terceiras pessoas, excluídas as que servem à Justiça Eleitoral, podendo ser chamadas as servidoras e os servidores nomeados nos termos do § 2º do art. 67 desta Resolução e previamente convocados para a cerimônia.

§ 2º Cada participante definirá os números utilizados para preenchimento da cédula, podendo optar por voto nominal, voto de legenda ou voto em branco.

§ 3º Se o número utilizado para preencher a cédula não corresponder à candidatura registrada ou à legenda habilitada na eleição, o voto será considerado nulo."

"Art. 65. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art65) .....

§ 1º A fiscalização será realizada, em todas as fases dos trabalhos da auditoria de funcionamento das urnas eletrônicas, nos Tribunais Regionais Eleitorais, com exceção da coleta e do transporte desses equipamentos, por representante das instituições conveniadas ou das empresas previamente credenciadas pelo TSE.

....." (NR)

"Art. 66. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art66) A instituição conveniada ou a empresa de auditoria encaminhará ao Tribunal Superior Eleitoral, em até 5 (cinco) dias úteis após cada turno, relatório conclusivo da fiscalização realizada na auditoria de funcionamento das urnas eletrônicas.

.....

§ 2º Os relatórios individuais de auditoria de cada Tribunal Regional Eleitoral e o relatório consolidado conclusivo, elaborados pela instituição pública de fiscalização ou pela empresa especializada em auditoria contratada, serão publicados no sítio eletrônico da Justiça Eleitoral em até 30 (trinta) dias após o segundo turno." (NR)

"Art. 72. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art72)

.....

.....

§ 3º As urnas e os equipamentos utilizados na auditoria de funcionamento das urnas eletrônicas, como os computadores utilizados com o SAVP, permanecerão armazenados e lacrados pelo mesmo tempo estabelecido no Calendário Eleitoral para as demais urnas de votação, sendo observado, no que couber, o previsto no Capítulo VII desta Resolução." (NR)

"Art. 76. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art76) .....

.....

a) cópia do extrato de carga, com a identificação do conjunto de lacres relativo à urna da seção eleitoral escolhida ou sorteada, para apresentá-lo à fiscalização durante os procedimentos de auditoria no dia da votação;

....." (NR)

"Art. 78. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art78) .....

I - exame do extrato de carga, para verificar que se trata da urna da seção eleitoral escolhida ou sorteada;

....." (NR)

"Art. 81. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art81) .....

Parágrafo único. Após a data mencionada no caput, os pedidos de auditoria que tenham por objeto computadores e mídias formatados ficarão prejudicados, sendo possível o acesso somente às cópias dos arquivos armazenados pela Justiça Eleitoral." (NR)

"Art. 83. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art83) A Justiça Eleitoral preservará a integridade dos arquivos de log gerados durante o processo de envio, recebimento e processamento dos boletins de urna até a data estabelecida no Calendário Eleitoral." (NR)

"Art. 85-A. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art85a) O procedimento administrativo não previsto nesta Resolução e a ação judicial que questionarem o funcionamento dos sistemas de votação ou de apuração somente serão admitidos se apresentados indícios substanciais de anomalia técnica atestados sob responsabilidade de profissional habilitado.

§1º O procedimento administrativo disciplinado no caput será dirigido ao Tribunal Eleitoral competente.

§2º A(o) requerente, a autora ou o autor responderão em caso de atuação temerária ou de litigância de má-fé, devendo ser aplicada multa proporcional à gravidade na conduta e, se for ocaso, adotadas as providências para apuração de infração ético-disciplinar e ilícitos penais." (NR)

"Art. 86. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art86) Admitida a petição apresentada nos termos do caput do art. 85-A, a autoridade judiciária designará dia e hora para realização de audiência pública, intimando o partido, a coligação ou a federação reclamante, o Ministério Público, a Ordem dos Advogados do Brasil e as demais pessoas interessadas, sendo então escolhida e separada uma amostra das urnas eletrônicas questionadas na ação.

