**TRIBUNAL SUPERIOR ELEITORAL**

Ofício nº 635 GAB-DG

Brasília, 21 de fevereiro de 2018.

A Sua Senhoria o Senhor
DIEGO DE FREITAS ARANHA
dfaranha@ic.unicamp.br

Assunto: **Convite. Teste de Confirmação. Teste Público de Segurança 2017**

Prezado Diego,

O Tribunal Superior Eleitoral, em cumprimento ao art. 37 do edital do *Teste Público de Segurança de 2017* e ao art. 16, § 1º, da Resolução TSE nº 23.444/2015, realizará, nos dias 7 e 8 de maio de 2018, o Teste de Confirmação dos sistemas eleitorais relativo ao *Teste Público de Segurança 2017* (TPS – 2017).

Na ocasião, os investigadores e/ou grupos de investigadores poderão repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha ou a vulnerabilidade explorada. **A nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano que identificou a falha ou a vulnerabilidade explorada, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.**

Dessa forma, visando à Transparência do Processo Eleitoral Brasileiro e ao atendimento dos normativos reguladores do TPS, convido-o a participar do **Teste de Confirmação nos dias 7 e 8 de maio de 2018, das 9h às 18h, no espaço multimídia no subsolo do Edifício Sede do Tribunal Superior Eleitoral, em Brasília – DF.**

**Solicito que seja informado, até o dia 6/4/2018, o interesse na participação do referido evento. Após essa data, caso não haja manifestação, o investigador não estará habilitado a realizar o teste de confirmação.**

Caso haja interesse no custeio de diárias e passagens, encaminhar o formulário "TPS2017 – Formulário Diárias e Passagens – Teste de Confirmação.docx" (anexo) preenchido em ferramenta de edição de texto (não entregar documento preenchido à mão e digitalizado).

Atenciosamente,

**RODRIGO CURADO FLEURY**
**DIRETOR-GERAL**

Documento assinado eletronicamente em **21/02/2018, às 19:15**, 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=0662085&crc=674F19EF, informando, caso não preenchido, o código verificador **0662085** e o código CRC **674F19EF**.

2018.00.000001601-6 Documento nº 0662085 v7

Diego F. Aranha
Instituto de Computação – UNICAMP
Av. Albert Einstein, 1251
Campinas/SP, Brasil – CEP 13082-852

21 de Março, 2018

À Diretoria Geral do Tribunal Superior Eleitoral,

Prezado Rodrigo Curado Fleury,

No papel de representante do Grupo 1, participante dos Testes Públicos de Segurança (TPS) realizados entre 28 de Novembro e 01 de Dezembro de 2017, e composto por Pedro Barbosa, Thiago Carneiro, Caio Lüders e Paulo Matias, confirmo o recebimento do convite para os testes de confirmação no TSE, a serem conduzidos entre 7 e 8 de Maio próximos.

Apesar das condições de trabalho ruins, com restrições artificiais de tempo, escopo, uso de papel e recursos tecnológicos, a equipe foi capaz de detectar durante o TPS múltiplas vulnerabilidades no software de votação, como armazenamento inseguro de chaves criptográficas no código-fonte e ausência de verificação de integridade de módulos do software. A exploração dessas vulnerabilidades permitiu recuperar o conteúdo às claras de cartões de memória para instalação de software, adulterar o software e consequentemente introduzir código estranho para execução no equipamento, de maneira a forçar que seu comportamento desviasse do originalmente programado.

A capacidade de adulterar o software de votação foi ilustrada de múltiplas formas: pela adulteração dos registros cronológicos mantidos pela urna, acoplamento de um teclado para emitir comandos, violação do sigilo de um voto específico, e até alteração de mensagens apresentadas ao eleitor para fazer propaganda para um certo candidato. Houve progresso substancial no desvio de votos entre candidatos distintos, dado que todas as condições necessárias para tal já haviam sido alcançadas com a adulteração do software de votação, bastando apenas descobrir as posições dos programas a serem modificadas. Houve ainda sucesso ao se descobrir essas posições para impedir a urna eletrônica de registrar os votos de um eleitor, disparando um erro de consistência no software. As atividades da equipe foram interrompidas às 18h da sexta-feira, dia 01 de Dezembro, após determinação da organização do evento e a instrução de que "nenhum resultado após aquele momento teria validade".

