TPS 2021
6ª edição

Relatório final da Comissão Avaliadora

Brasília, 30 de maio de 2022.

1 Introdução

A Comissão Avaliadora, designada pela Portaria TSE nº 588, de 10 de setembro de 2021, 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 11 membros, contou nesta segunda etapa com a presença dos representantes dos seguintes órgãos:

- TSE – Dr. Sandro Nunes Vieira
- TSE – Dra. Christine Peter
- MPF – Patricia Sumie Hayakawa
- Congresso Nacional – Robson Paniago de Miranda
- PF – Perito Criminal Thiago de Sá Cavalcanti
- TCU – Auditor André Luiz Furtado Pacheco
- TCU – Auditor Cláudio Lisboa de Souza
- SBC – Professor Doutor Rafael Timóteo de Sousa Júnior
- Comunidade Acadêmica – Professor Doutor Mamede Lima-Marques
- Comunidade Acadêmica – Doutor Osvaldo Catsumi Imamura
- Comunidade Acadêmica – Professor Doutor Jamil Salem Barbar

O propósito deste relatório é apresentar os resultados dos testes de confirmação dos investigadores e grupos de investigadores.

2 Resultados do Teste de Confirmação

Nos dias 11, 12 e 13 de maio de 2022 foi realizada, no Tribunal Superior Eleitoral, a etapa Teste de Confirmação referente ao TPS 2021[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".

Estiveram presentes, nesta etapa, os grupos responsáveis pelos Planos de Teste 3, 6, 16 e 20.

2.1 Plano de Teste 3 [**Verificação do comportamento do parâmetro urna `mcriptografar`**)]. Foi verificado durante a abertura de investigação do código fonte um conjunto de parametrizações da urna que compõem a compilação do código para carga inicial. Dentre estes parâmetros, identificou-se o parâmetro `mcriptografar` - com parametrização default (*True*). Entendemos ser uma possível vulnerabilidade porque poderia desabilitar a criptografia com sua alteração. Precisamos avaliar o comportamento resultante com o parâmetro modificado.

Dos achados e da avaliação desta comissão em novembro/2021: O investigador percebeu um parâmetro no código fonte (`mcriptografar`) que tinha a sua condição inicial de operação de forma explícita e que isso poderia comprometer a integridade do Boletim de Urna (BU) gerado, caso essa condição fosse alterada.
Não obtendo êxito nas tentativas no arquivo de configuração, foi solicitada à equipe técnica de apoio a alteração dessa condição inicial para não criptografar, deixando-o em claro.
O BU, com as modificações realizadas no seu conteúdo, foi transmitido, mas rejeitado por inconsistência durante a verificação da sua assinatura digital no processo de transmissão.
Todavia, foi percebido que o BU original era recebido e validado mesmo sendo transmitido em claro, somente com a sua assinatura digital.
A equipe técnica da Justiça Eleitoral informa que o procedimento de configuração da criptografia do BU existe no sistema da Urna Eletrônica para permitir a geração de BU em claro quando a mesma for cedida para ser utilizada em eleições na sociedade.

Adequações realizadas pelo TSE: Estuda-se a possibilidade de não rejeitar o BU em claro na recepção.

Teste de confirmação: Foi realizada uma transmissão de BU em claro e confirmado que o mesmo foi assinalado com uma informação de erro na listagem de acompanhamento.

Avaliação do teste de confirmação: A alteração da configuração para não criptografar o BU não apresentou nenhuma anomalia no comportamento do sistema de transmissão e

[1] EDITAL DO TESTE PÚBLICO DE SEGURANÇA - TPS - ELEIÇÕES 2022, disponível em https://www.justicaeleitoral.jus.br/tps/arquivos/TPS-edital.pdf

recepção do BU, pois o sistema verifica somente a assinatura do arquivo. A princípio, o sistema de transmissão e recepção do BU é somente um meio de transporte de arquivo eletrônico de forma segura, verificando se o arquivo recebido é o mesmo transmitido, o que foi comprovado no teste. A abertura do BU é resolvida na instância posterior ao recebimento do BU.
Cabe à Justiça Eleitoral analisar e registrar os riscos associados ao uso da criptografia nas eleições oficiais e avaliar a necessidade da cifração do BU. Apesar de ser uma questão pontual, a decisão deverá ser consistente com todo o processo.