.....

§ 6º Até o encerramento do processo de auditoria a que se refere o caput deste artigo, os cartões de memória de carga permanecerão lacrados e as mídias de resultado com os dados das respectivas urnas escolhidas e os computadores utilizados para a geração das mídias serão preservados.

....." (NR)

"Art. 87. (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art87) No dia das eleições, o horário oficial de Brasília será observado em todas as unidades da federação, desde a instalação das seções eleitorais até a divulgação de resultados." (NR)

Art. 2º Ficam revogados:

I - o parágrafo único do art. 3º da Res.-TSE nº 23.673/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art3); e

II - o parágrafo único do art. 52 da Res.-TSE nº 23.673/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art52).

Art. 3º Os incisos I, II, III, IV e V do parágrafo único do art. 3º da Res.-TSE nº 23.673/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021#art3) serão renumerados, respectivamente, como incisos IX, X, XI, XII e XIII do caput do mesmo artigo.

Art. 4º Esta Resolução entra em vigor na data de sua publicação oficial.

Brasília, 27 de fevereiro de 2024.

MINISTRA CÁRMEN LÚCIA – RELATORA

Este texto não substitui o publicado no DJE-TSE, nº 29, de 4.3.2024, p. 168-172.
(https://sintse.tse.jus.br/documentos/2024/Mar/4/diario-da-justica-eletronico-tse-edicao-extraordinaria/resolucao-no-23-728-de-27-de-fevereiro-de-2024-altera-a-resolucao-tse-no-23-673-de-14-de-dezembro-de)

7.24 Anexo X – Relatório de esclarecimento

Relatório de Esclarecimento às Recomendações Proferidas pela Comissão Avaliadora do TPS 2023

Na data de 9 de junho de 2025, a Comissão Reguladora se reuniu e elaborou a seguinte manifestação quanto às recomendações proferidas pela Comissão Avaliadora do TPS 2023.

No que se refere ao item 4.1 do Relatório Final da Comissão Avaliadora que trata das recomendações quanto ao processo e ambiente de realização do TPS.

a. Disponibilizar documentos relativos aos processos e sistemas eleitorais de forma permanente, como apresentações sobre o processo eleitoral, módulos que compõem os sistemas e perguntas e respostas para dirimir dúvidas.

Manifestação da Comissão Reguladora: **Recomendação acolhida**. A Comissão Reguladora irá disponibilizar documentos dos sistemas eleitorais de forma permanente no site do Teste Público da Urna, tais como, apresentações das áreas técnicas da STI/TSE explicando o processo eleitoral, visão sistêmica dos sistemas eleitorais e seus módulos, entre outros. Ademais, os membros da Comissão Reguladora estão à disposição da Comissão Avaliadora e investigadores para dirimir quaisquer dúvidas, antes, durante e depois do Teste Público da Urna.

b. Disponibilizar acessórios de mercado, compatíveis com a urna, tais como: cabos, adaptadores, microfones, fones de ouvido e ferramentas para facilitar a execução dos testes pelos investigadores.

Manifestação da Comissão Reguladora: **Recomendação acolhida.** Durante a fase de execução dos testes, os acessórios básicos previstos no edital são previamente colocados à disposição dos investigadores de forma a garantir a execução dos planos de testes. Além disso, itens adicionais que não foram inicialmente incluídos no ambiente dos testes são prontamente providenciados, desde que disponíveis no ambiente do TSE, e entregues aos participantes, por meio de requisições específicas, devidamente autorizadas pela Comissão Reguladora.

c. Apresentar e permitir acesso a todo o ambiente disponibilizado para os testes em um momento anterior ao TPS.