Apesar do registro claro desses eventos em relatório técnico publicado pelo TSE [1], esse não parece ter sido o entendimento dos representantes do Tribunal que participaram da Audiência Pública no Senado em 13 de Março deste ano [2]. Foram repetidas as alegações de que **a equipe não foi capaz de "alterar o voto" ou "modificar destinação de voto" depositado na urna eletrônica**. Essas alegações são estritamente falsas, na medida que o ataque parcial já foi capaz de **impedir** que votos fossem registrados pelo equipamento, portanto alterando sua destinação. O desvio de votos entre candidatos é uma consequência natural e lógica desse resultado, tendo sido validado em ambiente simulado no computador disponibilizado à equipe, e só não foi demonstrado na urna por falta de tempo e interesse posterior do próprio TSE.

Na mesma ocasião, também foi relatado pelo Sr. Giuseppe Janino, secretário de Tecnologia da Informação, que as vulnerabilidades encontradas eram **novas e não estavam presentes na versão do sistema examinada na edição de 2012 do TPS**. A falsidade dessa afirmação pode ser trivialmente verificada na página 25 do relatório publicado pela equipe vencedora naquele evento, dentro da seção 4.1.5 que documenta as múltiplas vulnerabilidades detectadas no sistema, intitulada "Presença de chaves no código-fonte" [3]:

*O compartilhamento da chave de cifração das mídias é agravado pela sua presença às claras no código-fonte do software. Isto significa que qualquer agente interno que possua acesso ao repositório onde é mantido o código-fonte também possui automaticamente acesso à chave criptográfica que protege as partições cifradas dos cartões de memória, podendo realizar o vazamento de impacto devastador mencionado anteriormente. Além disso, isto também significa que a chave de cifração faz parte do módulo do sistema operacional responsável por acessar a partição cifrada e tornar disponível seu conteúdo, e por isso precisa estar armazenada às claras dentro do próprio cartão de memória. Ou seja, o objeto cifrado é armazenado no mesmo lugar em que é armazenada a chave criptográfica que o decifra, qualificando este mecanismo como apenas de ofuscação ao invés de verdadeira segurança.*

Para verificação independente, esse mesmo relatório foi publicado em volume dedicado à Justiça Eleitoral dos Cadernos Adenauer 1/2014, páginas 117-133 [4].

Em virtude do **desrespeito público e recorrente quanto aos resultados técnicos** obtidos pelas equipes, como aliás tem acontecido de forma frequente após os Testes Públicos de Segurança, a equipe que represento decidiu por **impor um requisito adicional para sua participação nos testes de confirmação**. Além dos testes de confirmação das correções para vulnerabilidades descobertas, conforme previsto em edital, a equipe solicita poder prosseguir com os ataques de desvio de votos por adulteração do software demonstrado como vulnerável durante o TPS 2017. Para isso, solicita também ter disponível a mesma versão do software disponibilizada no TPS 2017, além de uma urna eletrônica capaz de receber a carga desta versão, com mesma revisão de hardware da utilizada no TPS 2017.

O objetivo da equipe é demonstrar experimentalmente que uma vulnerabilidade de software no ambiente da urna pode ser catastrófica: assim como em qualquer sistema de software, o acesso privilegiado é suficiente para adulterar o funcionamento do sistema de maneira arbitrária. Tal fato é bem compreendido pela comunidade técnica, mas parece não ser de entendimento dos representantes do Tribunal. Além disso, é notório que as mitigações em software discutidas no escopo do TPS não resolvem os principais problemas de segurança da urna eletrônica. Temos esperança que, com uma demonstração mais enfática das consequências de uma vulnerabilidade de software, talvez façamos entender a importância da implementação do registro físico do voto pelo Tribunal.

Caso não seja possível atender à solicitação, a colaboração da equipe com as atividades do TPS 2017 está encerrada. As referências acima podem ser encontradas abaixo:

[1] `http://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017`

[2] `https://www.youtube.com/watch?v=ECVkrxiQDRc`

[3] `https://sites.google.com/site/dfaranha/projects/relatorio-urna.pdf`

[4] `http://www.kas.de/wf/doc/13775-1442-5-30.pdf`

Atenciosamente,

Prof. Dr. Diego F. Aranha,
Representande do Grupo 1 no TPS

**TRIBUNAL SUPERIOR ELEITORAL**

Ofício nº 635 GAB-DG

Brasília, 21 de fevereiro de 2018.