2.2 Plano de Teste 6 [**Teste não intrusivo da urna eletrônica 2015 (keylogger não intrusivo)**] - Será colocado um invólucro na urna com o objetivo de coletar os votos, relacionando os mesmos com o *timestamp*.

Dos achados e da avaliação desta comissão em novembro/2021: O teste consiste na instalação de uma capa no teclado da urna eletrônica, devidamente projetada, munida de sensores capazes de transmitir todas as teclas pressionadas pelo eleitor para o registro do seu voto, possibilitando a coleta dos votos a distância.
O dispositivo prototipado foi muito bem construído cobrindo toda superfície frontal da urna, dificultando a percepção da alteração efetuada na urna. O funcionamento ocorreu de forma planejada possibilitando a leitura de todas as teclas utilizadas na urna durante uma votação.

Adequações realizadas pelo TSE: Revisão dos procedimentos de treinamento de mesários e simulação com três cabines de votação de diferentes alturas.

Teste de confirmação: Os ajustes na altura das cabines de votação melhoram a visão dos mesários para observar movimentos anormais realizados pelo eleitor. Todavia, foi evidente que a redução da altura da cabine de votação aumenta a dificuldade para colocar um invólucro sobre os teclados da urna, mas não suficiente para impedir o ato.

Avaliação do teste de confirmação: A simulação realizada indica a relevância dos controles e ação dos mesários durante o trânsito do eleitor desde a sua entrada na seção até a saída após a conclusão do voto. Os TRE, que efetivamente operacionalizam as eleições nas seções eleitorais, devem manter estudos e discussões continuadas para o aprimoramento dos processos.
A viabilidade do emprego da proposta apresentada é uma questão que deve ser acompanhada pela Justiça Eleitoral pois a disponibilidade da engenharia da tecnologia a ser utilizada pode ocorrer a qualquer momento, impactando na atenção necessária dos mesários na seção eleitoral.

2.3 Plano de Teste 12 [**Extração de dados e configurações do Kit JE Connect**] - 1. Obter senhas e configuração da VPN a partir de uma mídia do JE Connect. 2. A partir dos dados obtidos tentar se conectar diretamente à rede do TSE. 3. Verificar a existência de vulnerabilidades no RecArquivos utilizando técnicas de *fuzzing* 4. Verificar a possibilidade de acesso direto ao banco de dados e as suas rotinas.

Dos achados e da avaliação desta comissão em novembro/2021: A proposta de teste de obtenção dos dados de configuração e senhas gravadas internamente no sistema do kit de transmissão de dados de eleição foram executadas com relativo sucesso. As senhas de acesso aos aplicativos e de inicialização foram fornecidas após algumas tentativas sem sucesso.
A partir desse ponto, os investigadores conseguiram avançar nos seus planos e obter as chaves gravadas internamente no sistema e obtendo o controle de acesso às partições do disco do computador alvo.
Os resultados obtidos demonstraram que um usuário interno habilitado somente para ativar o aplicativo de transmissão de dados pode chegar a partes do sistema que deveriam estar protegidas para impedir acesso a outros recursos do computador e da rede.
Apesar de obter o acesso à VPN (rede com conexão protegida), não obtiveram sucesso para observar os detalhes da porta conectada no destino por conta dos demais mecanismos de segurança de rede existentes.
A configuração do ambiente estava simulando o período eleitoral e a senha de acesso expirou às 20h da sexta-feira, forçando a inicialização de todo o processo no dia seguinte com uma nova senha (“oficial” para as eleições), liberada somente no dia anterior das eleições.
O teste demonstrou uma vulnerabilidade de acesso à rede que, mesmo estando protegida por outros mecanismos e contendo a invasão exclusivamente no ambiente definido pelo canal da VPN, pode permitir o desenvolvimento de ações que podem gerar novos riscos de ataques.