Manifestação da Comissão Reguladora: **Recomendação acolhida**. O ambiente utilizado para a realização do teste é cuidadosamente preparado, com antecedência, para garantir a segurança do evento e a execução dos planos de testes. Sendo assim, é possível autorizar o acesso ao ambiente à Comissão Avaliadora com uma semana de antecedência aos testes, mediante agendamento prévio. E, durante a realização do Teste Público da Urna, os membros da Comissão Avaliadora têm acesso a todos os ambientes, inclusive à visualização dos códigos-fontes, mediante assinatura do Termo de Responsabilidade.

d. Disponibilizar uma visão sistêmica do código fonte de forma a nortear e facilitar a leitura do código, bem como, um mapa identificando os módulos e programas nos moldes do documento "Visão Sistêmica das Eleições".

Manifestação da Comissão Reguladora: **Recomendação acolhida.** O ambiente do Teste Público da Urna já possui diversas documentações dos módulos e programas que compõe os sistemas objetos do teste. Tais documentações estão em processo de melhoria contínua e serão disponibilizados novos diagramas correlacionando os diversos componentes dos sistemas. Ademais, os membros da Comissão Reguladora estão à disposição da Comissão Avaliadora e investigadores para dirimir quaisquer dúvidas, antes, durante e depois do Teste Público da Urna.

e. Disponibilizar um espaço, quando necessário, que permita gravação de som de um ambiente de eleições com mínimo ruído.

Manifestação da Comissão Reguladora: **Recomendação não acolhida.** As eleições ocorrem em ambientes naturalmente ruidosos. Assim, a disponibilização de salas especiais antirruído levaria à criação de circunstância atípica ao próprio processo eleitoral.

f. Criar um período de esclarecimento de dúvidas, posterior ao período de disponibilização dos vídeos e apresentação dos sistemas eleitorais, para o melhor entendimento dos processos e do código fonte.

Manifestação da Comissão Reguladora: **Recomendação acolhida**. Durante o período de visualização dos códigos-fontes os investigadores e membros da Comissão Avaliadora podem esclarecer suas dúvidas junto à equipe técnica. Adicionalmente, temos prevista a realização da Audiência Pública, que visa esclarecer dúvidas sobre o edital ou sobre o Teste Público em geral.

g. Avaliar a possibilidade de acesso ao código fonte além da estrutura do TSE, por exemplo, no ambiente dos TRE.

Manifestação da Comissão Reguladora: **Recomendação não acolhida.** O acesso aos códigos-fontes é restrito e normatizado em resolução do Tribunal Superior Eleitoral que prevê sua disponibilização em sala específica construída para esse fim. Art. 10 da Resolução TSE nº 23.673, caput:

Art. 10. O acompanhamento dos trabalhos será realizado no TSE, em ambiente controlado, sem acesso à internet, sendo vedado portar qualquer dispositivo que permita o registro ou a gravação de áudio ou imagem e retirar, sem a expressa autorização da STI/TSE, qualquer elemento ou fragmento dos sistemas ou programas elaborados ou em elaboração.

h. Disponibilizar infraestrutura de instalação de software no ambiente de Teste Público de Segurança a fim de agilizar a instalação de ferramentas pelas equipes para a realização dos testes aprovados.

Manifestação da Comissão Reguladora: **Recomendação acolhida.** Será disponibilizada uma terceira estação de trabalho contendo as ferramentas mais utilizadas do mercado para testes de

segurança. Ademais, havendo a necessidade de outras ferramentas estas poderão ser obtidas pelos investigadores a partir de solicitação direcionada à Comissão Reguladora.

i. Disponibilizar durante a fase de confirmação do TPS, uma ferramenta que permita a comparação de forma visual dos códigos alterados.

Manifestação da Comissão Reguladora: **Recomendação acolhida.** Será disponibilizada ferramenta que permita a comparação de forma visual dos códigos alterados.

j. Providenciar a configuração do ambiente de TPS para cada equipe, conforme estabelecido no plano de teste aprovado. Para tal, é essencial:

1. Examinar o plano de teste elaborado pelos investigadores, identificando a necessidade de quaisquer equipamentos externos necessários para a realização dos testes. Na eventualidade de tais equipamentos serem de responsabilidade do Tribunal Superior Eleitoral (TSE), estes deverão ser preparados e disponibilizados antecipadamente. No caso de os equipamentos serem providos pelos investigadores, recomenda-se que sejam entregues com antecipação, visando minimizar atrasos e otimizar o processo de espera e liberação deles no momento da execução dos testes.