A Sua Senhoria o Senhor
DIEGO DE FREITAS ARANHA
dfaranha@ic.unicamp.br

Assunto: **Convite. Teste de Confirmação. Teste Público de Segurança 2017**

Prezado Diego,

O Tribunal Superior Eleitoral, em cumprimento ao art. 37 do edital do *Teste Público de Segurança de 2017* e ao art. 16, § 1º, da Resolução TSE nº 23.444/2015, realizará, nos dias 7 e 8 de maio de 2018, o Teste de Confirmação dos sistemas eleitorais relativo ao *Teste Público de Segurança 2017* (TPS – 2017).

Na ocasião, os investigadores e/ou grupos de investigadores poderão repetir, em versão ajustada do sistema eleitoral, os testes que identificaram a falha ou a vulnerabilidade explorada. **A nova execução dos testes não poderá ter direcionamento diferente do estipulado no plano que identificou a falha ou a vulnerabilidade explorada, podendo o plano ser alterado somente em função das correções realizadas nos sistemas afetados.**

Dessa forma, visando à Transparência do Processo Eleitoral Brasileiro e ao atendimento dos normativos reguladores do TPS, convido-o a participar do **Teste de Confirmação nos dias 7 e 8 de maio de 2018, das 9h às 18h, no espaço multimídia no subsolo do Edifício Sede do Tribunal Superior Eleitoral, em Brasília – DF.**

**Solicito que seja informado, até o dia 6/4/2018, o interesse na participação do referido evento. Após essa data, caso não haja manifestação, o investigador não estará habilitado a realizar o teste de confirmação.**

Caso haja interesse no custeio de diárias e passagens, encaminhar o formulário "TPS2017 – Formulário Diárias e Passagens – Teste de Confirmação.docx" (anexo) preenchido em ferramenta de edição de texto (não entregar documento preenchido à mão e digitalizado).

Atenciosamente,

**RODRIGO CURADO FLEURY**
**DIRETOR-GERAL**

Documento assinado eletronicamente em **21/02/2018, às 19:15**, 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=0662085&crc=674F19EF,

informando, caso não preenchido, o código verificador **0662085** e o código CRC **674F19EF**.

**TRIBUNAL SUPERIOR ELEITORAL**

Memorando nº 52 STI

À Diretoria-Geral

Assunto: **Resposta. Representante. UNICAMP. Teste de Confirmação. Teste Público de Segurança**

1. Trata-se de manifestação quanto à resposta da equipe do prof. Diego Aranha (Grupo 1) ao convite para participação no Teste de Confirmação relativo ao Teste Público de Segurança - TPS 2017. Por oportuno, faz-se também uma série de esclarecimentos sobre diversas questões apontadas pelo professor em seu documento, de acordo com as manifestações da Coordenadoria de Sistemas Eleitorais (SEI 0700908) e da Seção de Voto Informatizado (SEI 0701159).

2. Em sua resposta, o prof. Diego Aranha condiciona a participação da sua equipe no Teste de Confirmação nos seguintes termos:

> Além dos testes de confirmação das correções para vulnerabilidades descobertas, conforme previsto em edital, a equipe solicita poder prosseguir com os ataques de desvio de votos por adulteração do *software* demonstrado como vulnerável durante o TPS 2017. Para isso, solicita também ter disponível a mesma versão do *software* disponibilizada no TPS 2017, além de uma urna eletrônica capaz de receber a carga desta versão, com mesma revisão de *hardware* da utilizada no TPS 2017.

**3. Esta Secretaria de Tecnologia da Informação entende que não há elementos que justifiquem que a condição imposta pela equipe do prof. Diego Aranha seja acatada pelo Tribunal, tanto do ponto de vista normativo quanto do técnico**.