Adequações realizadas pelo TSE: Ajuste para uma atuação mais robusta dos módulos que monitoram e controlam o acesso à VPN e as operações realizadas para a transferência do BU aos sistemas de recepção e totalização, rejeitando os acessos não previstos e revogando as credenciais autenticadas e habilitadas inicialmente.

Teste de confirmação: Apesar do processo de obtenção do certificado ter ocorrido com sucesso, o mesmo foi imediatamente invalidado por ter sido utilizado por meios não previstos (módulo JE Connect oficial), impedindo o acesso para o estabelecimento de conexão pela rede (VPN). Outros procedimentos foram realizados com o segundo kit fornecido, mas sem sucesso.

Avaliação do teste de confirmação: Os ajustes realizados tornaram o processo de acesso à rede mais seguro, restringindo a conexão e a transferência dos BU a processos que são executados e verificados tanto na conexão como nos processos de transferências de arquivos.

Todavia, há necessidade de uma revisão geral para avaliar novamente as vulnerabilidades e os riscos associados tanto nos módulos de conexão e transmissão como de recepção e tratamento das transações na rede.

2.4 Plano de Teste 16 [**Segurança do JE Connect e do Firefox**] - Garantir a integridade e segurança do JE Connect com o Firefox em cenários de falha e cenários de ataque diversos, pois esses são executados em ambientes fora do controle do TSE.

Dos achados e da avaliação desta comissão em novembro/2021: O teste objetiva ter acesso à rede por meio do aplicativo de transmissão de dados (JE Connect).

O investigador verificou uma vulnerabilidade existente no acesso à rede do aplicativo copiando o caminho em uma outra seção do navegador, como se fosse uma nova requisição de acesso, e conseguiu navegar na rede com sucesso.

O uso de produtos comerciais deve ser estudado com cuidado pela Justiça Eleitoral por terem sido desenvolvidos para garantir as facilidades necessárias para a navegação na rede de dados.

Como a restrição de acesso à rede foi um requisito estabelecido para a aplicação (JE Connect) e a sua camada de proteção (SIS) e não para o navegador web (Firefox), que faz parte integrante do sistema de transmissão, a vulnerabilidade foi bem explorada pelo investigador.

Adequações realizadas pelo TSE: Ajustes no ambiente para monitorar e controlar os processos e teclas utilizadas, rejeitando os caracteres não necessários para a operação de conexão à rede.

Teste de confirmação: Os testes confirmaram que não foi possível inserir os comandos necessários para passar pelo sistema de controle de conexão da rede.

Avaliação do teste de confirmação: Os ajustes necessários para que o navegador atue de forma integrada com o JE Connect reduzem sensivelmente a superfície de ataque disponível. A segurança do sistema de transmissão do BU eleva o seu nível de confiabilidade, associando-se aos demais ajustes realizados em decorrência do plano de teste 12.

Foi percebida uma degradação no desempenho do JE Connect por conta dos ajustes realizados. Recomenda-se uma revisão e avaliação de impacto durante as eleições.

2.5 Plano de Teste 20 [**Violar o sigilo do voto**] - O TSE garante o direito do voto a todos os cidadãos, incluindo aquelas pessoas com deficiência visual. Neste contexto, as urnas eletrônicas proporcionam a inclusão social desses cidadãos. Basicamente, consiste de uma fonte de ouvido no qual o deficiente visual, ao digitar nas teclas identificada por impressão em braille, pode-se ouvir o número digitado, ratificando sua opção de voto. A tentativa de violar o sigilo do voto, consiste em capturar o áudio

disponibilizado por esta saída de áudio e, consequentemente, em quebrar o sigilo do voto para pessoas com ou sem deficiência visual durante o processo de votação, observando a ordem dos votantes da respectiva seção eleitoral.

