

# Avaliações sobre o Teste de Segurança

Comissão de Avaliação:

## 1. Planos de Teste

Os planos de testes apresentados em resposta ao edital, dos Testes Públicos de Segurança do Sistema Eletrônico de Votação, pelos seis grupos e três investigadores individuais totalizaram dezenove propostas.

### 1.1 Dos Planos de Teste não Realizados e não Avaliados

Alguns dos planos de teste originalmente propostos para execução durante o evento não foram realizados por motivos diversos. Quais sejam: (a) indeferimento da Comissão Disciplinadora, (b) falta de material, (c) falta de tempo hábil para execução do teste com completude, (d) deferimento parcial da Comissão Disciplinadora e não execução.

- (a) Segue abaixo a relação dos indeferidos pela Comissão Disciplinadora por estarem em desacordo com o escopo definido para a investigação<sup>1</sup>:
- G2PT1 – Quebra de sigilo do voto utilizando um aparelho celular
  - G4PT1 – Injeção de código e violação da rotina de aleatoriedade
  - G5PT4 – Quebra do sigilo do voto eletrônico
  - I3PT1 – Comprometimento da transferência dos resultados obtidos nas urnas para o servidor do TRE/TSE
- (b) O plano de teste G5PT3, "Tentativa de comprometimento do MSD através da interface JTAG", não foi realizado por não apresentar especificação para a confecção de interface de dados necessária para a execução do mesmo.
- (c) Os seguintes planos não foram realizados por motivos dos investigadores admitirem não haver tempo suficiente para sua completa execução:
- G1PT2 – Tentativa não rastreável de fraude no resultado da votação
  - G4PT4 – Mapeamento de voto com o eleitor
- (d) Os seguintes planos não foram realizados por terem sido deferidos parcialmente pela Comissão Disciplinadora e não tendo sido executados.
- G2PT2 – Fraude no sistema de apuração utilizado no exterior

<sup>1</sup> Anotação: Para fins de identificação dos testes, os grupos e os investigadores individuais serão representados pelas letras "G" e "I", respectivamente e o plano de trabalho por "PT", seguido de numeração seqüencial de ordenamento de cada teste nas propostas apresentadas.

Todos os planos de testes não realizados não foram considerados pela Comissão Avaliadora para fins de avaliação.

### 1.2 Dos Planos de Teste Realizados e não Avaliados

Os planos de teste submetidos ao Teste Público de Segurança que foram executados, mas que não apresentaram contribuição relevante para o processo de aprimoramento do Sistema Eletrônico de Votação não foram avaliados por esta Comissão Avaliadora. Foi também observado que os referidos testes não foram concluídos conforme previsto nos seus respectivos planos de teste submetidos e aprovados pela Comissão Disciplinadora.

Os testes realizados e não avaliados são:

- G3PT1 – Boot com loader não assinado
- G3PT2 – USB-Ethernet
- G4PT2 – Invalidação do FlashCard
- G4PT3 – Proposta de Execução de Shellcode
- G6PT1 – Teste de Segurança do Sistema Eletrônico de Votação do TSE
- I1PT1 – Extração de Dados da Memória RAM da Urna Eletrônica
- I2PT1 – Teste de exploração dos Mecanismos de proteção de carga da Urna

### 1.3 Dos Planos de Teste Realizados e Avaliados

Os seguintes planos de teste foram realizados e avaliados, pois apresentam contribuições ao processo de aprimoramento do Sistema Eletrônico de Votação. Todos os testes avaliados, mesmo não tendo atingido todos os objetivos declarados no plano de testes submetidos, apresentaram resultados intermediários relevantes.

- G1PT1 – Tentativa não rastreável de quebra de sigilo de votação
- G3PT3 – Clonagem de memória flash de votação
- G5PT1 – Modificação do boot da urna
- G5PT2 – Tentativa de recuperação de dados da memória volátil do equipamento

## 2. Avaliação

- G1PT1 – Tentativa não rastreável de quebra de sigilo de votação
  - $\Delta t = 4$  (176 minutos até o primeiro resultado relevante)
  - P = 4 pontos de intervenção
    - Visualizar Código Fonte
    - Acesso físico:
      - Urna Eletrônica
      - Lacs
      - Mídia de Resultado (arquivos do RDV)
  - A = 1 (Falha)
  - E = 1 (Seção)

*(Handwritten signatures and initials in blue ink)*

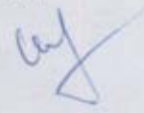

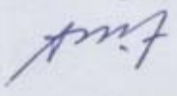

- Apresenta recomendações para o aprimoramento da segurança do ponto explorado.
  