Manifestação da Comissão Reguladora: **Recomendação parcialmente acolhida.** A configuração do ambiente do investigador pode depender de equipamentos providos pelo TSE ou pelo próprio investigador. No primeiro caso, os equipamentos são disponibilizados devidamente configurados previamente ao início do teste. No que diz respeito aos equipamentos trazidos pelos investigadores, é reservado a eles período inicial para efetivar a devida configuração. Registra-se que, em suas versões iniciais, o TPS consistia de período de três dias de execução que foi posteriormente ampliado podendo chegar até seis dias incluindo a configuração dos equipamentos trazidos pelos investigadores.

2. Disponibilizar uma urna desmontada para facilitar a visualização dos componentes internos e dos cabos com a devida documentação fornecida pelos fabricantes.

Manifestação da Comissão Reguladora: **Recomendação acolhida.** Será disponibilizada uma urna desmontada na área de inspeção dos códigos-fonte.

4. Quanto ao item 4.2 - Recomendações Gerais do Relatório Final da Comissão Avaliadora.

a. A transparência e a rastreabilidade no processo eletrônico de votação são fundamentais para a manutenção da confiança pública nas eleições. Nesse contexto, é essencial que o TSE permita um acompanhamento amigável e detalhado do processo de votação eletrônica para os diversos segmentos da sociedade, incluindo partidos políticos, universidades, público especializado e participantes do Teste Público de Segurança (TPS).

Para garantir um entendimento claro e abrangente do processo eleitoral, deve-se adotar uma abordagem que inclua explicações detalhadas e visuais das etapas de votação,

processamento e totalização dos votos. A apresentação didática de cada fase, desde a inserção do voto até o armazenamento e totalização dos dados, é crucial para garantir a compreensão pública e a confiança no sistema.

A apresentação dos códigos fonte aos diversos segmentos da sociedade, por exemplo, é essencial para assegurar a transparência e a confiabilidade do processo eleitoral. A disponibilização desses códigos deve ser acompanhada do uso de ferramentas adequadas para auditoria de código fonte, que permitam uma análise minuciosa e independente. Ao segmentar o código em módulos compreensíveis e auditáveis, e ao utilizar plataformas de auditoria que destacam possíveis vulnerabilidades, o TSE não apenas reforça a transparência e a confiança no processo eleitoral, mas também promove um ambiente de colaboração e escrutínio técnico que é essencial para a integridade e credibilidade das eleições.

Outrossim, faz-se importante a implementação de metodologias robustas para assegurar a integridade dos dados. Disponibilizar mecanismos de auditoria detalhados e acessíveis permitirá que especialistas em segurança da informação, representantes de partidos políticos e cidadãos interessados verifiquem o funcionamento interno dos sistemas eleitorais.

A adoção dessas medidas tornará o processo eleitoral mais acessível e confiável, fortalecendo a confiança pública e a legitimidade das eleições. É vital que o TSE continue a evoluir suas práticas, sempre com o objetivo de promover a transparência, a rastreabilidade, a integridade, a observabilidade e a verificabilidade do processo eleitoral, atendendo às expectativas de todos os envolvidos e promovendo uma democracia robusta e confiável.