Dos achados e da avaliação desta comissão em novembro/2021: O investigador testou a possibilidade de utilização da saída de áudio da urna eletrônica para transmitir todo o processo existente de acessibilidade para os eleitores com deficiência visual.
A vulnerabilidade explorada não se limita aos casos de deficientes visuais, uma vez que essa facilidade de áudio pode ser utilizada por um eleitor que tenha dificuldade em ler e interpretar as mensagens apresentadas na tela, ou para confirmar os números digitados, desde que habilitado pelo mesário para cada eleitor.

Adequações realizadas pelo TSE: Revisão dos procedimentos de treinamento de mesários para observar a habilitação do áudio, a conexão dos fones e o encerramento deste processo.

Teste de confirmação: Todos os movimentos, tanto de habilitação do áudio como a instalação do fone de ouvido, foram verificados, confirmando o correto funcionamento dos mesmos.

Avaliação do teste de confirmação: Os reforços no treinamento dos mesários mostraram-se suficientes para inibir este tipo de ataque.
Os mesários devem registrar na ata da seção eleitoral a habilitação e o uso da interface auditiva sempre que o eleitor necessitar, ou solicitar, a facilidade e não tiver registro no seu cadastro eleitoral.

3 Recomendações TPS 2021

As informações aqui apresentadas abrangem as recomendações do Relatório da Comissão Avaliadora registradas em dezembro de 2021, após o encerramento dos testes de segurança efetuados pelos investigadores inscritos, considerando as revisões efetuadas pela equipe técnica do TSE e os testes de confirmação. As recomendações anteriores que não fazem parte do escopo deste documento continuam mantidas para uma análise do TSE.

3.1 Documentação das barreiras facilitadas para a execução dos planos

Os testes estão evoluindo a cada etapa, identificando que os sistemas eleitorais desenvolvidos estão maduros e seguros quando observados como um sistema, ou

subsistema. Os elos entre os subsistemas asseguram a maior parte da segurança e confiabilidade do sistema.

Todavia, quando um subsistema, ou parte dele, é verificado, nota-se a falta de documentação adequada para suportar as decisões técnicas e tecnológicas adotadas. Analogamente, a alteração em um subsistema, independentemente da motivação, deveria nortear a revisão geral de todos os demais subsistemas e o sistema como um todo (análise de risco).

Ao facilitar as barreiras para que os investigadores possam avançar nos seus planos e intentos, há uma certa dificuldade em entender esse novo ambiente. As respostas fornecidas, ou as solicitações de facilidade atendidas estão ainda fundamentadas nos conhecimentos dos desenvolvedores e suas percepções.

Recomenda-se a revisão, complementação e divulgação desses documentos, para adequar os testes e os planos e garantir os objetivos do TPS de forma mais eficaz.

O registro claro das barreiras que foram elevadas para que o Plano de Testes pudesse ser executado torna-se imprescindível em todos os passos da documentação. A cada estágio vencido do Plano de Testes, o registro correspondente de barreiras abertas deverá ser mencionado. Isto fará com que o ambiente de teste torne-se mais transparente e realista do ponto de vista do registro de todos os elementos e condições necessárias para a realização dos mesmos.

A existência dos documentos dessa natureza contribui para que os investigadores e os interessados possam focar nas suas propostas e elaborar os planos de forma consistente com o tempo que o evento proporciona. Também serve de base de transparência para uso na divulgação dos resultados.

3.2 Quanto ao ambiente de realização do TPS

a. Considerando o regulamento que dispõe sobre a segurança física, o acesso ao ambiente e a divulgação dos resultados obtidos pelos investigadores no TPS, e a área preparada para que a imprensa e os observadores externos possam acompanhar o funcionamento do TPS, recomenda-se uma revisão dos espaços utilizados pelos investigadores para prover privacidade aos mesmos em relação ao público externo. O objetivo é a realização dos testes de forma reservada e em ambiente controlado.

b. Considerando que o TPS 2021 teve uma equipe de apoio técnico, composta pelo corpo acadêmico da USP, seria adequado disponibilizar uma bancada com todos os elementos usados no TPS, de forma a possibilitar a avaliação e testes operacionais para subsidiar tanto a equipe técnica como os investigadores.

c. Recomenda-se que todo o ambiente disponibilizado ao investigador esteja previamente descrito, especialmente quanto aos quesitos associados a barreiras de segurança liberadas por solicitação do investigador e constante no plano de teste apresentado e aprovado.