4. O Tribunal Superior Eleitoral, por meio da Resolução TSE Nº 23.444/2015, tornou obrigatória a realização do TPS com o objetivo de contar com a colaboração da comunidade acadêmica no processo de melhoria contínua dos sistemas eleitorais, a saber:

> 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.

5. Essa colaboração se dá por meio de planos de ataque produzidos pelas equipes de investigadores, que buscam explorar eventuais vulnerabilidades verificadas na fase prévia de análise do código-fonte dos sistemas eleitorais. Havendo sucesso na execução desses planos de ataque, a Resolução TSE Nº 23.444/2015 estabelece em seu art. 16 a possibilidade de os investigadores serem convocados para executar novamente em uma nova versão dos sistemas eleitorais os mesmos testes, nos seguintes termos:

> 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.

6. Portanto, **o normativo vigente sobre o TPS determina que o Teste de Confirmação deve ser realizado sobre nova versão do *software*, com as devidas correções, exclusivamente para a validação da mitigação das vulnerabilidades encontradas**.

7. Essa metodologia definida na Resolução visa estabelecer um processo lógico de melhoria dos sistemas eleitorais contendo a busca de vulnerabilidades executadas pelos investigadores, sua correção pela equipe técnica e posterior verificação desta correção pelos investigadores, garantindo assim não só a concretização do objetivo de aprimoramento dos sistemas eleitorais, como também a indispensável transparência ao processo de construção dos referidos sistemas.

8. Durante o TPS 2017, a equipe liderada pelo professor fez inúmeras tentativas de modificação do voto gravado no arquivo de RDV logo após a confirmação pelo eleitor. Esse ataque somente foi possível devido à presença de três vulnerabilidades, já devidamente documentadas por esta equipe técnica em seu relatório [1]:

1. obtenção da chave de criptografia do sistema de arquivos dos cartões de memória das urnas, o que permitiu à equipe do professor copiar os arquivos da mídia, modificá-los e recolocar versões alteradas na mídia de carga;
2. defeito no mecanismo de verificação de assinatura digital de bibliotecas de *link* dinâmico no kernel do Linux, o que permitiu que código executável adulterado fosse executado pela urna; e
3. ausência de assinatura digital complementar em duas bibliotecas de *link* dinâmico, o que impediu que o próprio *software* detectasse automaticamente a manipulação dessas bibliotecas.

9. Sobre a condição imposta pelo grupo para a participação no Teste de Confirmação do TPS 2017, **não há qualquer elemento técnico ou acadêmico que demonstre benefício na continuidade das tentativas de adulteração do voto**, tais como vinham sendo executadas em novembro. É importante lembrar que essas tentativas só foram possíveis diante da presença das três vulnerabilidades relatadas acima. Na medida em que esses defeitos são corrigidos, não faz sentido falar em execução de código arbitrário na urna eletrônica, uma vez que bibliotecas ou executáveis modificados não serão executados por apresentarem assinatura digital inválida. Todos os ataques bem-sucedidos demonstrados pelo grupo durante o TPS 2017 – alteração de mensagem no arquivo de log, utilização de teclado externo, decifração do RDV e alteração de texto na tela do *Software* de Votação – são consequência das três vulnerabilidades descritas acima. A tentativa de adulteração de voto é apenas mais uma ilustração desses três defeitos, não agregando nenhum valor técnico quanto à identificação das vulnerabilidades encontradas.

10. Encerrados os esclarecimentos sobre o mérito da solicitação da equipe liderada professor, faz-se necessário agora elucidar os demais pontos apresentados em seu documento de resposta.

11. A Secretaria de Tecnologia da Informação deste Tribunal entende que as condições de trabalho disponibilizadas para o TPS foram adequadas aos objetivos propostos ao teste, sendo as mesmas para todos os participantes. Todas as solicitações feitas pelo Grupo 1 e pelos demais investigadores foram prontamente analisadas e atendidas, não havendo restrições artificiais de qualquer espécie. Apenas seguiu-se a correta formalização dos requerimentos, como é

indispensável à administração pública. Ademais, todo o registro é fundamental para que um plano de teste seja repetível, de modo que as equipes técnicas desta STI possam trabalhar nas correções das vulnerabilidades que venham a ser encontradas durante o TPS.