Manifestação da Comissão Reguladora: Estão em curso as ações de aprimoramento contínuo dos processos de transparência, fiscalização e auditoria do sistema de votação. A Resolução TSE nº 23.673, que dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação, e todos os seus desdobramentos são aprimorados a cada pleito eleitoral em conformidade com a recomendação supracitada.

b. O TSE tem buscado evoluir a segurança e a transparência do sistema eleitoral em parceria com universidades brasileiras. Um desses aperfeiçoamentos é o mecanismo conhecido como "verificabilidade fim-a-fim", que permite aos eleitores uma confiança ainda maior de que suas escolhas foram registradas corretamente, sem diminuir o sigilo dos votos lançados. Projetos desse tipo, desenvolvidos conjuntamente por técnicos do TSE e pesquisadores brasileiros, abrem um novo caminho para a evolução contínua do sistema eleitoral brasileiro e devem ser incentivados;

Manifestação da Comissão Reguladora: O TSE busca, a partir das parcerias com as instituições de ensino superior, o engajamento da sociedade acadêmica nas pesquisas para o aprimoramento do sistema eletrônico de votação. Com isso, corrobora a manifestação da Comissão Avaliadora.

c. Considerando que os códigos fontes dos sistemas eleitorais desenvolvidos para a realização das eleições são complexos e extensos, e que as documentações existentes ainda são insuficientes para ampliar as abordagens de verificação e auditoria, seria recomendável avaliar os meios e os processos que podem agregar novos caminhos facilitando o acompanhamento técnico e processual

dos produtos empregados pela Justiça Eleitoral na preparação e operação das eleições, melhorando o fator "transparência" e "confiabilidade";

Manifestação da Comissão Reguladora: Quanto a esse item, esta Comissão já se manifestou nas alíneas "a" e "d" das considerações quanto ao processo e ambiente de realização do TPS (item 4.1 do Relatório da Comissão Avaliadora).

d. O FORTI, um encontro dos membros técnicos envolvidos em sistemas de tecnologia da informação, foi criado para compartilhamento dos conhecimentos técnicos e produtos internos desenvolvidos pelo TSE e TRE e trouxe um ganho sensível de produtividade e interação entre as equipes. Tendo em vista que a Justiça Eleitoral tem colhido muitos resultados positivos desta iniciativa, recomenda-se que seja avaliado a possibilidade de dar continuidade ao processo buscando o aprimoramento desta sinergia, em especial nas discussões e estudos de novas tecnologias de desenvolvimento de sistemas e segurança, assegurando a vanguarda na qualidade e tranquilidade das eleições no país;

Manifestação da Comissão Reguladora: Esta comissão entende que não é de sua alçada deliberar sobre o tema.

e. A Comissão Avaliadora, composta por especialistas não vinculados à Justiça Eleitoral, poderia ter a sua missão melhor especificada para uma atuação mais completa no contexto do TPS. O TPS é um nome dado inicialmente para a realização de um evento pontual que reúne os candidatos interessados na verificação dos sistemas eleitorais desenvolvidos para as eleições do ano subsequente. Todavia, após a realização de vários eventos, verifica-se não somente a qualidade das abordagens propostas, mas uma diversificação das metodologias e focos, tornando cada evento mais abrangente que os anteriores. Uma característica evolutiva que faz com que a abrangência das informações buscadas sejam ampliadas desde a concepção até a finalização das eleições. Assim sendo, a atuação da Comissão Avaliadora poderia acompanhar esta visão, ampliando a sua participação em todo o sistema eleitoral, concluindo o processo com a realização do TPS.

Manifestação da Comissão Reguladora: Esta comissão entende que não é de sua alçada deliberar sobre o tema.

Por fim, ressalta-se que essas respostas foram apresentadas à Diretoria-Geral deste Tribunal, no dia 10 de junho de 2025, por meio do Despacho do Secretário de Tecnologia da Informação (SEI 3260855) , constante do processo SEI 2023.00.000006577-4.

Secretaria de Tecnologia da Informação (STI)

Núcleo Estratégico de Comunicação de Informática (Neci)

Maio/2024

Esta obra foi composta na fonte Aktiv Grotesk, corpo 12 e entrelinhas de 16 pontos.

Tribunal
Superior
Eleitoral