3.3 Relativo ao modelo distribuído de conexão à rede da JE para envio dos dados de apuração da UE

a. Recomenda-se avaliar a adoção de modelo centralizado de conexão dos agentes remotos para facilitar a identificação de tentativas de acesso indevido e manter um registro centralizado de eventos no envio dos dados de apuração provenientes das urnas.

b. O Transportador continua sendo um item necessário para os agentes remotos. Para evitar *man-in-the-middle*, faz-se necessário uso de um aplicativo no lado do usuário para validação do servidor de aplicação para o qual serão enviados os arquivos de apuração (*certificate pinning* ou equivalente). As adequações efetuadas nos sistemas de monitoramento e controle do acesso à rede e funcionamento do aplicativo de transporte, após a revisão, melhoraram consideravelmente a segurança.

   Ainda, deve-se manter o Módulo Transportador o mais simples possível, eliminando funcionalidades desnecessárias à sua operação.

c. Avaliar os mecanismos de autenticação, autenticidade e auditoria existentes para acesso ao RecArquivos, imaginando o cenário onde as conexões são oriundas de um elemento na rede interna da JE, ou então no caso em que os boletins de urna e RDVs seriam enviados por fora do JEConnect, sem passar pelas validações no lado cliente;

d. Uso de *token* criptográfico para armazenamento das chaves privadas usadas pelos agentes remotos;

e. 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:

   e.1 Um dos pontos positivos de uso de certificado ICP-Brasil é que esse modelo facilitaria a logística de distribuição de *tokens*, já que os mesmos estariam de posse dos agentes externos previamente, para uso em outras atividades rotineiras.

   e.2 Analisar como operacionalizar a homologação dos agentes remotos que terão acesso ao sistema RecArquivos durante o pleito (cabe avaliar,

nesse caso, a adequação de um portal com duplo fator de autenticação com uso de login/senha e um *token* de autenticação).

Considerando que os boletins de urna enviados para totalização e as tabelas de correspondências deverão ser publicados tão logo que recepcionados pelo TSE, em atendimento ao Art 230, da Resolução 23.686, de 03 de março de 2022, as recomendações aqui registradas deverão ser revistas para estar consistentes com o modelo e os procedimentos a serem empregados nas eleições de 2022.

3.4 Dar maior publicidade ao Boletim de Urna com uma revisão da necessidade da criptografia a ele aplicado

a. Considerando que o boletim de urna é divulgado nas seções eleitorais após o encerramento da votação e as cópias distribuídas aos representantes dos partidos políticos presentes e ao comitê interpartidário, deve-se rever a necessidade em criptografar o boletim de urna. Todavia, isso será viável somente se a Justiça Eleitoral ampliar a divulgação do procedimento realizado na seção eleitoral e também viabilizar a sua distribuição na forma eletrônica. A função da criptografia em boletim de urna assinada digitalmente deverá ser revista.

b. Avaliar a possibilidade do TSE abrir canal de distribuição dos boletins de urna com os partidos e entidades de controle, facilitando a totalização pelos interessados. Não se vê aumento de risco ao processo eleitoral com essa abertura, já que são itens públicos disponíveis de forma impressa nas seções eleitorais após sua apuração. Porém é necessário dar ampla divulgação ao público em geral de que ele é um item aberto para que todos os cidadãos possam acompanhar o processo eleitoral.