12. Durante a realização do TPS 2017, todas as tentativas de modificação do voto foram detectadas pelo *Software* de Votação, que reportou inconsistência no registro dos votos e interrompeu a sua execução. Em sua resposta, o professor alega que o impedimento do registro de um voto na urna, ainda que seja por erro detectado pelo próprio *software*, já caracterizaria o desvio de votos. Contudo, essa afirmação não é correta. Em caso de mau funcionamento da urna eletrônica, inclusive por falha de *software*, os procedimentos de contingência são efetivados, os quais incluem a substituição do equipamento e até a adoção do voto manual em cédulas de papel. Dessa forma, permite-se que haja a continuidade da votação com a garantia do respeito à manifestação do eleitor. Portanto, não há que se falar em desvio de votos, mas sim em tentativa de negação de serviço – a qual é infrutífera devido aos procedimentos de contingência previstos.

**13. Quanto à alegação do prof. Diego Aranha de que o Sr. Secretário de Tecnologia da Informação deste Tribunal fez uma afirmação falsa perante comissão do Senado Federal, é necessário dizer que essa alegação é totalmente infundada e caluniosa**. Cabe ao corpo técnico do TSE, quando questionado sobre as ocorrências do TPS 2012, manifestar-se sobre o que foi realizado durante o evento. E, no Senado Federal, o questionamento foi expresso e claro quanto a não conformidade encontrada em 2012, relativa ao embaralhamento do RDV, e à sua permanência no *software* atual. É público e notório que a aleatoriedade dos votos gravados no RDV foi substancialmente melhorada, ainda em 2012, embora o prof. Diego tenha optado por não revisar essa questão, inclusive durante o TPS 2017.

14. Além disso, as três vulnerabilidades relatadas acima não foram exploradas no TPS 2012, sobretudo porque os defeitos 2 e 3 sequer estavam presentes naquela base de código-fonte. Quanto ao achado de número 1, ele de fato decorre de uma decisão de projeto que já estava presente em 2012. Esse tópico já foi comentado pelo Tribunal em outras oportunidades, e o próprio prof. Diego já reconheceu, em declarações recentes, que não há alternativa trivial para essa questão. Ainda assim, o corpo técnico da STI encontrou uma solução para a presença de chaves no código-fonte, que será submetida ao Teste de Confirmação do TPS 2017.

15. Ainda sobre a questão da presença de chaves no código, é importante destacar que foi uma escolha do prof. Diego à época não comunicar esse e outros tópicos diretamente ao Tribunal, mas sim fazê-lo por artigos publicados em meios diversos na Internet, semanas após o TPS 2012. Essa decisão não é compatível com uma postura colaborativa com a Justiça Eleitoral, com vistas ao aprimoramento da segurança dos sistemas eleitorais. A prática da indústria de *software* é a comunicação de vulnerabilidades primeiro ao desenvolvedor, para que esse possa corrigi-las e, em seguida, reconhecer e agradecer a autoria de quem identificou o defeito.

16. Outro ponto importante é que não há que se falar na necessidade de se esclarecer à equipe do Tribunal sobre as potencialidades da execução de código arbitrário num sistema informatizado. A adoção sistemática de técnicas de criptografia e assinatura digital, assim como a sua submissão a escrutínio público durante o TPS, demonstra por si só que esta equipe técnica tem plena ciência daquilo que um *software* maliciosamente adulterado é capaz de fazer.

17. Quanto à alegada notoriedade de que as mitigações de *software* no escopo do TPS não resolvem os problemas de segurança da urna eletrônica, é importante destacar que, em momento algum, o Grupo 1 documentou críticas relativas às soluções apresentadas pela STI em seu relatório técnico sobre os achados do TPS 2017. Na verdade, parece que todo o discurso é orientado à defesa da implantação do voto impresso. E sobre esse tópico, cabe apenas informar que a STI tem trabalhado para viabilizar a contratação de indústria eletrônica para a fabricação do quantitativo de módulos impressores adequado à primeira etapa de implantação do voto impresso, além de estar realizando grande esforço nas adaptações de *software* necessárias ao cumprimento da legislação vigente. Cabe destacar que técnicos da STI apresentaram artigo[2] em *workshop* científico organizado pelo próprio professor, no qual é apresentada a solução que está sendo implementada para as Eleições 2018, em detalhes.