- G3PT3 – Clonagem de memória flash de votação
  - $\Delta t = 4$  (130 minutos até o primeiro resultado relevante)
  - P = 4 pontos de intervenção
    - Visualizar Código Fonte
    - Acesso físico:
      - Urna Eletrônica
      - Lacres
      - Flash de Votação
  - A = 1 (Falha)
  - E = 1 (Urna)
  
- G5PT1 – Modificação do boot da urna
  - $\Delta t = 3$  (110 minutos até o primeiro resultado relevante)
  - P = 4 pontos de intervenção
    - Visualizar Código Fonte
    - Acesso físico:
      - Urna Eletrônica
      - Lacres
      - Flash de Carga
  - A = 1 (Falha)
  - E = 1 (Urna)
  
- G5PT2 – Tentativa de recuperação de dados da memória volátil do equipamento
  - $\Delta t = 7$  (280 minutos até o primeiro resultado relevante)
  - P = 4 pontos de intervenção
    - Visualizar Código Fonte
    - Acesso físico:
      - Urna Eletrônica
      - Lacres
      - Memória RAM
  - A = 1 (Falha)
  - E = 1 (Urna)

### 3. Planos não Realizados, mas com Considerações

Os planos de trabalho de teste dos grupos G6 e G2, em que se pese que não foram executados, possuem contribuições relevantes para o sistema eletrônico de votação. As propostas devem ser observadas e analisadas pelo TSE.

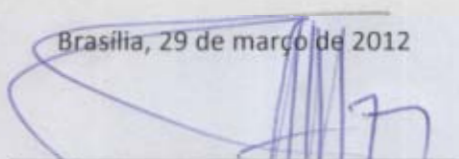
### 4. Pontuação Final e Classificação para fins de premiação

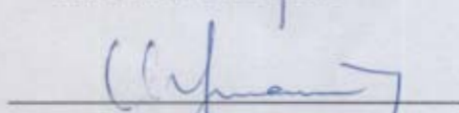
Segundo a fórmula definida para o critério de classificação, conforme apresentado no Edital nº 5/2012, a pontuação final dos grupos finalistas é apresentada a seguir:

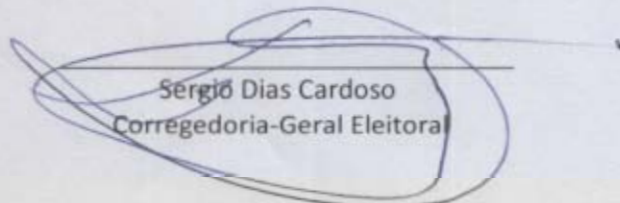
  




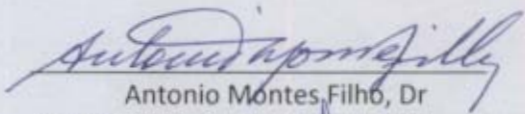
Grupo/Plano	Tempo ( $\Delta t$ )	Pontos Intervenção (P)	Tipo Ataque (A)	Extensão do Ataque (E)	Solução Recomendada	Pontuação Final
G1PT1	4	4	1	1	2	0,0313
G5PT1	3	4	1	1	1	0,0208
G3PT3	4	4	1	1	1	0,0156
G5PT2	7	4	1	1	1	0,0089

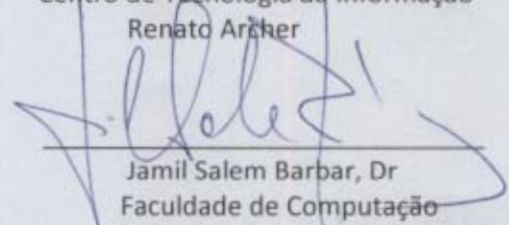
Brasília, 29 de março de 2012

  
 Mamede Lima-Marques, Dr  
 Departamento de Ciência da Comunicação  
 Universidade de Brasília

  
 Osvaldo Catsumi Imamura, Dr  
 Instituto de Estudos Avançados  
 Departamento de Ciência e Tecnologia Aeroespacial

  
 Sérgio Dias Cardoso  
 Corregedoria-Geral Eleitoral

  
 Antonio Montes Filho, Dr  
 Centro de Tecnologia da Informação  
 Renato Archer

  
 Jamil Salem Barbar, Dr  
 Faculdade de Computação  
 Universidade Federal de Uberlândia