3.5 Quanto às questões relativas às UE

a. Considerando que os riscos associados a disponibilização do código fonte da UE em plataforma aberta, além das dependências com o hardware para sua operação, podem ser avaliados por meio de estabelecimento de convênios e contratos específicos com entidades externas, de amplo espectro e idôneas, incluindo as entidades acadêmicas e de pesquisa.

b. Todos os melhoramentos tecnológicos previstos e adotados pelo TSE deverão estar documentados, desde os estudos preliminares teóricos e conceituais até a escolha definitiva para a adoção e incorporação na UE. Estes documentos devem servir de base para a reavaliação dos riscos.

c. Considerando que a Justiça Eleitoral utiliza as UE em eleições ordinárias em instituições e na sociedade, e parte dos aplicativos são compartilhados com as

eleições oficiais, recomenda-se uma revisão de todos os sistemas e subsistemas para mitigar os riscos associados e impactos decorrentes.

3.6 Busca por novas abordagens para os desafios do Processo Eleitoral

a. 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 for objeto desta premiação deve ter ampla publicidade, com justificativas para embasamento de sua concessão.

b. Criar “trilhas”, isto é, caminhos ou pontos focais, alinhadas com os objetivos específicos do processo eleitoral, mas não necessariamente associados ao hardware ou software em uso, para exercitar as investigações orientadas ao aprimoramento dos sistemas eleitorais, quebra de barreiras tecnológicas e geração de novas proposições conceituais para as eleições do futuro.

4 Considerações Finais

O evento do TPS 2021 apresentou uma equipe técnica capacitada para dar apoio aos investigadores, abrangendo a vasta área de conhecimento técnico e de procedimentos eleitorais. Esse ambiente proporciona respostas em tempo adequado para que os investigadores pudessem dominar, a cada dia do evento, as características inerentes dos processos e sistemas eleitorais, adequando os seus planos e avançando nos trabalhos. O tempo de exposição dos investigadores nesse tipo de ambiente é reduzido, mas adequado aos objetivos do TPS (exposição dos sistemas no período compreendido entre o preparo e a realização das eleições).

Observa-se ao longo dos eventos do TPS realizados de 2009 até o momento, que os resultados apresentados demonstram a maturidade dos sistemas eleitorais. Todavia, nota-se, em alguns testes, que os avanços obtidos pelos investigadores demonstram também a relevância dos subsistemas e componentes que, isoladamente, ainda apresentam espaços para melhoria nos quesitos relativos à qualidade do projeto e à dependência dos mecanismos de segurança externos ao mesmo (riscos internos e externos).

O retorno de alguns investigadores para verificar as correções e os ajustes realizados pela equipe técnica da Justiça Eleitoral foi um momento importante para registrar o início dos preparativos operacionais das eleições de 2022.

A publicação da Portaria nº 540, de 23 de agosto de 2021, do TSE, que dispõe sobre a instituição da Norma de Desenvolvimento Seguro de Sistemas, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral, renova o conjunto de documentos que regulamenta os desenvolvimentos realizados até o momento e acrescentará, com certeza, aperfeiçoamentos procedimentais e tecnológicos em consonância com as ameaças modernas. Aguarda-se que os quesitos de análise de cada caso de desenvolvimento e emprego dos mecanismos de segurança e as respectivas documentações estejam atendidos, ou encaminhados, para a realização das eleições gerais de 2022.

A análise dos processos, sistemas, subsistemas e componentes, avaliados continuamente de acordo com o cenário dinâmico de candidaturas, campanhas e divulgação de informações eleitorais garantirão a capacidade de rever os riscos de forma consistente, transmitindo a segurança e a confiabilidade aos eleitores para terem a certeza do valor do seu voto realizado, amparado pela Justiça Eleitoral.

Sandro Nunes Vieira

Patricia Sumie Hayakawa

Robson Paniago de Miranda

Thiago de Sá Cavalcanti

André Luiz Furtado Pacheco

Cláudio Lisboa de Souza

Rafael Timóteo de Sousa Júnior

Mamede Lima Marques

Osvaldo Catsumi Imamura

Jamil Salem Barbar