18. Por fim, **a STI sugere a convocação da equipe do prof. Diego Aranha para participar do Teste de Confirmação – nos termos da Resolução TSE Nº 23.44/2015, que estabelece que os testes serão executados em uma nova versão do sistema eleitoral com as**

**devidas correções – a qual poderá então dar continuidade à sua profícua colaboração junto à Justiça Eleitoral**. Para tanto sugere-se a extensão do prazo de resposta em até cinco dias úteis após a emissão do convite.

---

[1] http://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017

[2] Registro impresso do voto, autenticado e com garantia de anonimato. Anais do SBSeg 2017, pág. 666-676 (https://sbseg2017.redes.unb.br/wp-content/uploads/2017/04/20171109_ANAIS_SBSEG_2017_FINAL_E-BOOK.pdf)

Respeitosamente,

**GIUSEPPE DUTRA JANINO**
**SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO**

Documento assinado eletronicamente em **11/04/2018, às 19:24**, 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=0704613&crc=8AF7B31A, informando, caso não preenchido, o código verificador **0704613** e o código CRC **8AF7B31A**.

2018.00.000001601-6 Documento nº 0704613 v4

Diego F. Aranha
Instituto de Computação – UNICAMP
Av. Albert Einstein, 1251. Campinas/SP, Brasil

19 de Abril, 2018

À Diretoria Geral do Tribunal Superior Eleitoral,

Prezado Rodrigo Curado Fleury,

Novamente no papel de representante do Grupo 1, manifesto posicionamento da equipe quanto à resposta recebida do Tribunal Superior Eleitoral em 13 de Abril de 2018.

A equipe aprecia o entendimento da área técnica do Tribunal de que as vulnerabilidades detectadas durante o TPS 2017 permitem adulteração arbitrária do *software* de votação, e um ataque com sucesso de desvio de votos seria apenas consequência natural da exploração dessa capacidade. É importante salientar que a manifestação anterior da equipe é muito clara quanto ao sucesso na **alteração ou modificação da destinação de votos** (e não desvio), concretizado ao se efetivamente impedir seu registro eletrônico e disparar erro de consistência no *software*.

A respeito do armazenamento inseguro de chaves criptográficas no código-fonte, que a área técnica insiste em defender por "decisão de projeto", cabe esclarecimento. Como é de conhecimento do Sr. Giuseppe Janino, sucessivas reuniões foram realizadas após o TPS 2012 para tornar evidente que outras vulnerabilidades existiam na base de código, além daquela exercitada no plano de teste que venceu a competição. Não houve interesse do TSE em conhecer essas vulnerabilidades durante essas reuniões, dado que o Tribunal preferiu tratar a questão sob o prisma de um Termo de Sigilo que nunca foi assinado e envolvimento do departamento jurídico. Desta forma, é também boa prática de segurança proceder com a divulgação integral de vulnerabilidades detectadas quando há omissão da parte interessada. Essa responsabilidade apenas aumenta em se tratando de sistemas críticos de interesse público. Nos últimos 6 anos, o Tribunal teve inúmeras oportunidades de interagir com a comunidade técnica em busca de uma solução para esse problema, que admitidamente não é trivial, mas não se justifica não haver progresso em um período de tempo tão longo.

Sendo impossível demonstrar o ataque de desvio de votos na versão vulnerável do *software* e havendo múltiplos conflitos com compromissos pessoais de vários integrantes que impedem sua participação nos dois dias dos Testes de Confirmação, não será possível repetir integralmente os planos de teste executados com sucesso. Sugere-se então visita técnica protocolar ao TSE de parte da equipe em 08 de Maio apenas para conhecer e validar as contramedidas para mitigar os riscos de fraude causados pelas vulnerabilidades detectadas no TPS 2017. Caso haja concordância com a participação nesses termos, os formulários de auxílio para deslocamento seguem em anexo a essa resposta formal.

Por fim, a equipe aprecia os esforços da área técnica na implantação do voto impresso, apesar das inúmeras e sucessivas manifestações públicas do TSE contrárias à introdução do mecanismo.

Atenciosamente,

Prof. Dr. Diego F. Aranha,
Representante do Grupo 1 no TPS